From: Reed, Matt FIN:EX
To: Onciul-Omelus, Jamie FIN:EX
Cc: Hoskins, Chad FIN:EX
Subject: FOI training session
Date: Friday, July 28, 2017 11:56:00 AM
Attachments: image001.jpg

Hi Jamie,

I understand that I will be heading to the CFD FOI training with you on Monday, and was hoping that you would be able to send me the meeting notice for this session. Also, if possible, it would be helpful to either chat beforehand, or to see the deck that will be used for this session.

Thanks,

-m

Matt Reed
Senior Director, Strategic Privacy and Training
Privacy, Compliance and Training Branch,
250 514-8870

BC logo for sig

From:	Reed, Matt FIN:EX
To:	Campbell, Fred F PSA:EX
Cc:	Arslan, Alan FIN:EX; Begley, Rhianna FIN:EX
Subject:	IM117 stats
Date:	Thursday, July 20, 2017 10:58:00 AM
Attachments:	image001.jpg

Hi Fred,

Just a quick question – are you able to provide a stat for the total number of people that have taken the IM117 course in total across the system? We are able to see who has taken it at a point in time, but I was wondering if you had cross-sectional data that might provide a "number of people through the course" stat that would capture those that have taken the course and then left government.

Thanks,

-m

Matt Reed

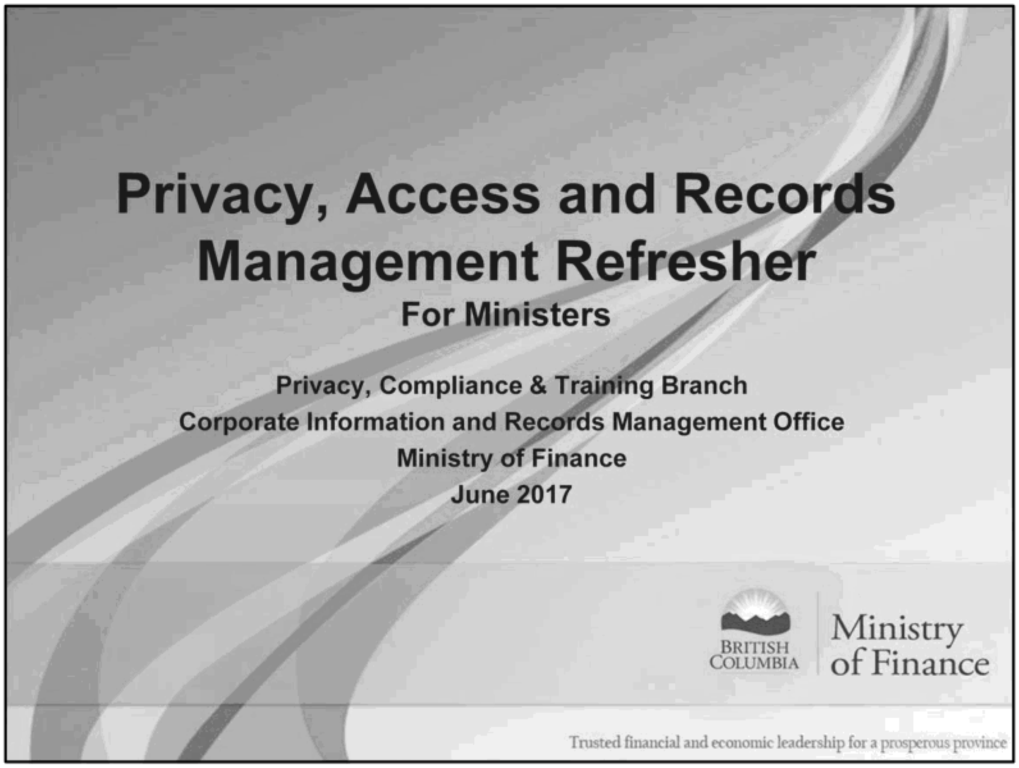
Senior Director, Strategic Privacy and Training
Privacy, Compliance and Training Branch,
Ministry of Finance
250 514-8870

BC logo for sig

All Completions for Course IM117

Count of NAME			
CORE	Active?	BUSINESS_DESCR	Total
Core	Active	Advanced Education	531
		Destination BC Corp.	78
		Energy and Mines	212
		Env Assessment Office	79
		Forests Lands Natural Res Ops	4048
		International Trade	123
		Jobs, Tourism & Skills	339
		Min Comm, Sport, Cultural Dev	269
		Min of Aboriginal Rel & Recon	222
		Min of Child & Family Dev	4322
		Min of Environment	883
		Min of Trans & Infrastructure	1480
		Ministry of Agriculture	354
		Ministry of Education	302
		Ministry of Finance	1719
		Ministry of Health	1160
		Ministry of Housing	135
		Ministry of Justice AG	3174
		Ministry of Justice SG	3130
		Ministry of Labour	239
		Natural Gas Development	84
		Office of the Premier	87
		Product Services	327
		Public Service Agency	457
		Sm Bus and Red Tape Reduction	144
		Social Development & Innov	1963
		Teachers Act Special Account	51
		Tech, Innov & Citizens' Serv	1128
	Terminated	Advanced Education	25
		Destination BC Corp.	2
		Energy and Mines	10
		Forests Lands Natural Res Ops	103
		International Trade	5
		Jobs, Tourism & Skills	23
		Min Comm, Sport, Cultural Dev	15
		Min of Aboriginal Rel & Recon	3
		Min of Child & Family Dev	199
		Min of Environment	59
		Min of Healthy Living & Sport	2
		Min of Trans & Infrastructure	81
		Ministry of Agriculture	31
		Ministry of Education	14
		Ministry of Finance	55

	Terminated	Ministry of Health	31
		Ministry of Housing	6
		Ministry of Justice AG	145
		Ministry of Justice SG	237
		Ministry of Labour	7
		Natural Gas Development	3
		Office of the Premier	8
		Product Services	16
		Public Service Agency	18
		Sm Bus and Red Tape Reduction	6
		Social Development & Innov	120
		Teachers Act Special Account	1
		Tech, Innov & Citizens' Serv	49
Core Total			**28314**
Non-Core	**Active**	BC Pension Corp	5
		BC Rep for Children & Youth	3
		Community Living BC	9
		Elections BC	1
		Office of the Auditor General	12
		Office of the Ombudsperson	8
		Royal BC Museum	1
	Terminated	BC Pension Corp	3
		BC Safety Authority	1
		Broadmead Care Society	6
		Community Living BC	10
		Environm'l Bds & Forest Comm's	1
		Legislative Assembly	8
		OBL Continuing Care Society	7
		Office of Info & Priv Comm	2
		Office of the Auditor General	1
		Office of the Ombudsperson	1
		Provincial Capital Commission	1
		Royal BC Museum	3
Non-Core Total			**83**
Grand Total			**28397**



Privacy, Access and Records Management Refresher

For Ministers

Privacy, Compliance & Training Branch
Corporate Information and Records Management Office
Ministry of Finance
June 2017

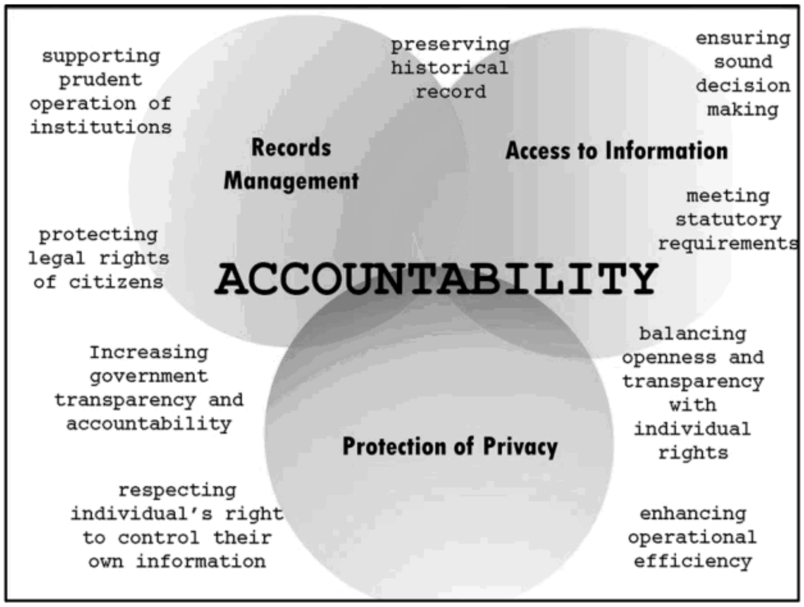
British Columbia | Ministry of Finance

Trusted financial and economic leadership for a prosperous province

- [personal introduction]

- I plan to share an overview of information management practices and training related to records management, Freedom of Information and Proactive Disclosure.

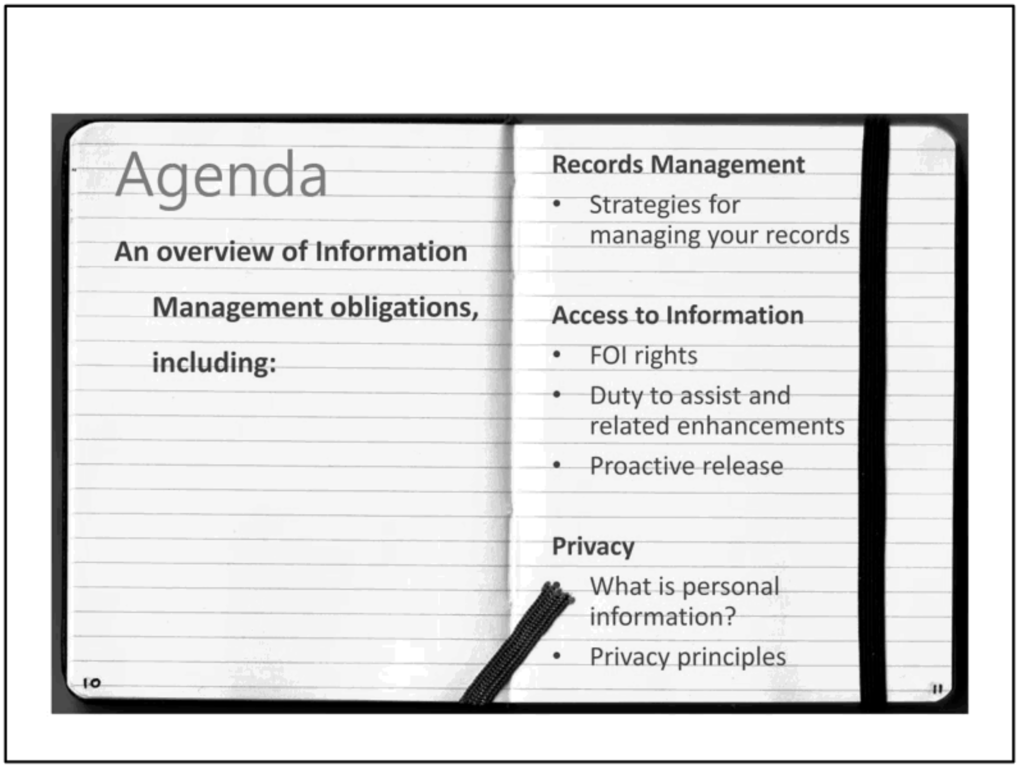
- The content and issues that we will be covering complements training that your Minister's Office staff have received – along with key contacts in each of your Deputy Ministers' Offices.


supporting prudent operation of institutions
preserving historical record
ensuring sound decision making
Records Management
Access to Information
meeting statutory requirements
protecting legal rights of citizens
ACCOUNTABILITY
balancing openness and transparency with individual rights
Increasing government transparency and accountability
Protection of Privacy
respecting individual's right to control their own information
enhancing operational efficiency

- As Ministers, you hold a number of responsibilities specific to information management.

- Generally, these are codified in legislation including the *Freedom of Information and Protection of Privacy Act* (or FOIPPA) and the *Information Management Act* (the IMA)
- These responsibilities fall into three general areas:
  - Records Management which is primarily governed by the IMA; and
  - Access to Information and Privacy which falls under FOIPPA.

- Collectively, these three disciplines drive the outcomes we see here – and which British Columbians expect:
  - supporting prudent operation of institutions
  - preserving our historical record
  - ensuring sound decision making
  - balancing openness and transparency with individual rights
  - enhancing operational efficiency
  - respecting individual's right to control their own information
  - Increasing government transparency and accountability
  - protecting the legal rights of citizens; and,
  - meeting other statutory requirements



Agenda

An overview of Information Management obligations, including:

Records Management

- Strategies for managing your records

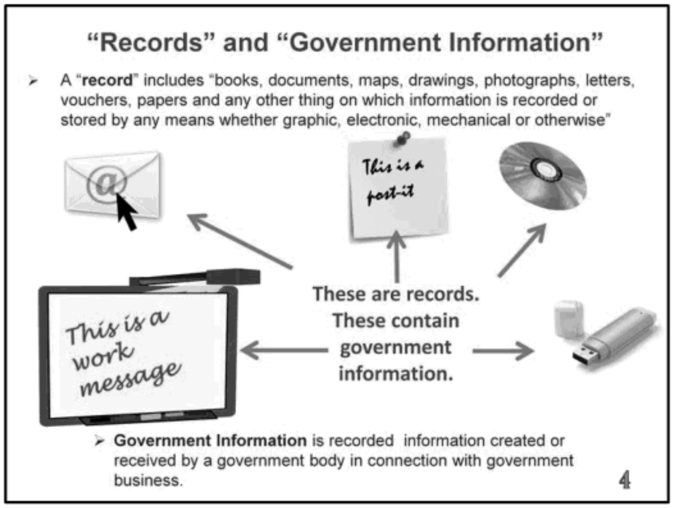
Access to Information

- FOI rights
- Duty to assist and related enhancements
- Proactive release

Privacy

- What is personal information?
- Privacy principles

- Today’s training will focus on key areas of responsibility and newly implemented process improvements, as they relate to your respective offices. We’ll touch on records management requirements, access to information including FOI rights, duty to assist, a number of process and policy enhancements, a new approach to proactive releases, as well as key privacy provisions.



“Records” and “Government Information”

- A “**record**” includes “books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by any means whether graphic, electronic, mechanical or otherwise”

This is a post-it
This is a work message

These are records. These contain government information.

- **Government Information** is recorded information created or received by a government body in connection with government business.

4

- So now, we can jump into our actual content and start getting **refreshed** on information management.

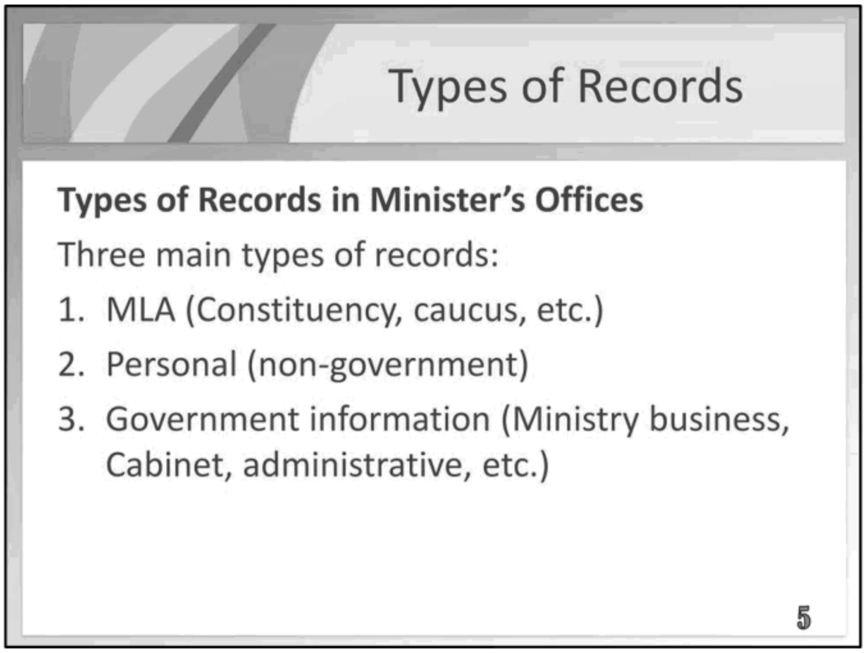
- Most of what we need to know in the area of information management focuses around the concepts of a “record” and “government information”, so it is important that we share a common understanding of these terms.

- A "record" is defined in legislation to include: books, documents, maps, drawings, e-mails, and any other places where you have put pen to paper, or typed something into a computer program. This definition is broad enough to include less obvious things like post-it notes stuck to your computer, text messages, and even Lync messages. So for the purposes of access to information or the protection of privacy, it’s this concept that you should keep in mind.

- Government Information is defined in the IMA as information created or received by a government body in connection with government business. When you’re thinking about records management, this is the concept to bear in mind.

- These two terms — “record” and “government information” are sometimes used interchangeably, and they are pretty similar.

- What’s important to understand is that in both cases it is the content and not the medium that matters.



Types of Records

Types of Records in Minister's Offices

Three main types of records:

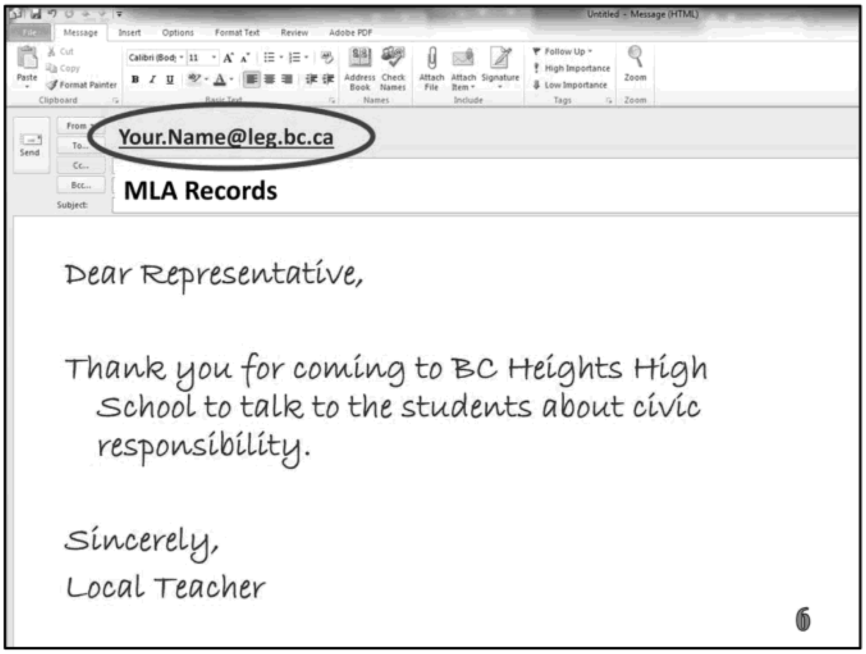
1. MLA (Constituency, caucus, etc.)
2. Personal (non-government)
3. Government information (Ministry business, Cabinet, administrative, etc.)

5

- In order to best understand records management and our access obligations we need to review the different types of record that your offices hold.

- In a Minister's Office there are three main types of records that you will deal with. I'm going to go into the details for each of these separately, but to start, in your work you likely deal with MLA, records that are strictly personal, and then those that are considered government records.

- Of course, these types of records may overlap – say, when you receive a constituent email as an MLA and then act on the email in your role as Minister. It's important that these two distinct roles are reflected as such in your record keeping practices. However, if records blend – your government records obligations will apply, including provisions under FOIPPA including responsibilities to protect privacy and provide access to these records, and your obligations under IMA to manage them appropriately.



Your.Name@leg.bc.ca

MLA Records

Dear Representative,

Thank you for coming to BC Heights High School to talk to the students about civic responsibility.

Sincerely,
Local Teacher

6

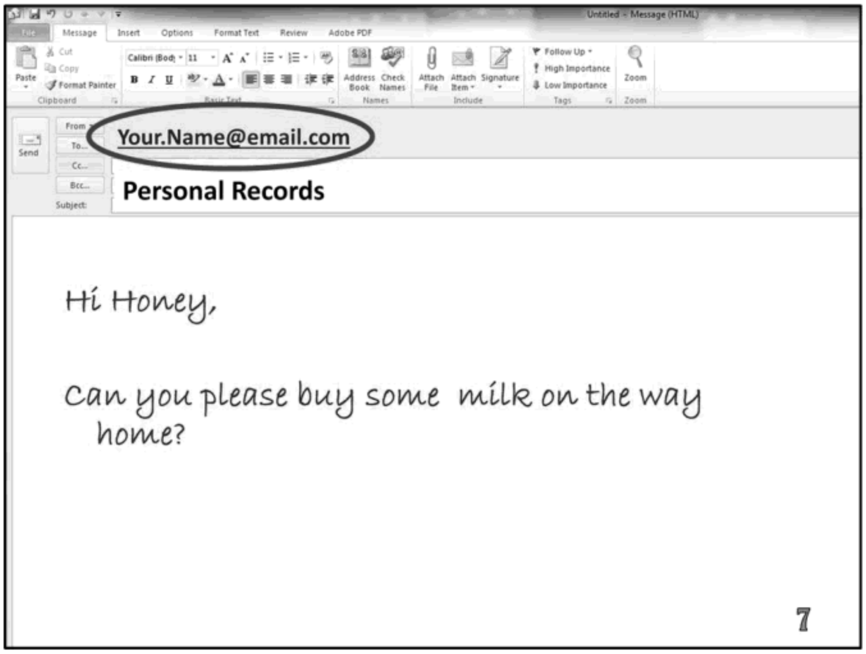
- MLA records are records created, accumulated or used by you acting in your MLA capacity. MLA records can include communications, speeches and meeting records with constituents about MLA business, Caucus committee meetings or records produced for Committees of the Legislative Assembly.

- Considering the purpose for the communication can support you in determining which type of record is appropriate. For instance, when a constituent asks a Minister to support them with an issue that is outside of the Ministerial portfolio, this would be an MLA record. If the question is within the Ministerial portfolio or the Minister moves from an advocacy role to that of an official decision making role, this same original record should be viewed as government information. You should also consider how the materials are received, for example, whether it was received to your legislative email account.

- Use of letterhead, titles and salutations in correspondence should also be considered to ensure that the record is being appropriately actioned in your capacity as either an MLA or Minister.

- This means that this thank you note we see here from the School District would be an MLA record. And due to the material's content and distribution through the dedicated leg.bc.ca email account, it would not be covered by the Information Management Act or FOIPPA.

- Finally, care should also be exercised to ensure that MLA records are not inappropriately distributed through the government email system as again they may become subject to FOIPPA's specific privacy and access provisions.



Your.Name@email.com

Personal Records

Hi Honey,

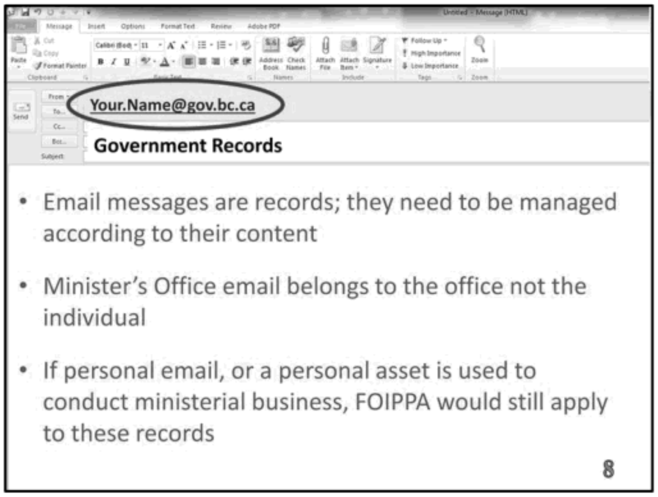
Can you please buy some milk on the way home?

- Personal records are records that are, as the name suggests, personal in nature. They relate to your private life or personal interests and are not received or created as part of your daily ministry or constituent business activities. Examples would include personal invitations, communications with family or friends (on non-government business), etc. These records, similarly **are not** covered by records management rules or privacy and access legislation, so we will again not linger on this type of record either, except to say that these records must be maintained separately from other records as much as possible.

- I would also like to stress that it is not the medium, the device or the format that dictates that something is personal, it is the **content** and **context**. For example, we understand that you can't restrict an individual from sending a work-related email to your personal account. It's important that we are clear that email, or any other work-related records produced on personal email or personal devices **are not** considered personal records, those are considered government records.

- Further, personal email accounts should never be used to carry out government business, except in extenuating circumstances. When it is used, there are rules you need to follow. This includes copying emails to your government email address, deleting the information from your personal account as soon as you can, and ensuring you have shared the least amount of sensitive information that is necessary in the circumstance.

- For example, a Minister may receive an unrequested email to their personal account that relates to their Cabinet mandate. The appropriate response would be to forward the material to their gov.bc.ca account, and manage the now-government email as appropriate according to government records schedules.



Your.Name@gov.bc.ca

Government Records

- Email messages are records; they need to be managed according to their content
- Minister's Office email belongs to the office not the individual
- If personal email, or a personal asset is used to conduct ministerial business, FOIPPA would still apply to these records

8

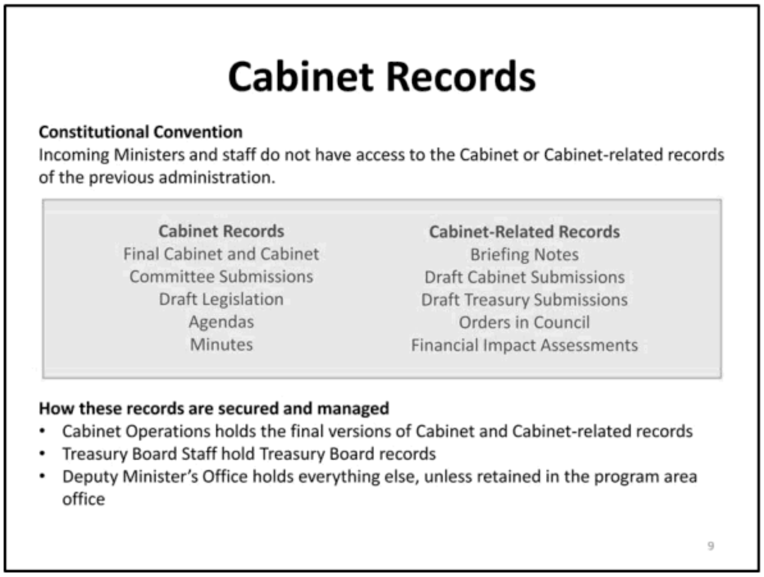
- What that leaves us with, after we remove personal and MLA records from the conversation is **"Government records",** which is essentially everything else.

- **Government** records, **including all those records that are produced in a Ministerial Office**, are covered by the IMA's records management requirements and FOIPPA's access and privacy requirements.

- As new Ministers, you may have brought with you, transition materials related to your new role. To be clear, any records brought in and used during the course of your work as a Minister, or stored on a government record keeping system are considered government information. You should consider carefully what previously created materials you would like to subject to government's legislative responsibilities.

- It is also important to point out that government records belong to your ministry and not to the person who sent or received them.

- Lastly, it is important that I emphasize that triple deleting email is never permitted.



Cabinet Records

Constitutional Convention
Incoming Ministers and staff do not have access to the Cabinet or Cabinet-related records of the previous administration.

Cabinet Records
Final Cabinet and Cabinet Committee Submissions
Draft Legislation
Agendas
Minutes

Cabinet-Related Records
Briefing Notes
Draft Cabinet Submissions
Draft Treasury Submissions
Orders in Council
Financial Impact Assessments

How these records are secured and managed

- Cabinet Operations holds the final versions of Cabinet and Cabinet-related records
- Treasury Board Staff hold Treasury Board records
- Deputy Minister's Office holds everything else, unless retained in the program area office

- Given the recent election, I want to call your attention to a specific protocol that applies during and after the transition to all new administrations. This protocol applies to Cabinet records and Cabinet-related records. While these types of records are highly confidential and are always protected, additional rules around how they are secured and managed come into play after an election.

- **Cabinet Records** are those that have been prepared for submission to or circulated for consideration by Cabinet or a Cabinet Committee. Cabinet records may include agendas, minutes, final versions of Cabinet and Cabinet Committee submissions, decision letters of Cabinet and its committees, staff analysis, draft legislation, regulations and Orders in Council circulated for consideration by Cabinet, presentation decks and papers.

- **Cabinet-Related Records** are records held by public bodies that are created or received by the public body, which may reveal the substance of deliberations of Cabinet or a Cabinet Committee. This may include: correspondence including email correspondence, briefing notes, drafts of Cabinet or Treasury Board submissions, draft regulations and Orders in Council, financial impact assessments, and memoranda regarding confidential work for the consideration of Cabinet.

- **Constitutional convention -** Established Constitutional convention requires that all records which may reveal the substance of deliberations of a prior Cabinet or its committees are treated as privileged information of that government. This means an incoming administration (i.e., incoming Ministers and political staff) does not have access to these documents without the express consent of the outgoing administration (during/after transition, by approval of the DM responsible and the outgoing Premier or delegate)

- So what happens to these records? Cabinet Operations or Treasury Board Staff hold the final versions of Cabinet Records and Cabinet-Related Records. Where the Cabinet record or Cabinet-related record is an integral part of ministry business files, a copy should be retained in the relevant operational/business unit files. These copies of Cabinet confidential records must be kept secure to ensure no unauthorized access, and must only be accessed by members of the public service, and on a need-to-know

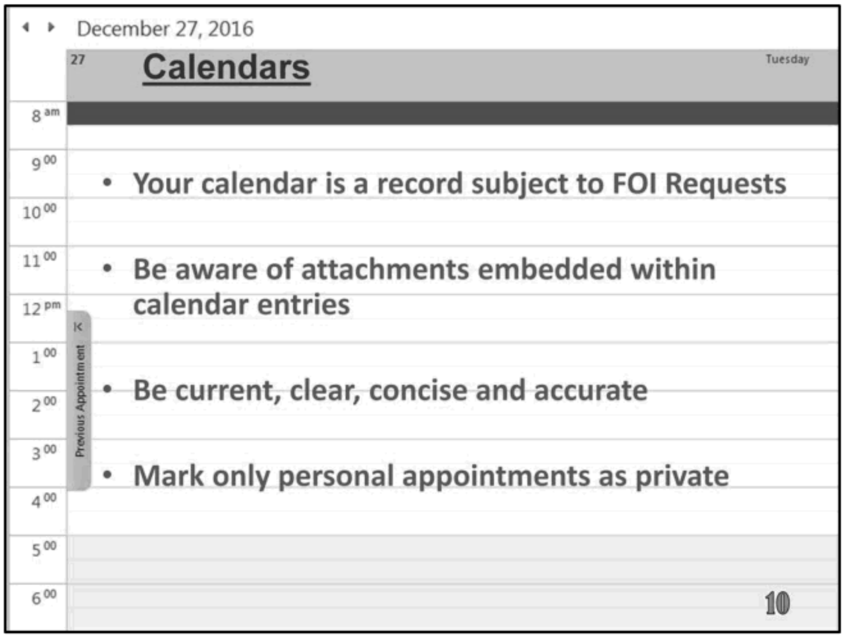
- In responding to requests of a new government, the proper procedure is for staff to paraphrase the information in the records and/or prepare new reports and submissions, rather than simply providing copies of old ones. Previous Cabinet submissions and materials used in their preparation may continue to be used as resource documents by Public Service staff preparing new submissions .

[content below for reference and to be used as needed]

- Although a new administration is precluded from viewing the records of a previous administration, it is generally permissible for a new administration to obtain information about decisions made by a previous administration, particularly where the information is necessary to ensure that government business will be carried out effectively.

- After a change in administration occurs, in providing advice to the new Executive Council, where the continuity of administration requires reference to records prepared for previous Executive Councils, it may be appropriate to paraphrase the contents of those materials.

- However, in disclosing information about the decisions made by a prior administration, employees must take care to continue to protect information about the options presented to the Executive Council in making the decision and any information related to the opinions



Calendars

- Your calendar is a record subject to FOI Requests
- Be aware of attachments embedded within calendar entries
- Be current, clear, concise and accurate
- Mark only personal appointments as private

10

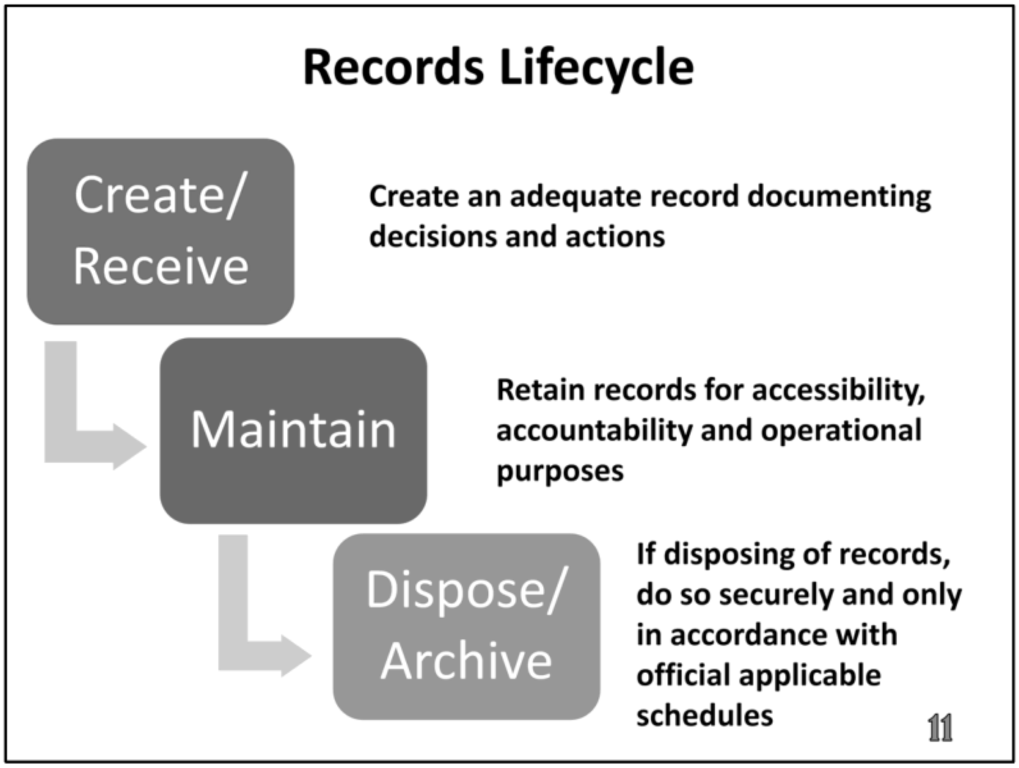
- The second records example I wanted to highlight is Outlook calendars.

- A Ministerial Directive under FOIPPA requires the monthly disclosure of calendars of Minister, Deputy Ministers, Associate Deputies, and Ministers of State. To facilitate consistency and ensure security in making these disclosures, certain practices need to be maintained within your offices:

- Your calendar will have to be:
  - Updated as changes occur;
  - Absent of meetings that were not attended or didn't happen;
  - Include current attendees lists; and
  - Ensure that only personal appointments are marked as private.

- I imagine many of you have staff that support you with this, and specialized information management training is available to them, which will offer specific guidance on calendar management practices.

- Now, we are going to switch gears from talking about these specific records you regularly deal with to a concept that applies to all of your records, we will speak to the records lifecycle.



Records Lifecycle

Create/ Receive

Create an adequate record documenting decisions and actions

Maintain

Retain records for accessibility, accountability and operational purposes

Dispose/ Archive

If disposing of records, do so securely and only in accordance with official applicable schedules

11

- As illustrated in the slide, the traditional lifecycle of a record is pretty simple – a record is created, it is maintained, and then the record *is either kept or disposed of.* For some, this lifecycle lasts but a few hours, and for others, the records are never disposed of, but rather are archived for historical purposes. Thinking about a record's lifecycle helps us to think through our obligations around creating, maintaining or disposing of a record.

- In the example of a Federal Provincial Territorial meeting, we can expect the administrative process to generate a wide range of supporting information including: a Federal government invitation to meet, Minister's briefing notes, Cabinet Submissions (e.g Negotiating Mandate), IGRS briefing binders, agendas, speeches, meeting minutes, post-event Briefing Notes, Treasury Board Submissions for matching provincial funding, Program announcements (Speeches and News Releases), Funding Agreements with third parties or Requests for Proposals, Contract awards, Project Management Progress Reports, Federal-Provincial Funding Contributions, Final Project Sign-offs, Provincial Audits and Federal Audits.

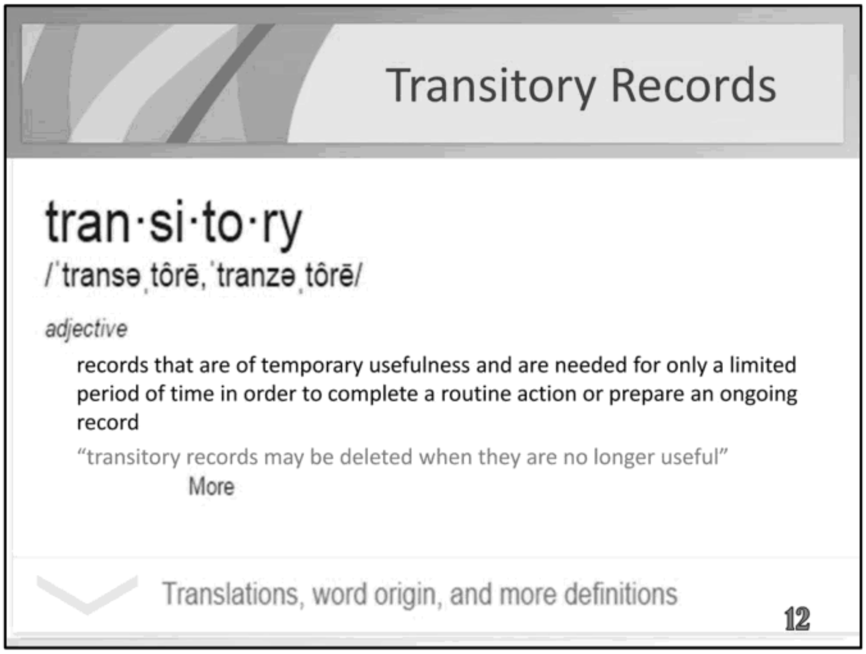
- Each of the records just referenced should be managed in the context of the lifecycle identified here.

- **[CREATE**]: As you work on a project, you naturally create and receive government information, such as a project charter, meeting agendas and minutes, email correspondence, and project plans and reports. To have an adequate record of the project, you need to have documentation of significant project activities, decisions and results.

- **[MAINTAIN]:** As you create and receive government information, it is important to ensure that you maintain the information so that it is available to those who need it and is kept for the required length of time. You should always retain information that details significant activities of your unit, as well as changes to existing programs or the establishment of new ones.

- Management of ministerial records are typically overseen by your Deputy Ministers' Offices, Cabinet Operations, GCPE and the Ministry of Finance's Ministers Office Support Services Unit in their capacity as **Offices of Primary Responsibility – or OPR**. At the Minister's discretion, some records may be retained within the Minister's Office, and in this instance the Minister's Office becomes the OPR for these records. The Minister's Office will be responsible for managing these records in accordance with applicable retention schedules.

- **[ARCHIVE/DISPOSE]:** Some records have historical value and should thus be maintained indefinitely, or archived in the government archives at the Royal BC Museum, or, in future, in a digital archive. Information schedules provide timetables which tell us how long different types of information is needed and when the information may be disposed of or sent to the government archives. This is important because you cannot dispose of information unless there is an information schedule to authorize it. Some information schedules identify information that must never be disposed of, but rather must be maintained until it is ready to be transferred to the government archives. Transitory information has its own information schedule that allows you to dispose of the information when it is no longer useful. We will speaking about transitory information in the next slide.



Transitory Records

tran·si·to·ry

/ˈtransəˌtôrē, ˈtranzəˌtôrē/

adjective

records that are of temporary usefulness and are needed for only a limited period of time in order to complete a routine action or prepare an ongoing record

"transitory records may be deleted when they are no longer useful"

More

Translations, word origin, and more definitions

12

- Good records management dictates that we need to retain records of value and dispose of records of temporary value, once they are no longer useful.

- This is best practice in information management and is essential for appropriately handling the escalating volume of records that government has in its control.

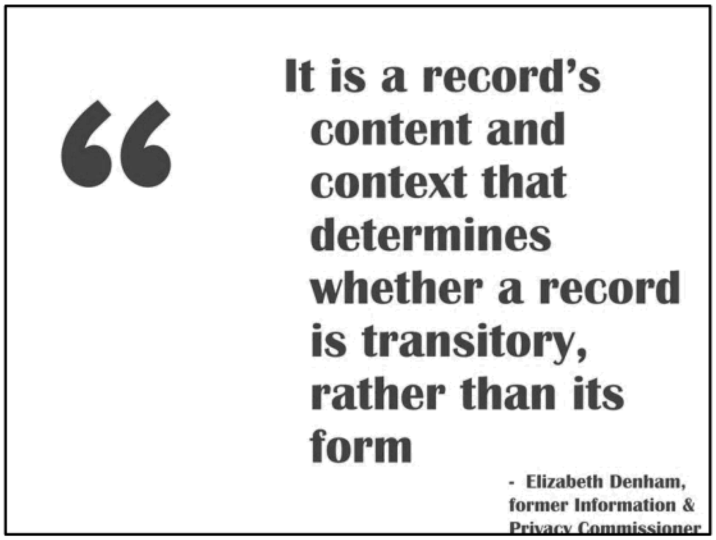
- David Loukidelis' December 2015 report reinforces this best practice and he noted that the province receives 284 million emails annually.

- Mr. Loukidelis likens good records management practices to that of good household management, saying that retention of all electronic records is an inappropriate practice akin to hoarding, and should be avoided at all cost.

- Information schedules, approved under the Document Disposal Act, or by Chief Records Officer under the Information Management Act , define criteria as to whether a record is an official government record which **must** be retained or is a transitory government record which **may** be disposed of. Even transitory information has its own information schedule that allows you to dispose of information when it is no longer useful.

- Simply put:
  - **Official** government records **must** be retained within the Minister's Office or an OPR such as the Deputy Minister's Office; and,
  - **Transitory** government records may be disposed of – following an assessment that they are appropriately categorized as transitory.

- If a record does not obviously present as an official government record – we need to determine whether or not that record is transitory, so let's do a deeper dive on this concept.



“ It is a record’s content and context that determines whether a record is transitory, rather than its form

- Elizabeth Denham, former Information & Privacy Commissioner

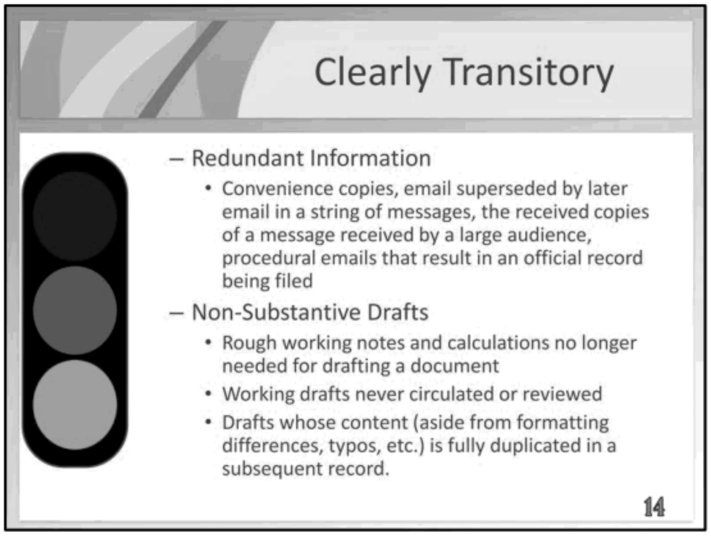
- As previously noted, a record’s value is related to its content and context rather than its form.

- Email, text messages, Lync and Blackberry Instant Messenger are simply communication mechanisms, which may include both official and transitory records. And, their content should be treated as such.

- In terms of a definition - Transitory records are those of **temporary** usefulness and are needed for only a limited period of time in order to complete a routine action or prepare an ongoing record.
  - They are not required to **document decisions** and actions or to support ongoing government business.
  - They are not **regularly filed** as standard records
  - They are not required to meet statutory requirements, **or**
  - They are **redundant,** extra copies

- It’s important to note that all transitory records are subject to FOI requests. Even though transitory information may be disposed of when it is no longer required, it is unlawful to delete or destroy any transitory record that is the subject of a current FOI request.

- And because of that, if you receive an FOI request, any transitory records that exist at that time, may be responsive to that FOI request. In other words, if you have an FOI request, you cannot delete the responsive transitory records. You may have been able to delete them previously, but if you kept them, they are responsive to the request and you must provide them.



Clearly Transitory

- Redundant Information
  - Convenience copies, email superseded by later email in a string of messages, the received copies of a message received by a large audience, procedural emails that result in an official record being filed
- Non-Substantive Drafts
  - Rough working notes and calculations no longer needed for drafting a document
  - Working drafts never circulated or reviewed
  - Drafts whose content (aside from formatting differences, typos, etc.) is fully duplicated in a subsequent record.

14

- So, how does your office determine if something is transitory? I am going to walk you through some examples to try to illustrate the decision making process in the context of the records that are produced in a Ministerial office.

- Duplicated information is a good example of what can be transitory. Imagine a typical email conversation that goes something like this:

  - Email from another office: “Have you considered the proposal that we talked about?”
  - You respond: “Yes, I like the idea, could you please send it in writing?”
  - Other office: “Here it is. Tell me if you need any changes.”
  - You: “Your proposal (attached) is approved.”

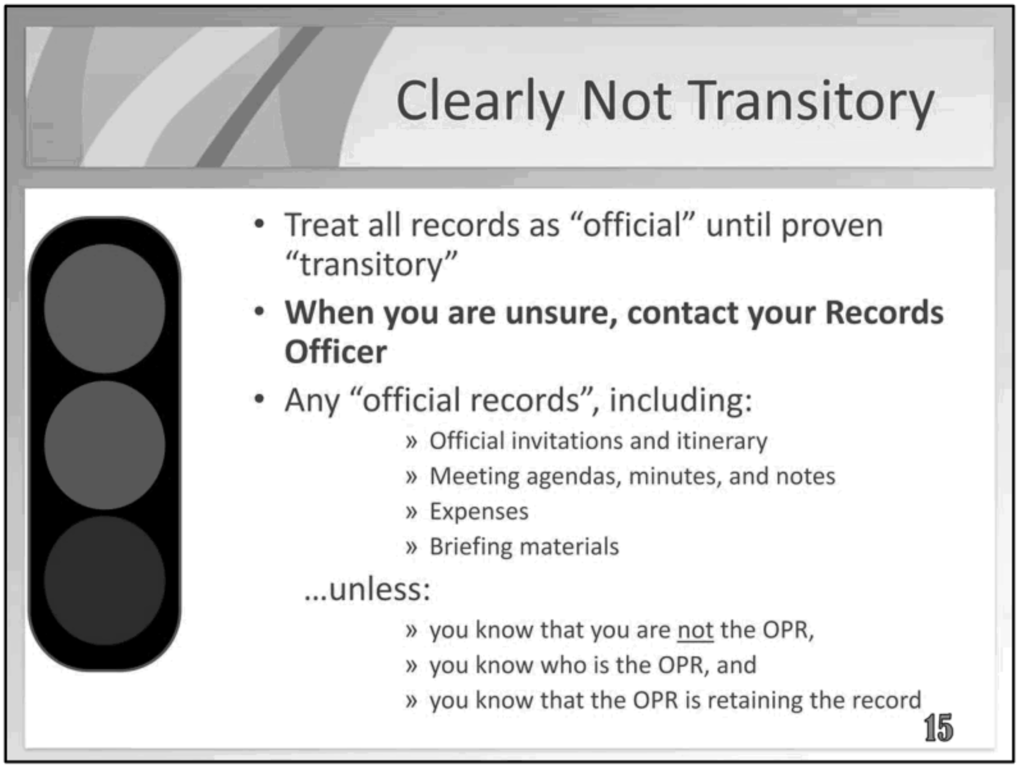
- In this simple example, you will end up with four emails, two sent and two received. Each of which contains the previous emails. In this example, you can feel confident deleting the first three emails if you are retaining the fourth, as the fourth contains the entire chain, as well as the decision.

- As another example, if you make a handwritten note while you are listening to a voicemail, and then copy your note into an email, you can delete the voicemail, and dispose of your handwritten note as transitory.

- Non-substantive prior drafts, which can include those that contain changes to elements like the formatting and margins, or corrections to grammatical errors are also transitory. Drafts that were never circulated or reviewed are also considered non-substantive.

- Even though transitory information may be disposed of when it is no longer required, it is unlawful to delete or destroy any transitory record that is the subject of a current FOI request.

- Transitory records also must not be deleted where they may be relevant to a current or an expected future legal action.



Clearly Not Transitory

- Treat all records as “official” until proven “transitory”
- **When you are unsure, contact your Records Officer**
- Any “official records”, including:
  - » Official invitations and itinerary
  - » Meeting agendas, minutes, and notes
  - » Expenses
  - » Briefing materials

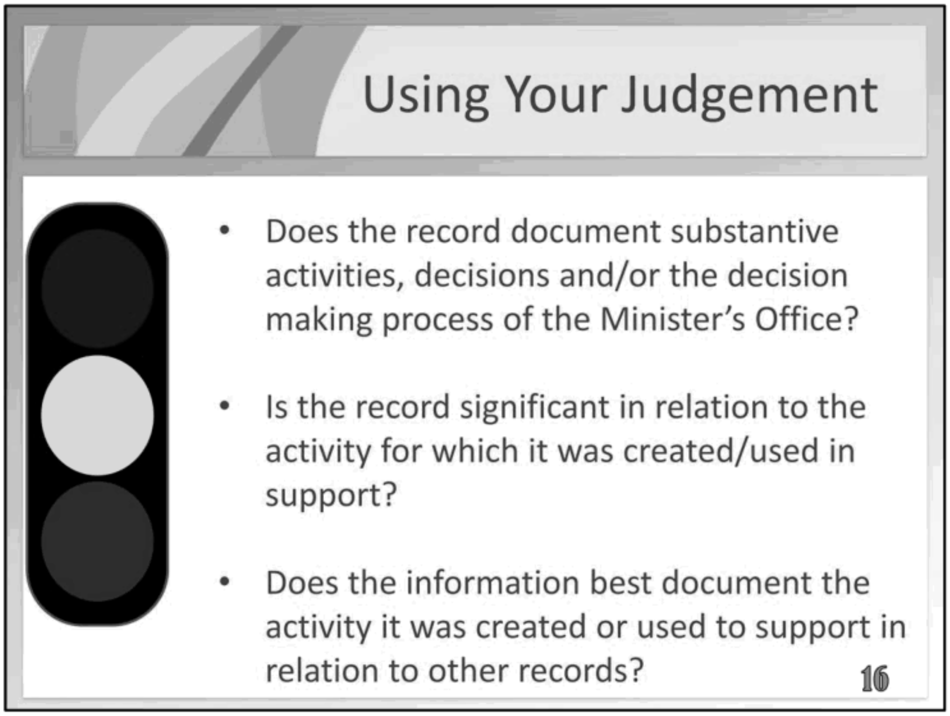
…unless:

- » you know that you are not the OPR,
- » you know who is the OPR, and
- » you know that the OPR is retaining the record

15

- On the other end of the spectrum, there are those records that are clearly **not** transitory.

- Information that is clearly not transitory would include incoming public correspondence, meeting minutes, and case files. You may, however, have copies of information such as meeting minutes that are transitory, provided that:
  - You know that you are not the Office of Primary Responsibility or OPR, and
  - Your office has no need to file your copies for its own business use.



Using Your Judgement

- Does the record document substantive activities, decisions and/or the decision making process of the Minister's Office?
- Is the record significant in relation to the activity for which it was created/used in support?
- Does the information best document the activity it was created or used to support in relation to other records?

16

- When faced with information that is neither clearly transitory or official, you will need to ask yourself these questions:
  - Does the information document an important activity, or decision?
  - To what extent is this already documented somewhere else?
  - Is the information important in relation to the activity for which it was created or which it was used to support?
  - In relation to other information, does this information best document the function or activity for which it was created or which it was used to support?
- If you are unsure as to whether something is transitory or not, you can contact your Records Officer in the Government Records Service (GRS) for assistance.

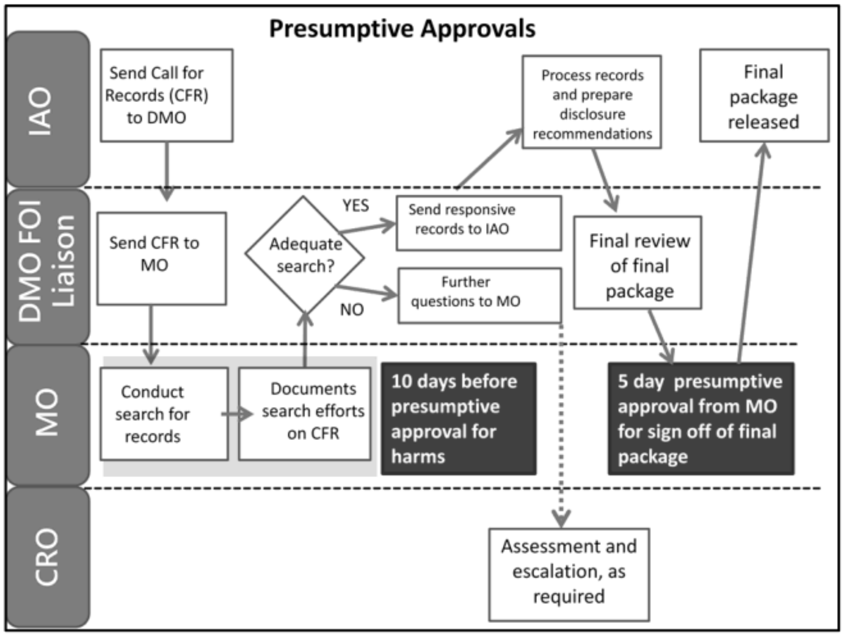
Freedom of Information

- Government’s commitment to improve the timelines, quality and service orientation of its FOI processes has been implemented through a number of critical reforms

- Many of these reforms build upon, and exceed, the recommendations issued by David Loukidelis. These include:

- New training expanding government’s ‘Duty to Assist’ applicants.
    - This duty requires that staff make every reasonable effort to assist applicants and to respond to each applicant openly, accurately and completely in a timely way. This means steering clear of narrow interpretations, it’s about getting to the underlying intent of a request and understanding the request from the applicant’s point of view.
    - Ultimately, we need to interpret requests in a manner that a “fair and rational person would expect”.
    - Accommodation may require a range of approaches, including:
        - engagement with the applicant to clarify their request;
        - provision of relevant records that fall outside the scope of the request - such as date ranges;
        - development of new materials to quickly address the request; and,
        - timely referral to other ministries, which are believed to hold responsive records.

- We are also working to drive a culture change for those continuing to assess whether a record ‘Can’ be withheld rather than ‘Should’ a record be withheld.



Presumptive Approvals

IAO

DMO FOI Liaison

MO

CRO

Send Call for Records (CFR) to DMO

Send CFR to MO

Conduct search for records

Documents search efforts on CFR

Adequate search?

YES

Send responsive records to IAO

NO

Further questions to MO

Process records and prepare disclosure recommendations

10 days before presumptive approval for harms

Final review of final package

5 day presumptive approval from MO for sign off of final package

Final package released

Assessment and escalation, as required

- Here we have an overview of the new FOI process specific to Minister's Offices – which includes several new process enhancements.

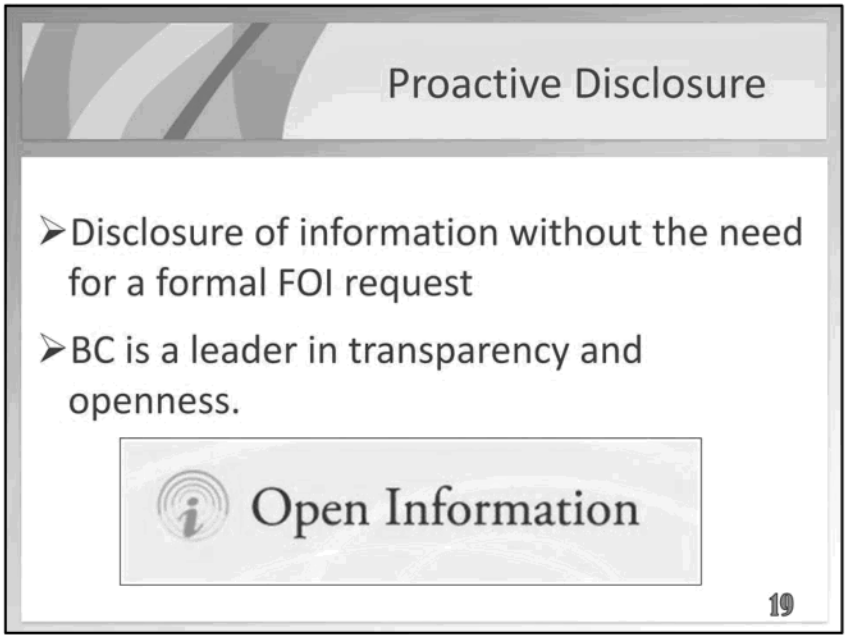
- With your DMO's support, we have established new career public servant FOI liaisons in each Deputy Ministers Office responsible for overseeing, documenting and reporting on records searches within Minister's Offices.

- Presumptive Approval processes have been recently introduced, which includes:
  - 10 day window for Ministers' Offices to identify potential harms; and,
  - 5 day window for Ministers' Offices to approve the final red line versions.

- These are critical steps for ensuring that we adhere to our legislated timelines.
- - And-

- We have established a new Escalation Process for Ministers Offices, which requires the Deputy Minister's Office FOI Liaison to identify to the Chief Records Officer all instances where insufficient records searches are identified or where No Responsive Records are reported when they are believed to exist. And - the CRO may in turn refer the matter to Minister de Jong – the minister responsible for FOI - for further resolution.

- Your staff and the Deputy Ministers' FOI Liaisons have been trained on the new processes and expectations. In the event that additional supports or training are required CIRMO staff are available to assist with the transition.



Proactive Disclosure

- Disclosure of information without the need for a formal FOI request
- BC is a leader in transparency and openness.

Open Information

19

- Proactive disclosure is the disclosure of information without the need for a formal FOI request. You may have also heard this referred to as “routine release”.

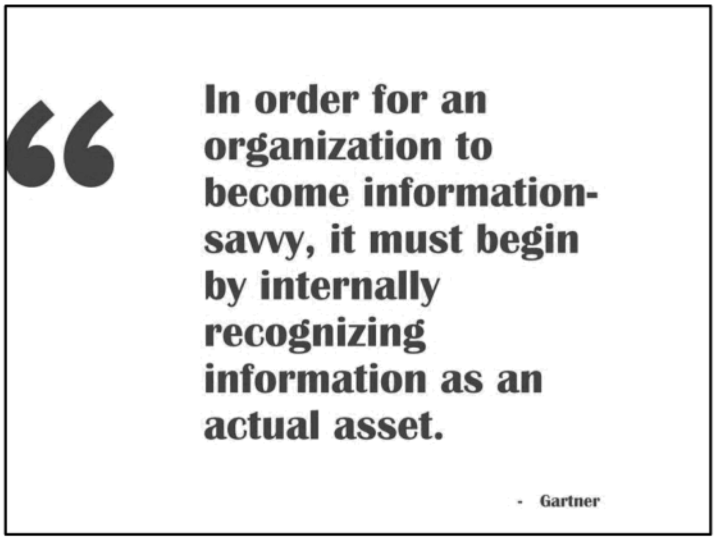
- There are lots of examples of proactively disclosed information. For one, BC’s Open Information site, which contains thousands of proactively disclosed records. There is also the BC Data catalogue which contains thousands of high-quality datasets.

- Corporately, we currently proactively release summaries of community gaming grants, Minster’s receipted expense information, summaries of FOI requests, calendars, and summaries of directly-awarded contracts, and more.

- Several of these disclosures are made on the Open Information site, which contains thousands of proactively disclosed records. Others are made through the BC Data catalogue which contains thousands more high-quality datasets.

- FOIPPA requires all ministers to establish categories of recorded information that can be proactively disclosed.

Other disclosures are more casual – your staff might give the general public non-personal and non-sensitive information over the phone, or via a website. Not all disclosures are repeatable -- and that’s okay. Sometimes a disclosure is a one-off. Any information a ministry makes available on its website, or when citizens call a hotline or come to a service counter is a proactive disclosure. Each time we do this, we contribute to citizens receiving the information they’re interested in, more efficiently.



“ **In order for an organization to become information-savvy, it must begin by internally recognizing information as an actual asset.**

- Gartner

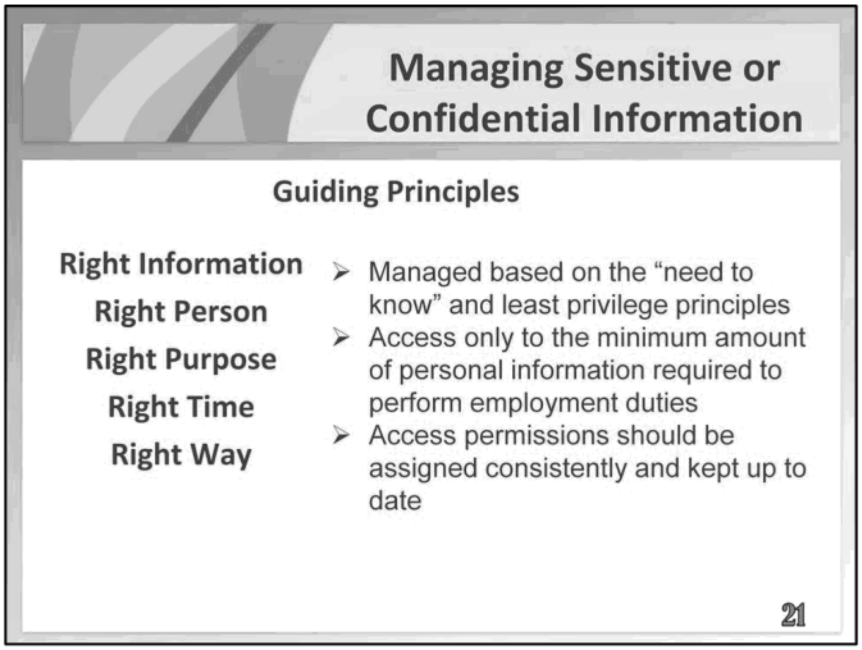
- Up until now, we have talked about openness – which is very important – but we need to ensure a balance. FOIPPA provides a balance between openness and the protection of privacy.

- In this spirit, we in the Ministry of Finance often speak of extending the culture that currently exists around protecting our financial resources to the informational resources we have in government. The measures that are in place to monitor the expenditure of dollars are extensive. We have to take that same culture and discipline and apply it to the protection of sensitive information.

- For me, this means that information is an asset and just like money, property or other more tangible government assets, we need to apply the rules and procedures to protect it.

[additional material]

- …information is not recognizable as a balance sheet asset — even though information meets all the criteria… - Douglas Laney, VP, Gartner



Managing Sensitive or Confidential Information

Guiding Principles

Right Information
Right Person
Right Purpose
Right Time
Right Way

- Managed based on the “need to know” and least privilege principles
- Access only to the minimum amount of personal information required to perform employment duties
- Access permissions should be assigned consistently and kept up to date

21

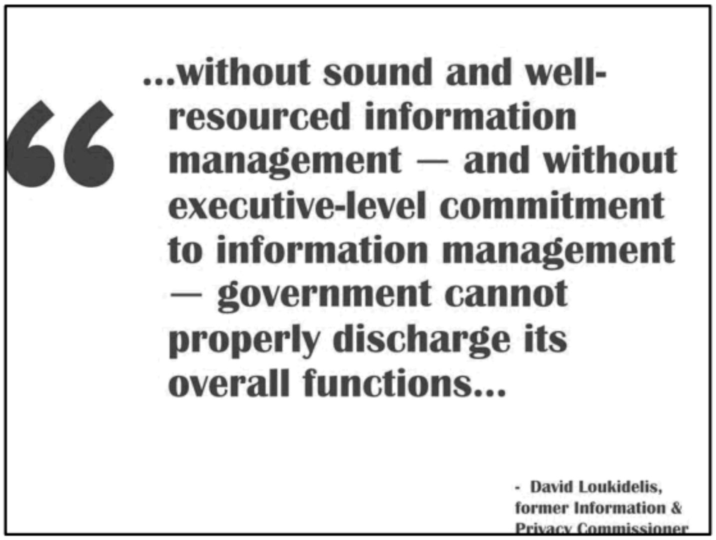
- The key to protecting privacy is to have a clear understanding of personal information.

- Personal information is defined as recorded information about an identifiable individual other than “contact information”. A citizen’s contact information is considered their business contact, when that information is used to connect with them in their business capacity. Essentially, their business card, as long as they are handing it out for business reasons.

- But everything else about the citizen, as an identifiable individual, is their personal information.

- We don’t have time to do a walk through of every provision of FOIPPA – that would take a long time. But we can remember, this very simply mantra for managing personal information or confidential information – Right Information; Right Person; Right Purpose; Right Time; and Right Way. These are the things you need to consider when you are collecting, using, and disclosing personal information.

- Some of the practices that we can pull out of this mantra would include managing information on a need to know – not a nice to know basis. Accessing, using, or disclosing the minimum amount of personal information necessary, and managing and auditing access permissions.



> **…without sound and well-resourced information management — and without executive-level commitment to information management — government cannot properly discharge its overall functions…**
>
> **- David Loukidelis, former Information & Privacy Commissioner**

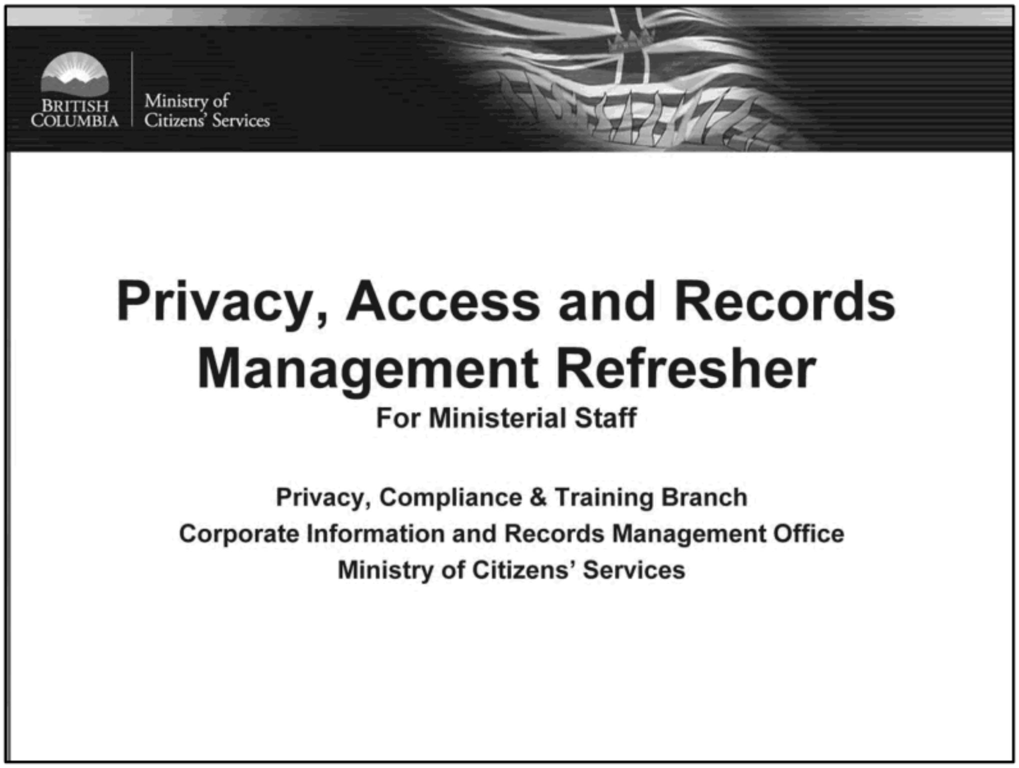
In order to summarize all of the materials we have addressed today, we need to return to the concepts of responsibility, accountability and transparency. This requires us to ensure that we have an understanding and a commitment at the most senior levels of government to the idea of managing information as an asset. With holistic information management practices, we will be able to demonstrate to the citizens of BC our commitment to accountability and transparency.

Thank you for your time and continued support for information management practices with government.

I welcome any comments or questions that you may have.

British Columbia | Ministry of Finance

British Columbia



BRITISH COLUMBIA | Ministry of Citizens' Services

Privacy, Access and Records Management Refresher

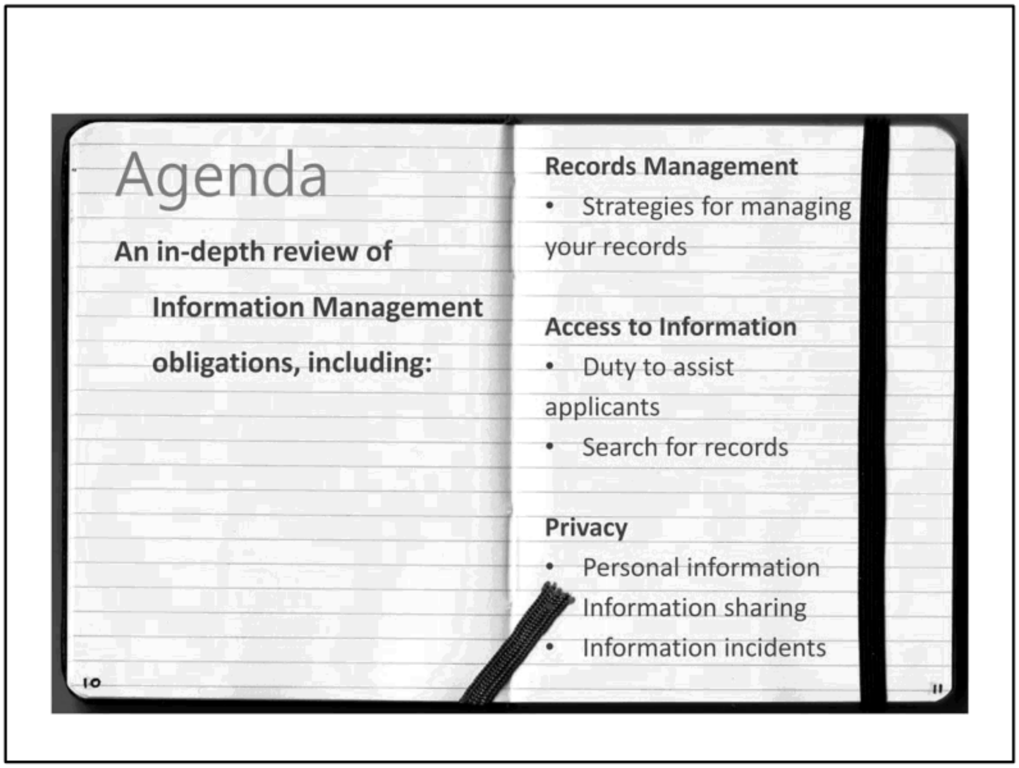
For Ministerial Staff

Privacy, Compliance & Training Branch
Corporate Information and Records Management Office
Ministry of Citizens' Services

Good morning/good afternoon.   [personal introduction].

I am here representing the Corporate Information and Records Management Office, or CIRMO for short. This is the division that is responsible for **information management** in government. CIRMO was established in December 2015 to consolidate government's critical information management functions in order to enhance government practices. CIRMO is led by the Chief Records Officer, [title and name].

As someone who works in Information Management - Privacy and FOIPPA in particular –I am very enthusiastic about this content and so my goal for the next 2 hours will be to share some of that passion with you. I know that you'll come away from today with a greater understanding of your information management obligations. But I also hope that you will gain some of my enthusiasm for information management too.



Agenda

An in-depth review of Information Management obligations, including:

Records Management

- Strategies for managing your records

Access to Information

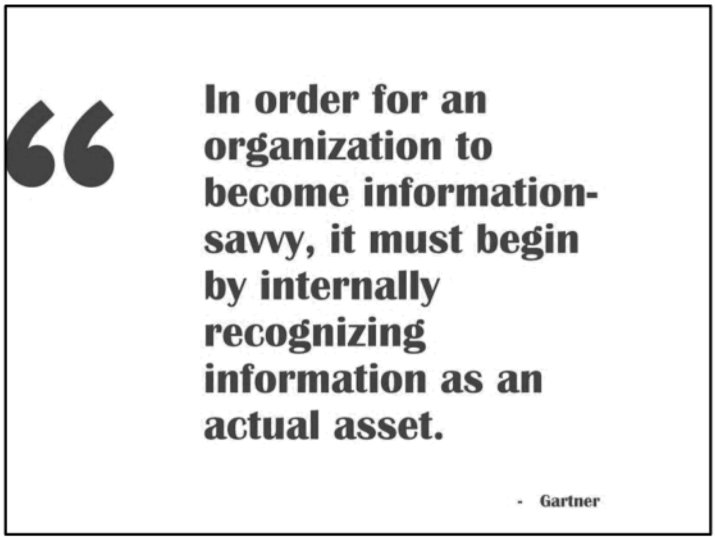
- Duty to assist applicants
- Search for records

Privacy

- Personal information
- Information sharing
- Information incidents

We are here today to get a bit of a refresher on our information management requirements and introduce new practices and controls that will improve information management practices and accountability. You have all received training on access, **or** said another way, on FOI - and you have all taken training on privacy and information sharing. However, as we all know, these are areas that have developed very quickly, given the massive increase in the volume of records we all hold. This is a result of digitization, email, and nearly unlimited electronic storage.

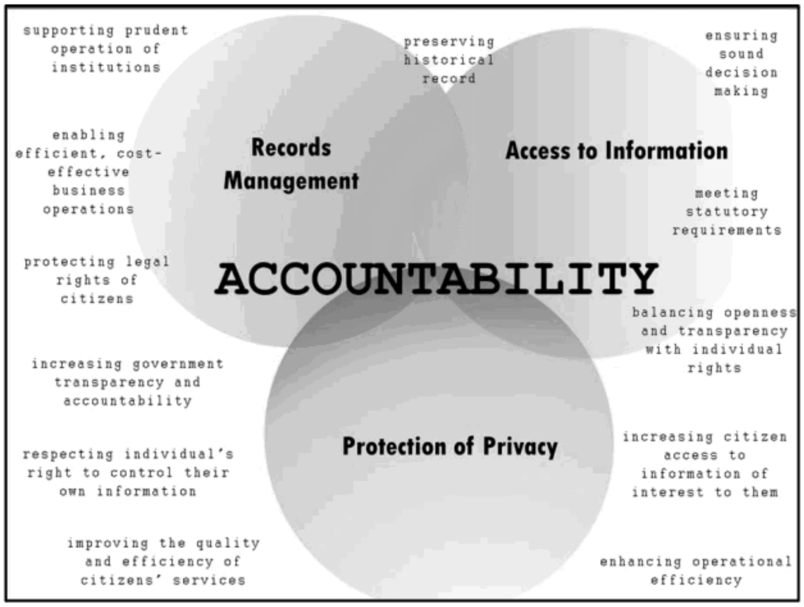
Today's training will focus on areas that have received the most attention, both from government officials, and the Information and Privacy Commissioner. We'll touch on **records management** requirements, **duty to assist** an FOI applicant and **proper search** for records, and then finish with a reminder of our **collective privacy obligations**, including what to do in the event of an information incident or **privacy breach**.



“In order for an organization to become information-savvy, it must begin by internally recognizing information as an actual asset.

- Gartner

- We in the Ministry of Citizens’ Services often speak of extending the culture that currently exists around protecting our physical or financial assets to the informational resources we have in government. The measures that are in place to monitor the expenditure of dollars, as an example, are extensive. We have to take that same culture and discipline and apply it to the protection of private information.



Records Management

Access to Information

Protection of Privacy

ACCOUNTABILITY

supporting prudent operation of institutions

preserving historical record

ensuring sound decision making

enabling efficient, cost-effective business operations

meeting statutory requirements

protecting legal rights of citizens

balancing openness and transparency with individual rights

increasing government transparency and accountability

increasing citizen access to information of interest to them

respecting individual's right to control their own information

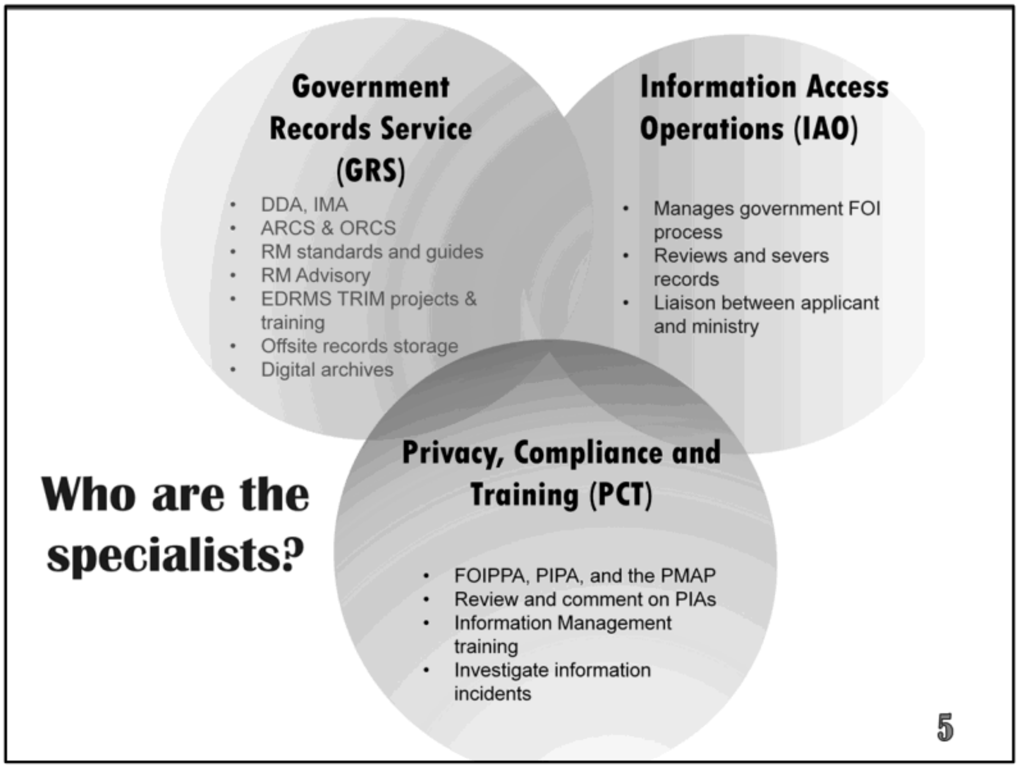
improving the quality and efficiency of citizens' services

enhancing operational efficiency

Which leads me to the foundations for today's material, or the three central areas of relevance – Records Management, Access to Information, and Protection of Privacy.

- Generally, these are codified in legislation including the *Freedom of Information and Protection of Privacy Act* (or FOIPPA) and the *Information Management Act* (the IMA)
- These responsibilities fall into three general areas:
  - Records Management which is governed by the IMA; and
  - Access to Information and Privacy which fall under FOIPPA.

- Collectively, these three disciplines drive the outcomes we see here – and which British Columbians expect:
  - supporting prudent operation of institutions
  - preserving our historical record
  - ensuring sound decision making
  - balancing openness and transparency with individual rights
  - enhancing operational efficiency
  - respecting individual's right to control their own information
  - Increasing government transparency and accountability
  - protecting the legal rights of citizens; and,
  - meeting other statutory requirements



Who are the specialists?

Government Records Service (GRS)

- DDA, IMA
- ARCS & ORCS
- RM standards and guides
- RM Advisory
- EDRMS TRIM projects & training
- Offsite records storage
- Digital archives

Information Access Operations (IAO)

- Manages government FOI process
- Reviews and severs records
- Liaison between applicant and ministry

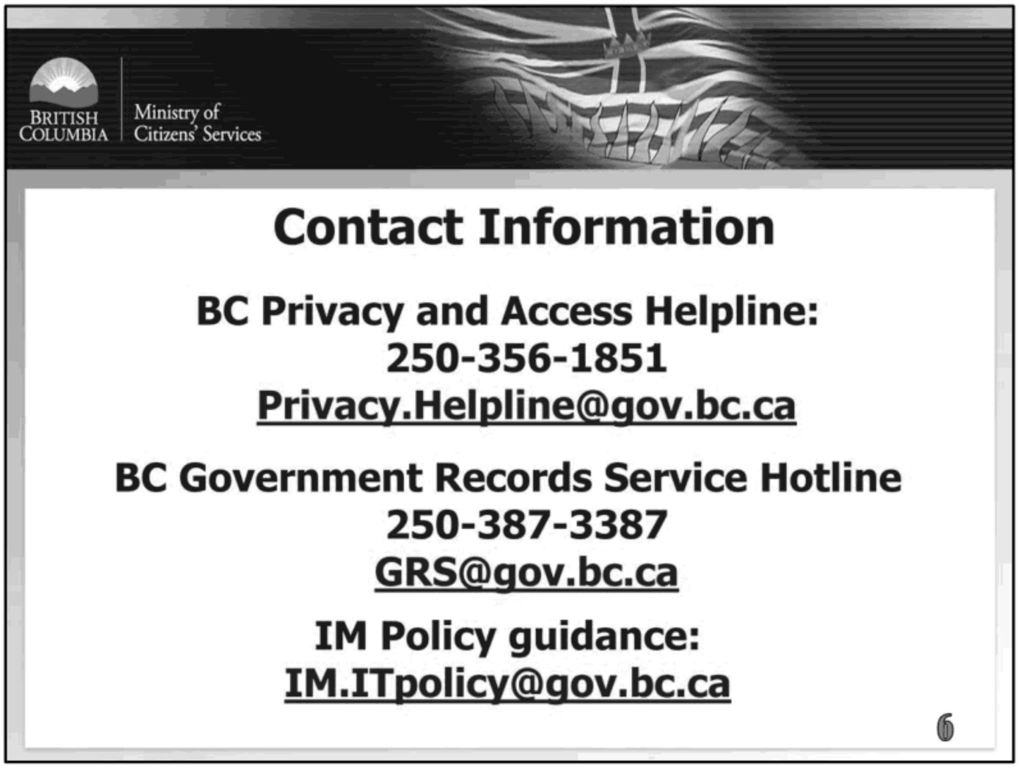
Privacy, Compliance and Training (PCT)

- FOIPPA, PIPA, and the PMAP
- Review and comment on PIAs
- Information Management training
- Investigate information incidents

Each of these three branches, all within CIRMO, provide a lot of **services** that we will **not talk about today** – but **for today**, we can boil it **down to rough terms** for the topic at hand.

So the Privacy branch supports ministries in operationalizing the privacy portions of the Freedom of Information and Protection of Privacy Act - FOIPPA for short. Information Access Operations, or IAO, manages the Access to Information, or FOI requirements of FOIPPA. And Government Records Service, or GRS, supports ministries in operationalizing the Information Management Act.

Additionally, CIRMO also houses a strategic policy and legislation shop, which is responsible for setting and advising on corporate IM policy such as Core Policy and Appropriate Use Policy, which we will touch on today.



BRITISH COLUMBIA | Ministry of Citizens' Services

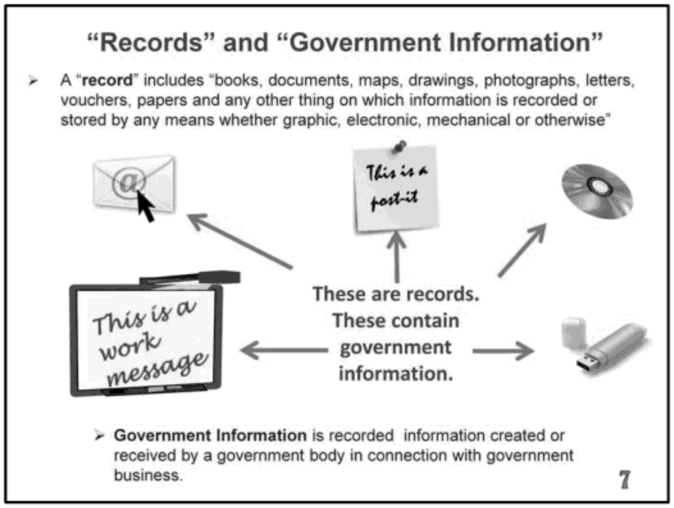
Contact Information

BC Privacy and Access Helpline:
250-356-1851
Privacy.Helpline@gov.bc.ca

BC Government Records Service Hotline
250-387-3387
GRS@gov.bc.ca

IM Policy guidance:
IM.ITpolicy@gov.bc.ca

In the event that you have any questions at all, either based on this training, or on the topic areas generally, then we have 3 great resources for you. You can direct any general privacy or access question through the Privacy and Access Helpline – if it is a question specific to a request, then you can direct your question to your DMO FOI Liaison – which is a new role that will function as your primary contact on access matters and liaise between IAO and your office. For any records management questions, about transitory records, records retention, disposition, ARCS/ORCS, etc., then you can call the GRS Hotline. Finally, if you have any questions about how to interpret or apply any IM policies, including core policy or the appropriate use policy. You will see this slide again, just to remind you of how important and great of a resource these are.



“Records” and “Government Information”

- A “**record**” includes “books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by any means whether graphic, electronic, mechanical or otherwise”

These are records. These contain government information.

This is a post-it
This is a work message

- **Government Information** is recorded information created or received by a government body in connection with government business.

7

- So now, we can jump into our actual content and start getting **refreshed** on information management.

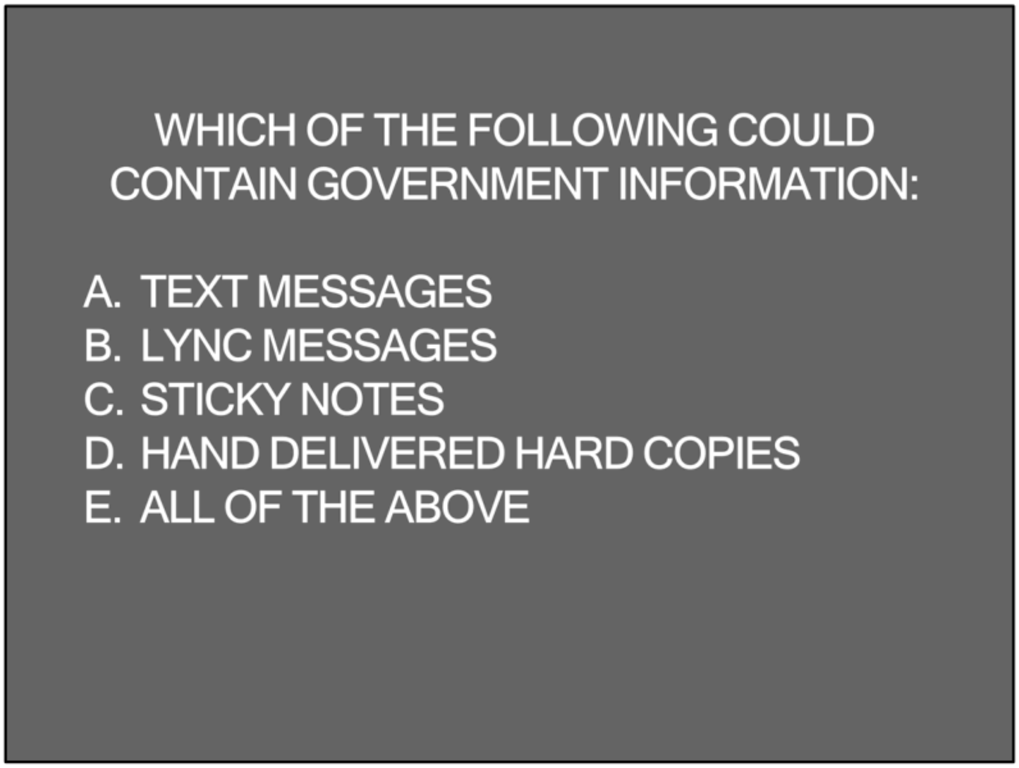
- Most of what we need to know in the area of information management focuses around the concepts of a “record” and “government information”, so it is important that we share a common understanding of these terms.

- A "record" is defined in legislation to include: books, documents, maps, drawings, e-mails, and any other places where you have put pen to paper, or typed something into a computer program. This definition is broad enough to include less obvious things like post-it notes stuck to your computer, text messages, and even Lync messages. So for the purposes of access to information or the protection of privacy, it’s this concept that you should keep in mind.

- Government Information is defined in the IMA as information created or received by a government body in connection with government business. When you’re thinking about records management, this is the concept to bear in mind.

- These two terms — “record” and “government information” are sometimes used interchangeably, and they are pretty similar.

- What’s important to understand is that in both cases it is the content and not the medium that matters.



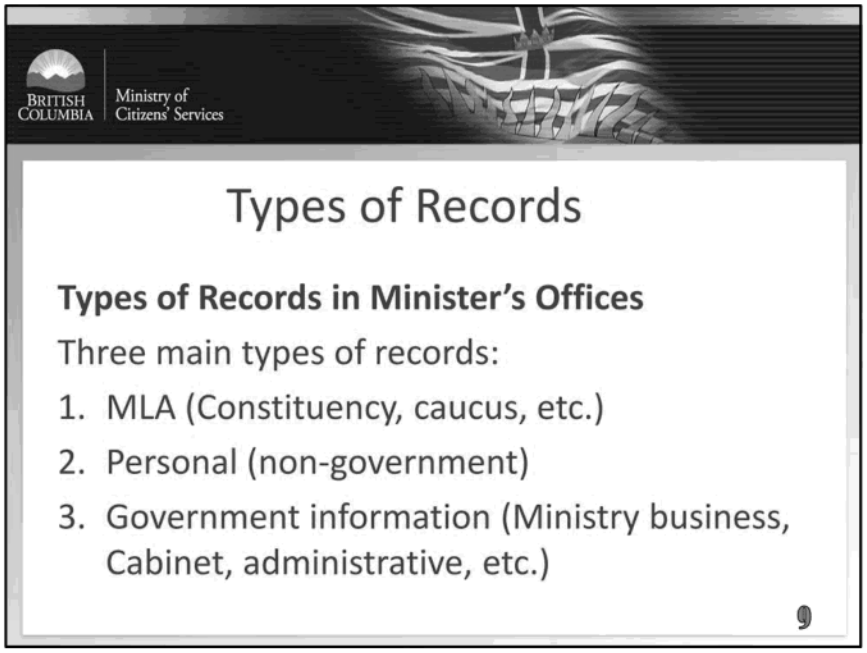
WHICH OF THE FOLLOWING COULD CONTAIN GOVERNMENT INFORMATION:

A. TEXT MESSAGES
B. LYNC MESSAGES
C. STICKY NOTES
D. HAND DELIVERED HARD COPIES
E. ALL OF THE ABOVE

We'll start with a bit of a knowledge test here… Which of the following could contain government information? Text messages, Lync Messages, Sticky Notes, hand delivered hard copies or all of the above.

The answer here is E - all of these could contain government information. it's important that we understand that It doesn't matter what medium is used to produce a record. What makes it government information is the context and, perhaps most importantly, the content - and that the information in the record relates to government business.

This is a great time to emphasize that **ownership** of media or hardware doesn't determine the ownership of the records or information – or **whether** something is a record or government information, for that matter. What I mean is, if you use your personal iPad because you're unexpectedly asked to comment urgently on a document while you're on vacation without your government-issued device – the work you produce on the iPad is still considered to be records or government information and is still subject to FOI, security and confidentiality protections, and other policy requirements. So, regardless of the fact that you used your own device. You need to treat that record just as you should any other containing government information – with the first step being to get it back on the government network and remove it from your personal iPad as soon as you have done that. There is more guidance on situations where it **is** and **is not** appropriate to use your own device in managing records, and that is in the Appropriate Use Policy. You need to know that this is only permitted in extenuating circumstances, and should be avoided where possible.



BRITISH COLUMBIA | Ministry of Citizens' Services

Types of Records

Types of Records in Minister's Offices

Three main types of records:

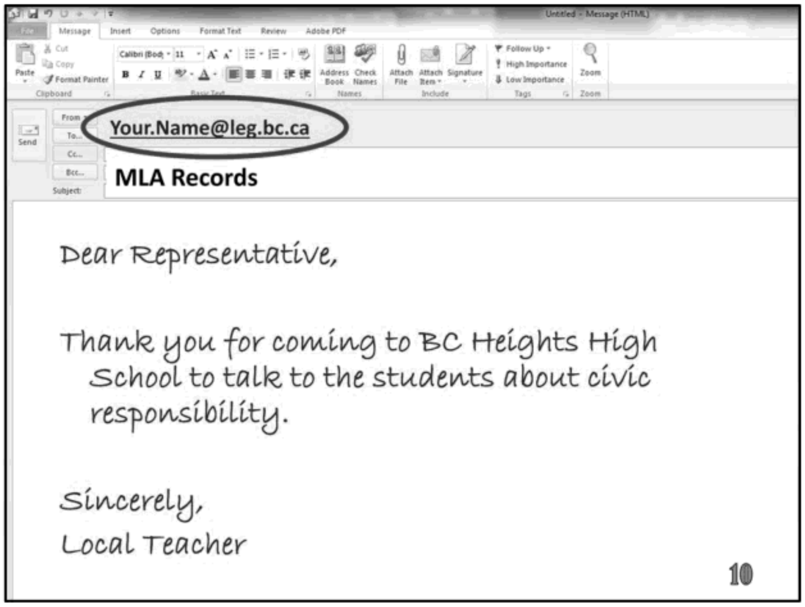
1. MLA (Constituency, caucus, etc.)
2. Personal (non-government)
3. Government information (Ministry business, Cabinet, administrative, etc.)

9

- In order to best understand our records management and access obligations we need to review the different types of record that your offices hold.

- In a Minister's Office there are three main types of records that you will deal with. I'm going to go into the details for each of these separately, but to start, in your work you likely deal with MLA, records that are strictly personal, and then those that are considered government records.

- Of course, these types of records may overlap – say, when your office receives a constituent email to the MLA but the email is then acted upon in the capacity of the Minister. It's important that these two distinct roles are reflected as such in your record keeping practices. However, if records blend – your government records obligations will apply, including provisions under FOIPPA including responsibilities to protect privacy and provide access to these records, and your obligations under IMA to manage them appropriately.



From: Your.Name@leg.bc.ca

Subject: **MLA Records**

Dear Representative,

Thank you for coming to BC Heights High School to talk to the students about civic responsibility.

Sincerely,
Local Teacher

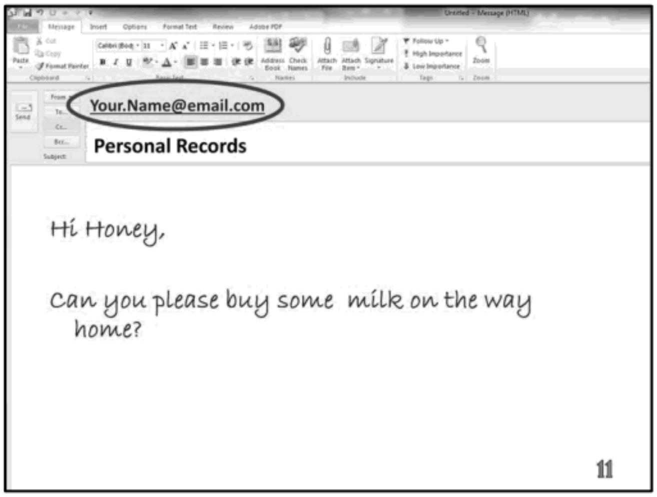
- MLA records are records created, accumulated or used by when the Minister is acting in his or her MLA capacity. MLA records can include communications, speeches and meeting records with constituents about MLA business, Caucus committee meetings or records produced for Committees of the Legislative Assembly.

- Considering the purpose for the communication can support you in determining which type of record is appropriate. For instance, when a constituent asks a Minister to support them with an issue that is outside of the Ministerial portfolio, this would be an MLA record. If the question is within the Ministerial portfolio or the Minister moves from an advocacy role to that of an official decision making role, this same original record should be viewed as government information. You should also consider how the materials are received, for example, whether it was received to your legislative email account.

- Use of letterhead, titles and salutations in correspondence should also be considered to ensure that the record is being appropriately actioned in either an MLA or Minister capacity.

- This means that this thank you note we see here from the School District would be an MLA record. And due to the material's content and distribution through the dedicated leg.bc.ca email account, it would not be covered by the Information Management Act or FOIPPA.

- Finally, care should also be exercised to ensure that MLA records in your office are not inappropriately distributed through the government email system as again they may become subject to FOIPPA's specific privacy and access provisions.



Your.Name@email.com

Personal Records

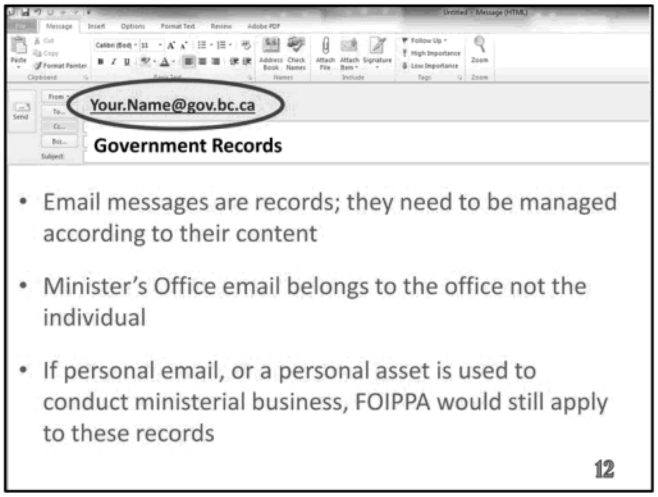
Hi Honey,

Can you please buy some milk on the way home?

- Personal records are records that are, as the name suggests, personal in nature. They relate to your private life or personal interests and are not received or created as part of your daily ministry or constituent business activities. Examples would include personal invitations, communications with family or friends (on non-government business), etc. These records, similarly **are not** covered by records management rules or privacy and access legislation, so we will again not linger on this type of record either, except to say that these records must be maintained separately from other records as much as possible. It is important to recognize here that not only will you be required to manage your own personal records, but may also encounter the personal records of the Minister, especially if in your capacity you deal with the Minister's calendar or correspondence (mail/email).

- I would also like to stress that it is not the medium, the device or the format that dictates that something is personal, it is the **content** and **context**. For example, we understand that you can't restrict an individual from sending a work-related email to your personal account. It's important that we are clear that email, or any other work-related records produced on personal email or personal devices **are not** considered personal records, those are considered government records.

- Further, personal email accounts should never be used to carry out government business, except in extenuating circumstances. When it is used, there are rules you need to follow. This includes copying emails to your government email address, deleting the information from your personal account as soon as you can, and ensuring you have shared the least amount of sensitive information that is necessary in the circumstance.



Your.Name@gov.bc.ca

Government Records

- Email messages are records; they need to be managed according to their content
- Minister's Office email belongs to the office not the individual
- If personal email, or a personal asset is used to conduct ministerial business, FOIPPA would still apply to these records

12

- What that leaves us with, after we remove personal and MLA records from the conversation is **"Government records",** which is essentially everything else.

- **Government** records, **including all those records that are produced in a Ministerial Office**, are covered by the IMA's records management requirements and FOIPPA's access and privacy requirements.

- It is also important to point out that government records belong to your ministry and not to the person who sent or received them.

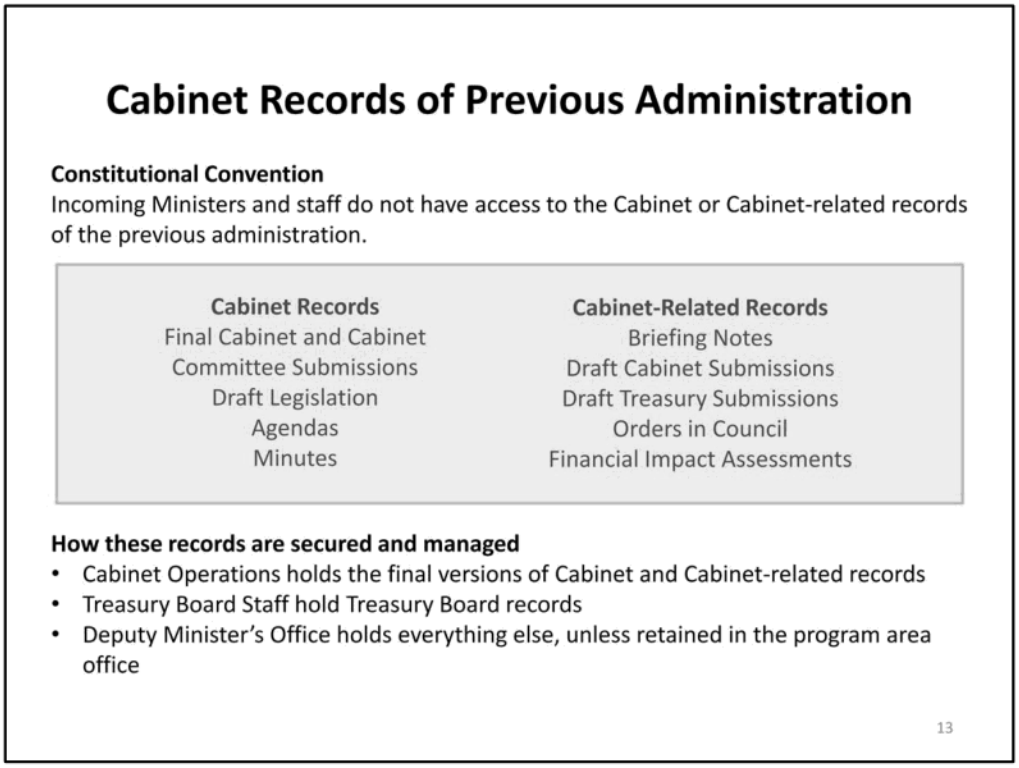
- Lastly, it is important that I emphasize that triple deleting email is never permitted.

I'm going to dig a bit deeper into a **few of these following examples** in a moment, but to get your minds around what we mean when we say government records, think about all of the types of records one might accumulate in the course of the daily administration of a ministry:

- Cabinet and Treasury Board submissions
- CLIFF records (records in govt's secure electronic database for storing records, often used for tracking approvals)
- Meeting minutes, agendas and handouts
- Planning and performance reviews and evaluations
- Texts and instant messages
- briefing notes, backgrounders, presentations and speaking notes.

This would also include both official records and transitory records – which we will discuss a little later.

For the moment, we are going to talk about three specific types of records that you will encounter frequently, and then discuss a few tips around how to manage these types of records.



Cabinet Records of Previous Administration

Constitutional Convention

Incoming Ministers and staff do not have access to the Cabinet or Cabinet-related records of the previous administration.

Cabinet Records

Final Cabinet and Cabinet Committee Submissions
Draft Legislation
Agendas
Minutes

Cabinet-Related Records

Briefing Notes
Draft Cabinet Submissions
Draft Treasury Submissions
Orders in Council
Financial Impact Assessments

How these records are secured and managed

- Cabinet Operations holds the final versions of Cabinet and Cabinet-related records
- Treasury Board Staff hold Treasury Board records
- Deputy Minister’s Office holds everything else, unless retained in the program area office

- Given the recent election, I first want to call your attention to a specific protocol that applies during and after the transition to all new administrations. This protocol applies to Cabinet records and Cabinet-related records. While these types of records are highly confidential and are always protected, additional rules around how they are secured and managed come into play after an election.

- **Cabinet Records** are those that have been prepared for submission to or circulated for consideration by Cabinet or a Cabinet Committee. Cabinet records may include agendas, minutes, final versions of Cabinet and Cabinet Committee submissions, decision letters of Cabinet and its committees, staff analysis, draft legislation, regulations and Orders in Council circulated for consideration by Cabinet, presentation decks and papers.

- **Cabinet-Related Records** are records held by public bodies that are created or received by the public body, which may reveal the substance of deliberations of Cabinet or a Cabinet Committee. This may include: correspondence including email correspondence, briefing notes, drafts of Cabinet or Treasury Board submissions, draft regulations and Orders in Council, financial impact assessments, and memoranda regarding confidential work for the consideration of Cabinet.

- **Constitutional convention -** Established Constitutional convention requires that all records which may reveal the substance of deliberations of a prior Cabinet or its committees are treated as privileged information of that government. This means an incoming administration (i.e., incoming Ministers and political staff) does not have access to these documents without the express consent of the outgoing administration (during/after transition, by approval of the DM responsible and the outgoing Premier or delegate)

- So what happens to these records? Cabinet Operations or Treasury Board Staff hold the final versions of Cabinet Records and Cabinet-Related Records. Where the Cabinet record or Cabinet-related record is an integral part of ministry business files, a copy should be retained in the relevant operational/business unit files. These copies of Cabinet confidential records must be kept secure to ensure no unauthorized access, and must only be accessed by members of the public service, and on a need-to-know

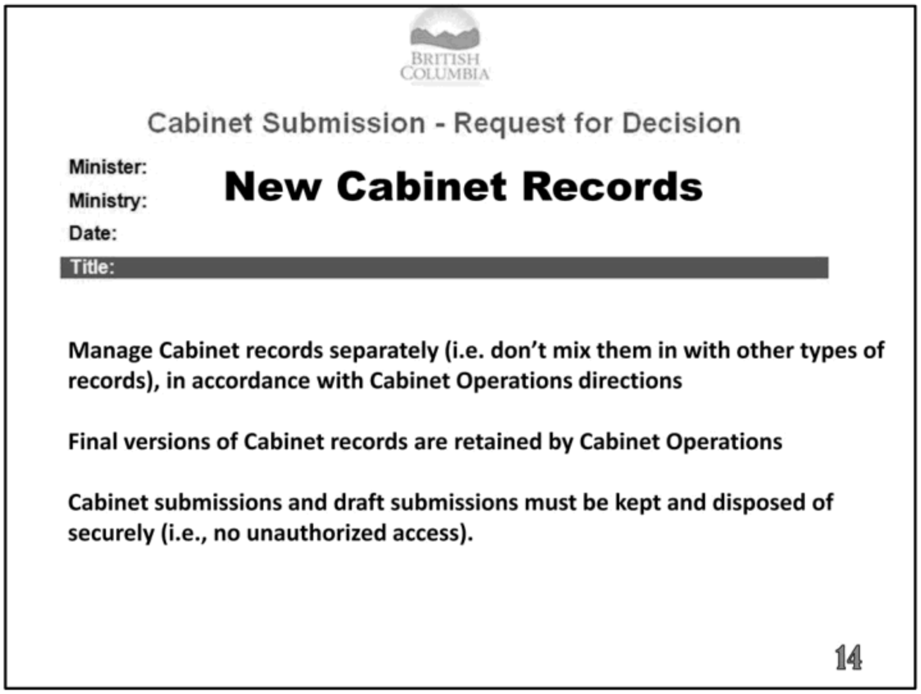
- In responding to requests of a new government, the proper procedure is for staff to paraphrase the information in the records and/or prepare new reports and submissions, rather than simply providing copies of old ones. Previous Cabinet submissions and materials used in their preparation may continue to be used as resource documents by Public Service staff preparing new submissions .

[content below for reference and to be used as needed]

- Although a new administration is precluded from viewing the records of a previous administration, it is generally permissible for a new administration to obtain information about decisions made by a previous administration, particularly where the information is necessary to ensure that government business will be carried out effectively.

- After a change in administration occurs, in providing advice to the new Executive Council, where the continuity of administration requires reference to records prepared for previous Executive Councils, it may be appropriate to paraphrase the contents of those materials.

- However, in disclosing information about the decisions made by a prior administration, employees must take care to continue to protect information about the options presented to the Executive Council in making the decision and any information related to the opinions


BRITISH
COLUMBIA

Cabinet Submission - Request for Decision

Minister:
Ministry:
Date:
Title:

New Cabinet Records

Manage Cabinet records separately (i.e. don't mix them in with other types of records), in accordance with Cabinet Operations directions

Final versions of Cabinet records are retained by Cabinet Operations

Cabinet submissions and draft submissions must be kept and disposed of securely (i.e., no unauthorized access).

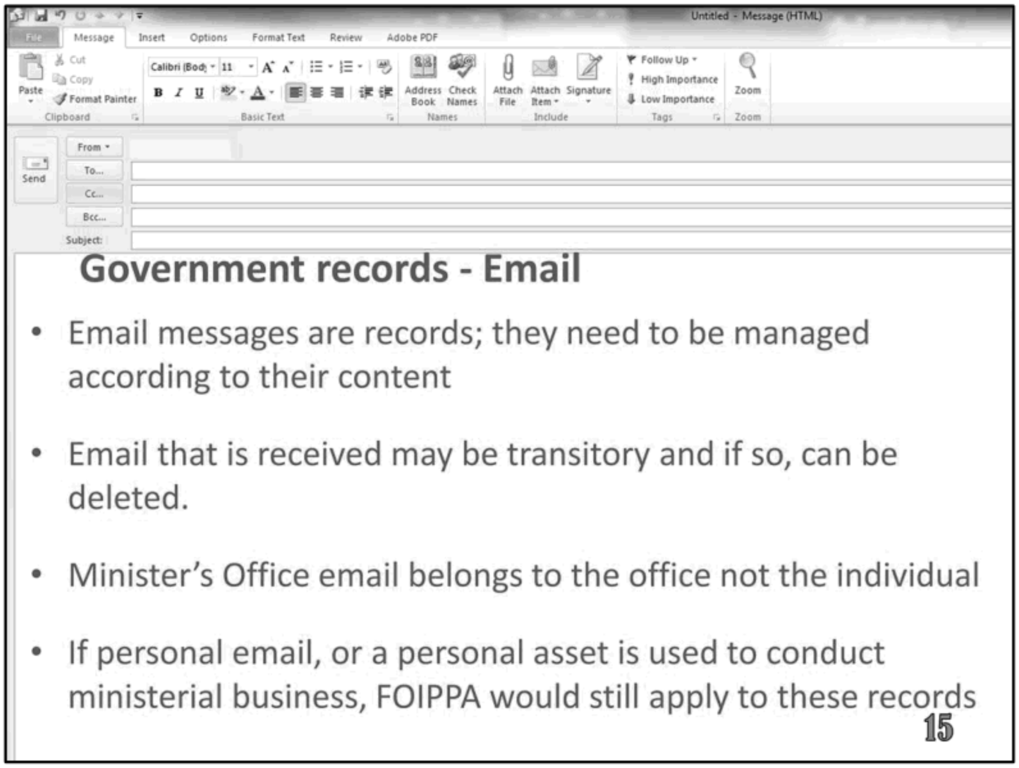
14

While we have spoke about how Cabinet records from previous administrations are treated, we must also speak about how Cabinet records created by the new government should be managed.

It's important that you **have**, or develop a system to manage Cabinet records separately from other government records. Cabinet records should not be mixed in with other types of records. **Final versions** of Cabinet records are retained by Cabinet Operations. So, you should follow Cabinet Operations directions on how you should manage these records.

It is important that you keep and dispose of draft and final Cabinet submissions **securely**. This is true of all government records, but there is an inherent need to protect Cabinet integrity that may require **additional** security measures.

This also seems like an important time to highlight that these types of records – as with the other types of government records we have discussed - **are** responsive to FOI requests. This means that if you have cabinet records that respond to an FOI request, you would provide them to your DMO FOI Liaison. It is **your** responsibility to ensure that when providing cabinet records to DMO FOI Liaison that they are made aware of this sensitivity. They will ensure IAO is made aware of this sensitivity so they are able to review the records and apply severing recommendations that will protect any cabinet confidences. Rely on the **FOIPPA exceptions** to dictate what records can be withheld from release and IAO will guide you here. In general, Cabinet confidential information is mandatorily withheld from disclosure, with a few exceptions, e.g. where the record has been in existence for over 15 years.



Government records - Email

- Email messages are records; they need to be managed according to their content
- Email that is received may be transitory and if so, can be deleted.
- Minister's Office email belongs to the office not the individual
- If personal email, or a personal asset is used to conduct ministerial business, FOIPPA would still apply to these records

15

The next record example I'll walk you through is government email. It is important to remember that work emails contain government information. How you manage email depends on its content. You may have heard the misconception in public that all emails are transitory. We'll deal with this concept of transitory in a moment – but for now, just remember that an email **is** a record. This is important because it is actually the content of that email that determines its value. The form of the record – the fact that it is an email - isn't a factor in determining whether or not you need to keep it.

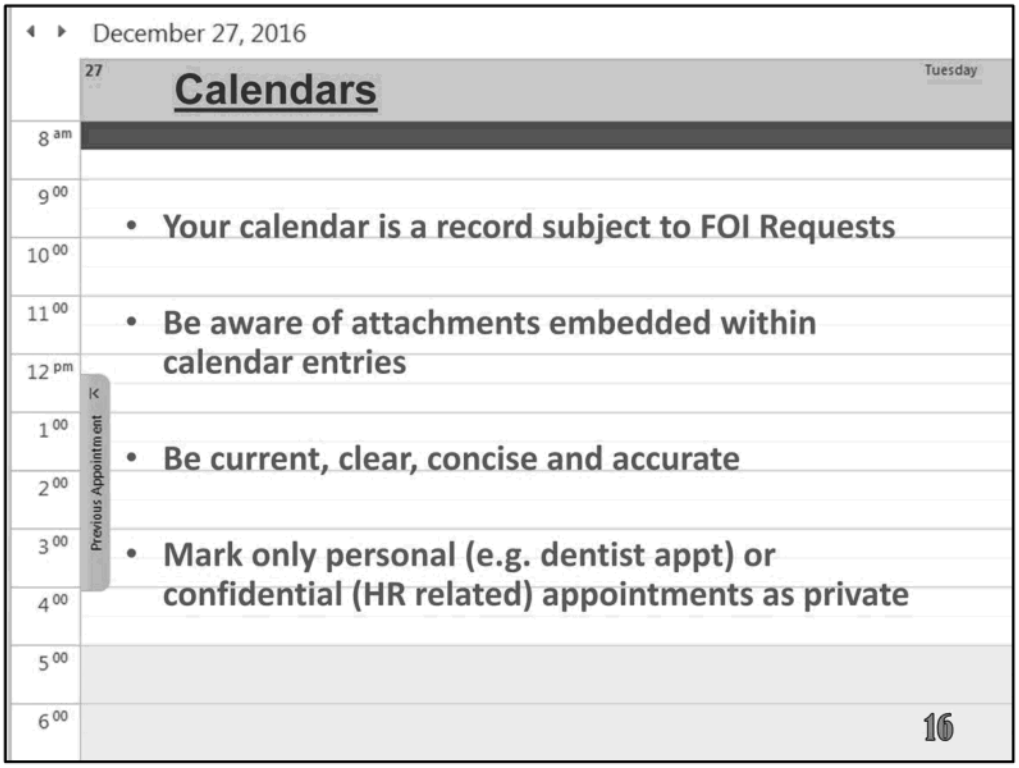
I also want to reiterate the point that your email records that pertain to government business, are government records no matter the email account you are using, but you should also avoid using your personal email account to do your work. In the extenuating circumstance when you absolutely must do so, there are rules you have to follow, which include "cc-ing" your government email account, deleting the emails from your personal email account as soon as possible, and ensuring you share the least amount of sensitive information that is necessary in the circumstance. Where that sensitive information is someone's personal information, use additional caution to ensure that it is adequately protected. In general, personal information cannot be shared outside of Canada. We will review data residency requirements later in this material.

I want to share some email management tips here. These are not mandatory requirements, but instead are strategies that you can implement to support you in creating records that are more manageable when responding to an FOI request. You know your work and therefore you are able to determine which emails are important to that work. If you have emails with information that will either be useful to document the work of your office or for others in doing their work, then you should file those emails in your office recordkeeping system. Likely, for most of you, this won't be a significant number of your emails. Most of the information we share by email is repeated in other documents and is already stored elsewhere. But if you think the email contains the best documentation of an action or decision, you should save a copy, or use the email to prepare a formal document and then dispose of it.

It can be challenging to manage emails when they contain a lot of different topics or move into overlapping and lengthy threads. If you can, try to be specific, to limit the content of your email to one subject area, and to clean up email chains and lengthy threads. You should also try to stay on top of tasks like regularly deleting transitory email. Many emails are only of temporary use and are therefore considered transitory.

For example, a ministry-wide notice to all employees can usually be disposed of as transitory. It is the responsibility of the initiating office to file and maintain an official copy, in their office recordkeeping system.

Lastly, it is important that I emphasize that triple deleting email is never permitted. If you don't know what triple deleting is, then don't worry, this is not something you can accidentally do.



Calendars

- Your calendar is a record subject to FOI Requests
- Be aware of attachments embedded within calendar entries
- Be current, clear, concise and accurate
- Mark only personal (e.g. dentist appt) or confidential (HR related) appointments as private

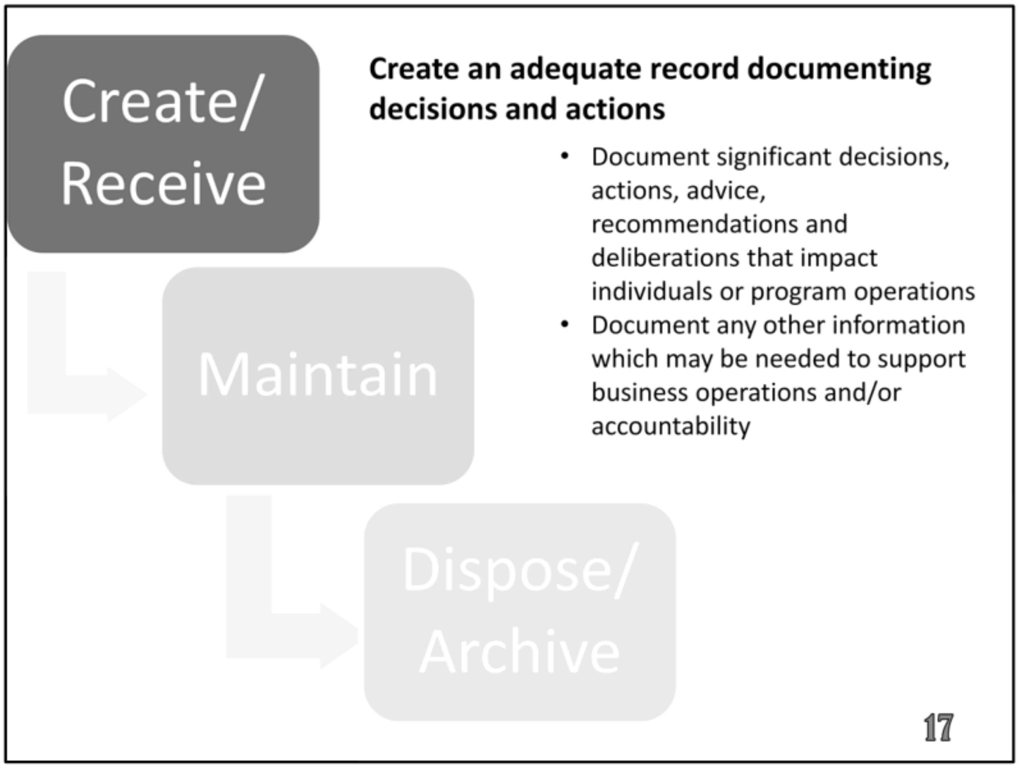
16

The final records example I wanted to highlight is Outlook calendars. As you may know, A Ministerial Directive under FOIPPA requires the monthly disclosure of calendars of Minister, Deputy Ministers, Associate Deputies, and Ministers of State. To facilitate consistency and ensure security in making these disclosures, certain practices need to be maintained within your offices

Calendars should be maintained so that entries are consistent, clear and current. You can do this by keeping the subject heading for meetings informative and concise. You can keep your calendar current by updating the calendar as changes occur. This means removing meetings that did not occur or were not attended and by updating the calendar entry to reflect who actually attended a meeting. And as for **personal** appointments - like a dentist appointment or a reminder to pick up the kids from school, mark these as **private** – that way details will not show up in a printed copy or to anyone other than the calendar owner or a delegate. However, you need to ensure that **only personal or confidential appointments** are labeled as “private”.

If you are interested in receiving a dedicated training session on how to maintain calendars contact your DMO FOI Liaison – their contact information is in your resource package.

We are now going to move from talking about specific record types or concepts that can be applied to all records – namely the record lifecycle.



Create an adequate record documenting decisions and actions

- Document significant decisions, actions, advice, recommendations and deliberations that impact individuals or program operations
- Document any other information which may be needed to support business operations and/or accountability

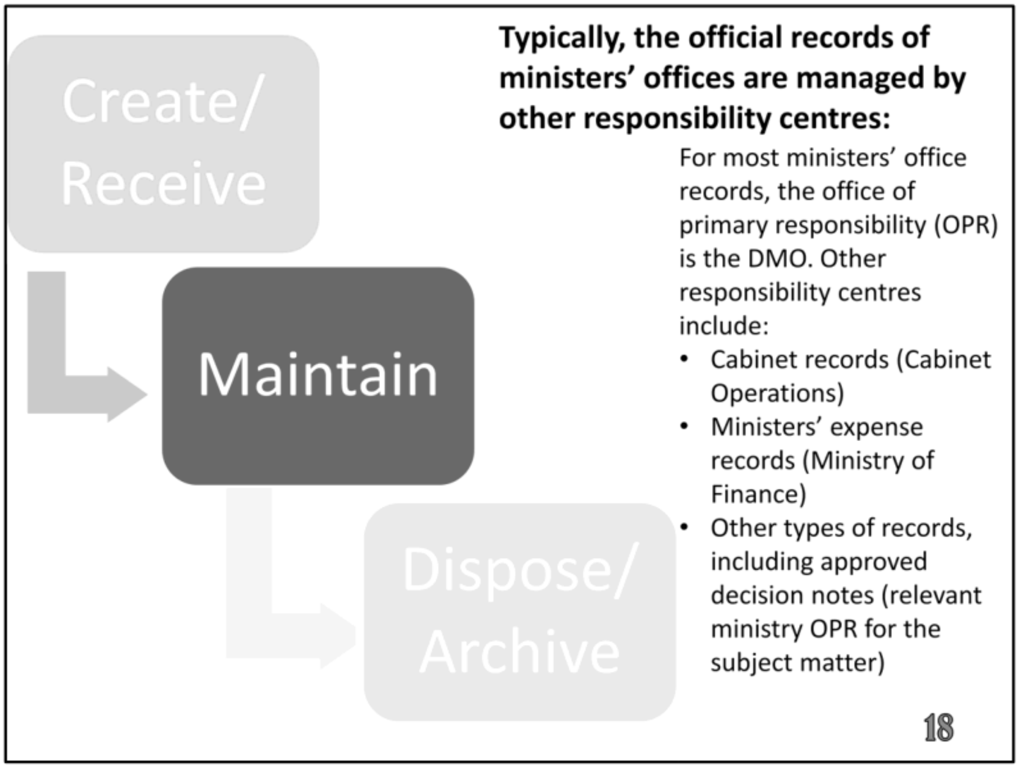
17

Now it’s time to talk about what to do with government information, from the beginning to the end of its lifecycle. The lifecycle of government information is simple - information is created or received, you use and maintain it, and then the information is either disposed of or sent to the government archives. Some information only lives for a few minutes or hours, and some is never disposed of, but rather is permanently preserved in the government archives.

Always ensure that you are creating a full and accurate account of decisions and actions that support business operations. We will now walk through each stage of the lifecycle of government information in order to learn more about it. We’ll use an example to make these stages easier to understand. Think about a project where your office is leading a large project involving several offices across different divisions of your ministry.

Create/Receive

As you work on the project, you naturally create and receive government information, such as a project charter, meeting agendas and minutes, email correspondence, and project plans and reports. To have a full and accurate record of the project, you need to have documentation of significant project activities, decisions and results.



Create/ Receive

Maintain

Dispose/ Archive

Typically, the official records of ministers' offices are managed by other responsibility centres:

For most ministers' office records, the office of primary responsibility (OPR) is the DMO. Other responsibility centres include:

- Cabinet records (Cabinet Operations)
- Ministers' expense records (Ministry of Finance)
- Other types of records, including approved decision notes (relevant ministry OPR for the subject matter)

18

As you create and receive government information, it is important to ensure that you maintain the information so that it is available to those who need it and is kept for the required length of time. You should always retain information that details significant activities of your unit, as well as changes to existing programs or the establishment of new ones.

Going back to our example, any information that is needed by your office to perform or document project activities must be filed in your office recordkeeping system. You can file these temporarily, in a collaboration system such as SharePoint, but be sure to transfer them to the recordkeeping system when you have wrapped up the project.

A recordkeeping system is a shared system organized according to government information schedules. Two examples of office recordkeeping systems are an appropriately organized office network drive, sometimes called your "LAN", or the government Enterprise Document and Records Management System (EDRMS), known as TRIM. This office recordkeeping system does not include locations that are only available to you, such as your desktop, home drive or the hard drive of your computer.

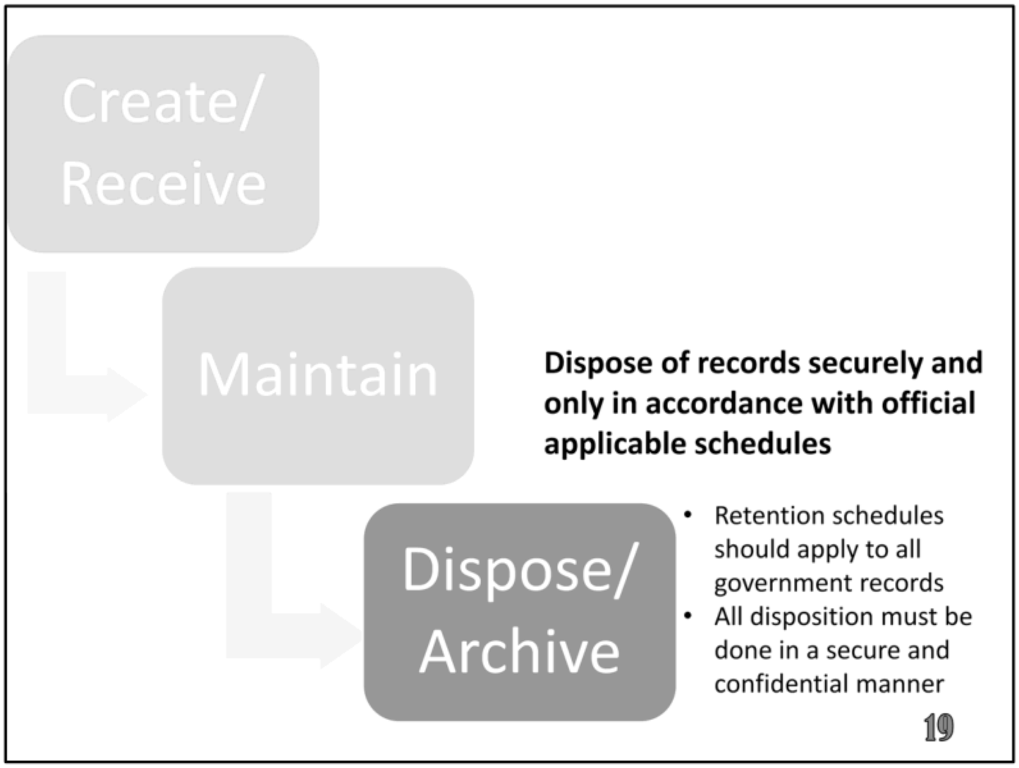
Your office may also use other information systems for recordkeeping. This is fine, as long as they have appropriate information management controls, including use of information schedules. These schedules specify how long each category of information must be kept. Within the office recordkeeping system for government we use ARCS, which stands for the Administrative Records Classification System, and ORCS, which stands for Operational Records Classification System.

In our example, project information would be categorized according to the ARCS classification for large administrative projects. Of course, not all government information has to be kept - and this will be discussed later.

Since your project involves multiple offices of your ministry, you will need to be clear about which office is the office of primary responsibility (or "OPR") for the project. The OPR maintains the official file copy of government information. For most records involving the minister's office, the OPR is the Ministry's DMO. The DMO is able to provide continuity and appropriate public service administration of the records of successive ministers.

Minister's office official records need to be retained at minimum for 10 years (under the Executive records schedule), after which they are reviewed by an archivist before archival selection. Examples of other responsibility centres include Cabinet Operations for Cabinet records; and Ministry of Finance for Minister's Office expense records.

In our example, you are the project lead and your Ministry's DMO is the OPR. If other offices in your ministry need to keep copies of project information for their own business purposes, they can keep them as "non-OPR" copies and dispose of them when they no longer need them.



Create/ Receive

Maintain

Dispose/ Archive

Dispose of records securely and only in accordance with official applicable schedules

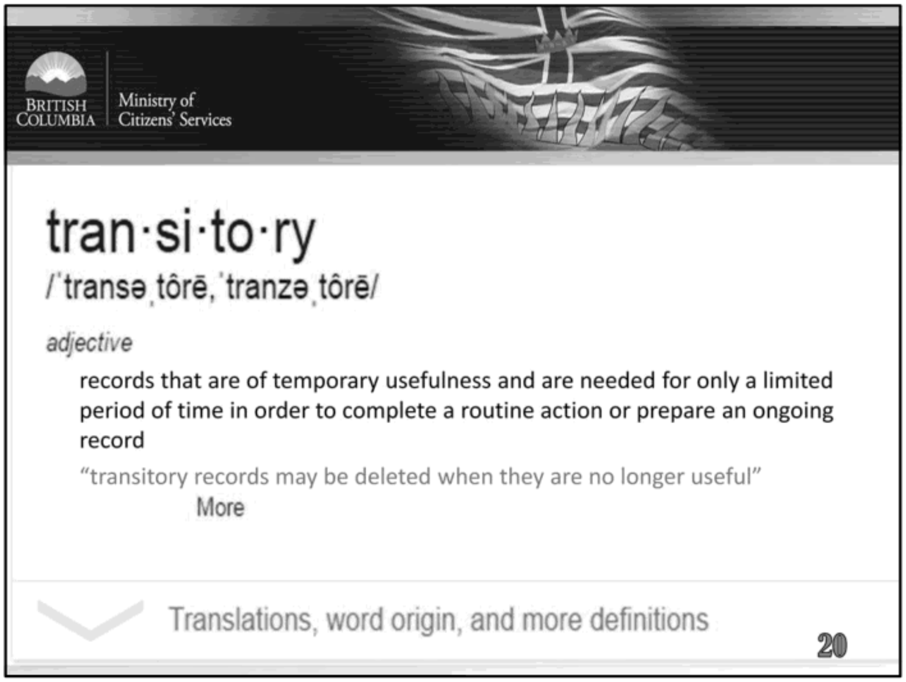
- Retention schedules should apply to all government records
- All disposition must be done in a secure and confidential manner

So, now that we know with whom and where records are maintained, we can talk about disposition. Information schedules provide timetables which tell us how long different types of information is needed and when the information may be disposed of or sent to the government archives.

This is important because you cannot dispose of information unless there is an information schedule to authorize it. Some information schedules identify information that must never be disposed of, but rather must be maintained until it is ready to be transferred to the government archives. Transitory information has its own information schedule that allows you to dispose of the information when it is no longer useful. You will learn more about transitory information shortly.

All disposals must be carried out in a secure and confidential manner. The more sensitive information is, the more measures we have to take to ensure it is securely and appropriately disposed of. Your Records Officer in the Government Records Service (GRS) can help with this.

Returning to our example, once the project is completed or cancelled and the appropriate amount of time has elapsed, your project file can be reviewed by an archivist for decision on archival. If you work in an office not subject to the Executive Records Schedule (i.e., not in a minister’s or DM’s office), you can dispose of your project file two years after the project is completed or cancelled.



BRITISH COLUMBIA | Ministry of Citizens' Services

tran·si·to·ry

/ˈtransəˌtôrē,ˈtranzəˌtôrē/

adjective

records that are of temporary usefulness and are needed for only a limited period of time in order to complete a routine action or prepare an ongoing record

"transitory records may be deleted when they are no longer useful"

More

Translations, word origin, and more definitions

20

- Good records management dictates that we need to retain records of value and dispose of records of temporary value, once they are no longer useful.

- This is best practice in information management and is essential for appropriately handling the escalating volume of records that government has in its control (for example, the Province receives 284 million emails annually).

- good records management practices have been likened to that of good household management, with the retention of all electronic records an inappropriate practice akin to hoarding. This should be avoided at all cost.

- Information schedules, approved or continued under the Information Management Act , define criteria as to whether a record is an official government record which **must** be retained or is a transitory government record which **may** be disposed of. Even transitory information has its own information schedule that allows you to dispose of information when it is no longer useful.

- Simply put:
  - **Official** government records **must** be retained within the Minister's Office or an OPR such as the Deputy Minister's Office; and,
  - **Transitory** government records may be disposed of – following an assessment that they are appropriately categorized as transitory.

It may be surprising how something that seems so simple on the surface can become fairly complex. So, let's do a deeper dive into the concept of transitory records. Starting with a test of your knowledge.

WHICH OF THE FOLLOWING STATEMENTS IS TRUE:

A. TRANSITORY RECORDS CAN BE DISPOSED OF AT ANY TIME.
B. ALL INSTANT MESSAGES ARE TRANSITORY
C. TRANSITORY RECORDS ARE SUBJECT TO FOI
D. DELETING A RECORD MAKES IT TRANSITORY

Which of the following statements is TRUE:
a) Transitory Records can be disposed of at any time. (FALSE)
b) All Instant Messages are transitory. (FALSE)
c) Transitory Records are subject to FOI. (TRUE)
d) Deleting a record makes it transitory. (FALSE)

So, the correct answer is "c". All transitory records are subject to FOI requests. And because of that, if you receive an FOI request any transitory records that exist at that time, may be responsive to that FOI request. In other words, if you have an FOI request, you **cannot delete** the responsive transitory records. While you were **able** to delete them previously, if you kept them, they are responsive to the request and you must provide them to IAO.

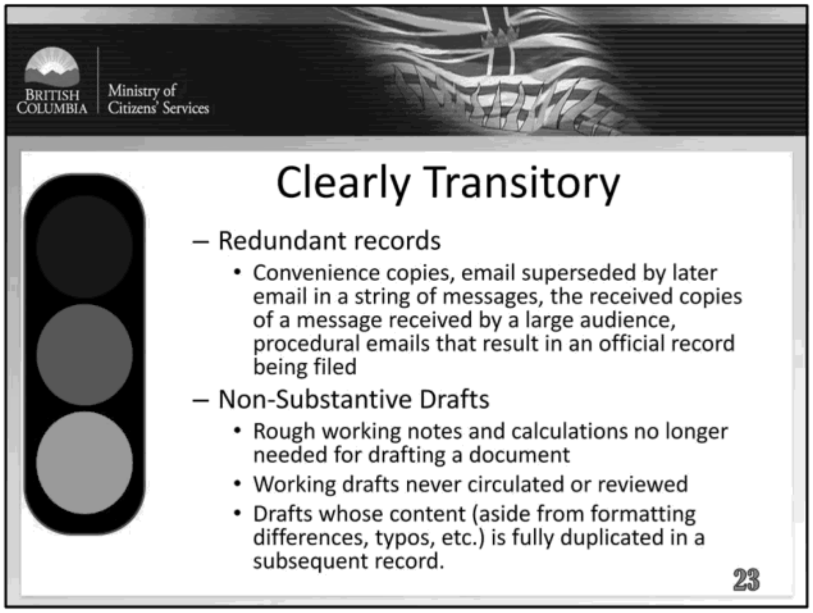
> “It is a record’s content and context that determines whether a record is transitory, rather than its form
>
> - Elizabeth Denham, Information & Privacy Commissioner

One of the things I really want you to take away from our training today is a very clear understanding that it is the **content, context** or **value** of a record, not the record’s form that you need to consider. In other words, **emails** should not be considered transitory. Instead, the content of a specific email may be. Ditto on instant messages. While most people don’t conduct serious business over Lync or text message, if they do, those records need to be kept and filed appropriately.

In terms of a definition,

Transitory records are of **temporary** usefulness and are needed for only a **limited period of time** in order to complete a **routine** action or prepare an ongoing record.

- They are not required to **document decisions** and actions or to support ongoing government business.
- They are not **regularly filed** as standard records
- They are not required to meet statutory requirements, **or**
- They are **redundant,** extra copies



BRITISH COLUMBIA | Ministry of Citizens' Services

Clearly Transitory

- Redundant records
  - Convenience copies, email superseded by later email in a string of messages, the received copies of a message received by a large audience, procedural emails that result in an official record being filed
- Non-Substantive Drafts
  - Rough working notes and calculations no longer needed for drafting a document
  - Working drafts never circulated or reviewed
  - Drafts whose content (aside from formatting differences, typos, etc.) is fully duplicated in a subsequent record.

- So, how does your office determine if something is transitory? I am going to walk you through some examples to try to illustrate the decision making process in the context of the records that are produced in a Ministerial office.

- Duplicated information is a good example of what can be transitory. Imagine a typical email conversation that goes something like this:

  - Email from another office: "Have you considered the proposal that we talked about?"
  - You respond: "Yes, I like the idea, could you please send it in writing?"
  - Other office: "Here it is. Tell me if you need any changes."
  - You: "Your proposal (attached) is approved."

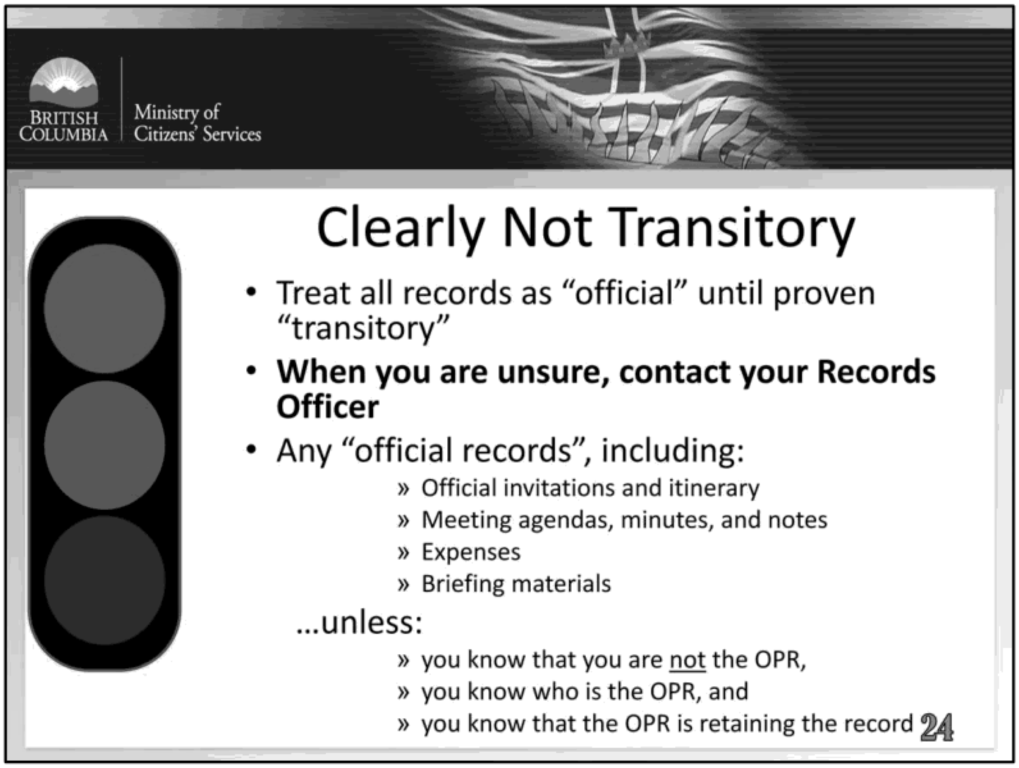
- In this simple example, you will end up with four emails, two sent and two received. Each of which contains the previous emails. In this example, you can feel confident deleting the first three emails if you are retaining the fourth, as the fourth contains the entire chain, as well as the decision.

- As another example, if you make a handwritten note while you are listening to a voicemail, and then copy your note into an email, you can delete the voicemail, and dispose of your handwritten note as transitory.

- Non-substantive prior drafts, which can include those that contain changes to elements like the formatting and margins, or corrections to grammatical errors are also transitory. Drafts that were never circulated or reviewed are also considered non-substantive.

- Even though transitory information may be disposed of when it is no longer required, it is unlawful to delete or destroy any transitory record that is the subject of a current FOI request.

- Transitory records also must not be deleted where they may be relevant to a current or an expected future legal action.



BRITISH COLUMBIA | Ministry of Citizens' Services

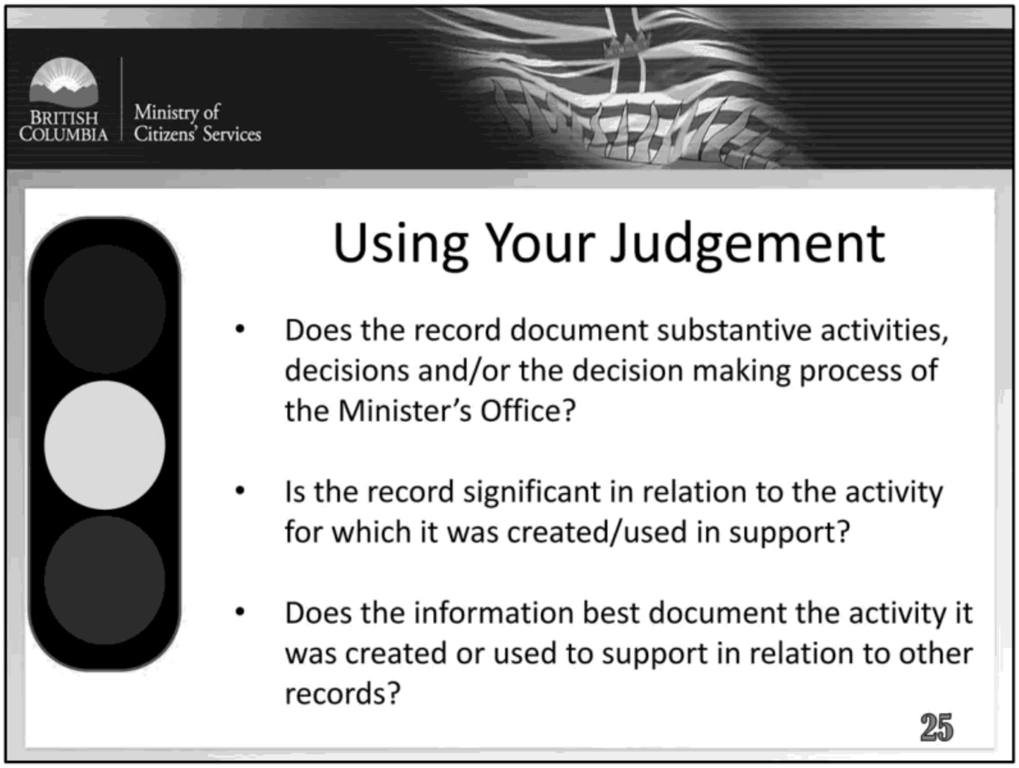
Clearly Not Transitory

- Treat all records as "official" until proven "transitory"
- **When you are unsure, contact your Records Officer**
- Any "official records", including:
  - » Official invitations and itinerary
  - » Meeting agendas, minutes, and notes
  - » Expenses
  - » Briefing materials

…unless:

- » you know that you are not the OPR,
- » you know who is the OPR, and
- » you know that the OPR is retaining the record 24

- On the other end of the spectrum, there are those records that are clearly **not** transitory.
- Information that is clearly not transitory would include incoming public correspondence, meeting minutes, and case files. You may, however, have copies of information such as meeting minutes that are transitory, provided that:
  - You know that your office does not hold the relevant OPR file, and
  - Your office has no need to file your copies for its own business use.

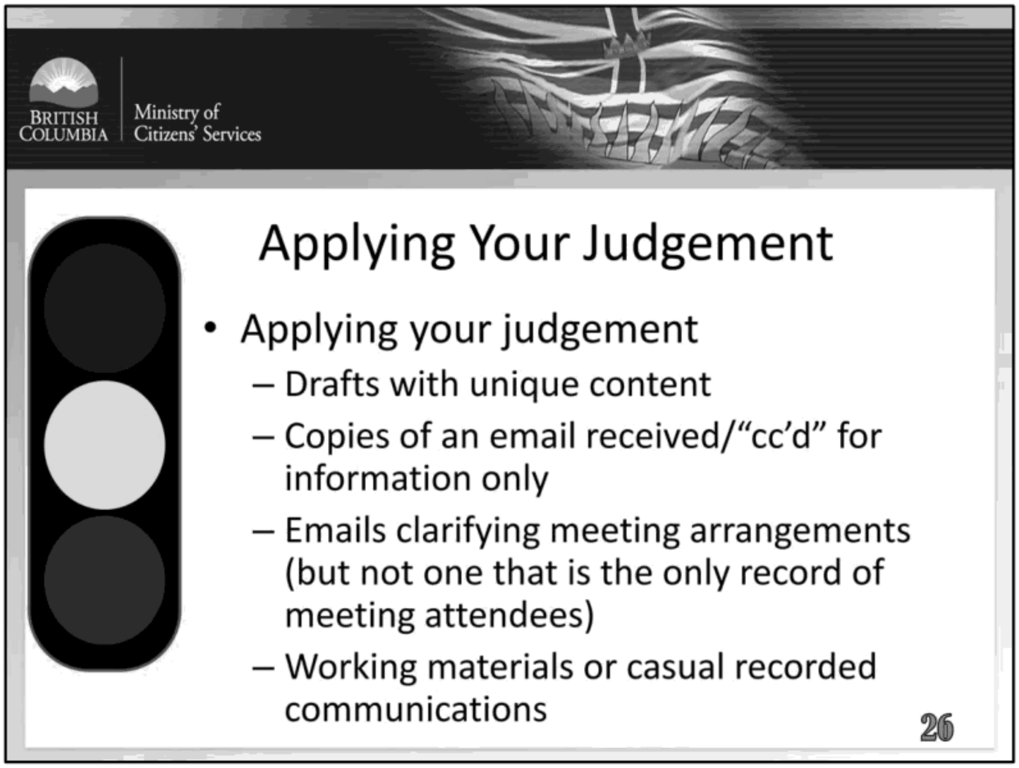

BRITISH COLUMBIA
Ministry of Citizens' Services

Using Your Judgement

- Does the record document substantive activities, decisions and/or the decision making process of the Minister's Office?
- Is the record significant in relation to the activity for which it was created/used in support?
- Does the information best document the activity it was created or used to support in relation to other records?

25

- When faced with information that is neither clearly transitory or official, you will need to ask yourself these questions:
  - Does the information document an important activity, or decision?
  - To what extent is this already documented somewhere else?
  - Is the information important in relation to the activity for which it was created or which it was used to support?
  - In relation to other information, does this information best document the function or activity for which it was created or which it was used to support?
- If you are unsure as to whether something is transitory or not, you can contact your Records Officer in the Government Records Service (GRS) for assistance.



BRITISH COLUMBIA | Ministry of Citizens' Services

Applying Your Judgement

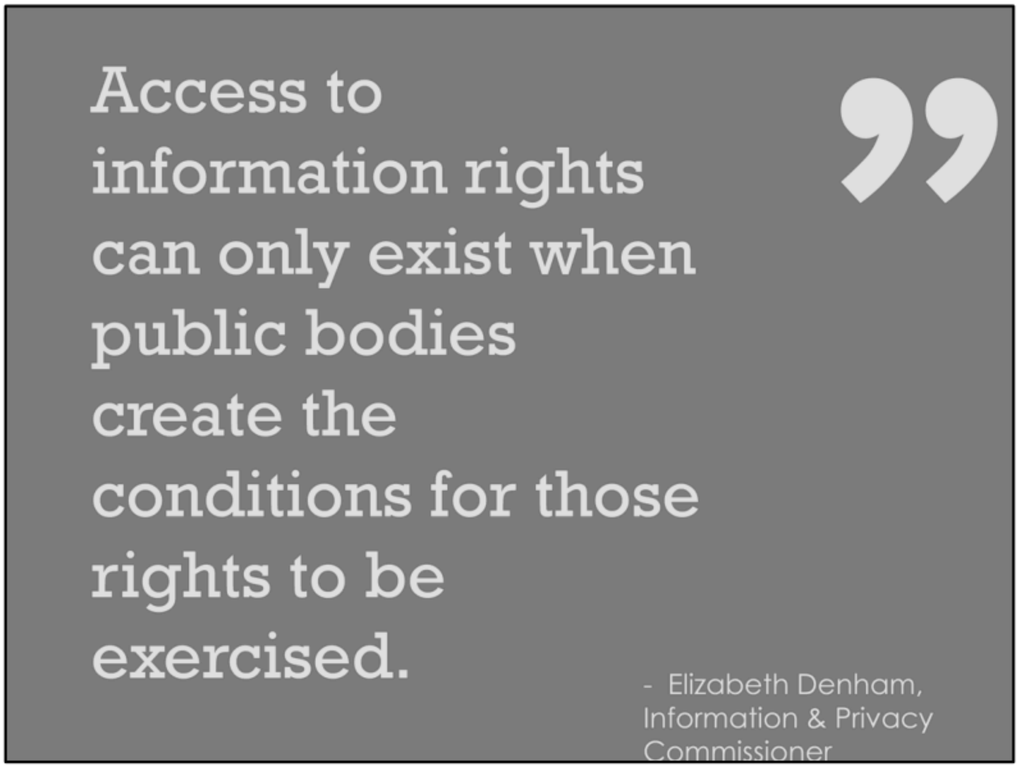
- Applying your judgement
  - Drafts with unique content
  - Copies of an email received/"cc'd" for information only
  - Emails clarifying meeting arrangements (but not one that is the only record of meeting attendees)
  - Working materials or casual recorded communications

26

I've got a couple examples here that are meant to make you second guess things a little bit and demonstrate that you shouldn't make broad-brushed assumptions about types of records, and that records need to be assessed on a case by case basis.

As I have said, drafts can be transitory, however, some drafts will have unique content. The determination depends on the unique content. If a change is to an editor's comment suggesting a change of one particular word – this would suggest it is transitory. However, if the one particular word that is changed is "approved" from "not approved", then that is definitely not a transitory record. And this is a good example on why "draft" – "or minor edits" does not equal "transitory".

I know that this can seem complicated, but you are all trusted public service employees who have been empowered to make these decisions. If you are not confident that a reasonable, disinterested outsider would agree with you, then you should refer to the transitory records guide, and if you are still unsure it's important that you consult with a Records Officer.



Access to information rights can only exist when public bodies create the conditions for those rights to be exercised.

- Elizabeth Denham, Information & Privacy Commissioner

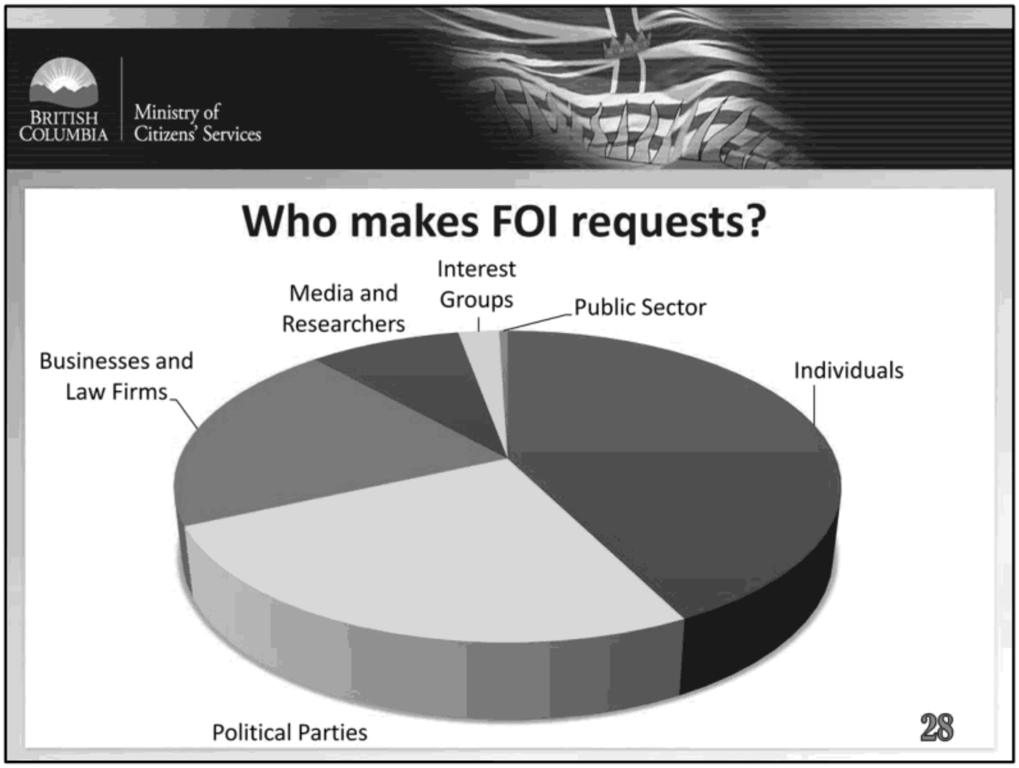
So why the focus on transitory records? We want to make sure that you are keeping the right records so that those records are available for accountability purposes. As the Commissioner recently said “Good governance and good record keeping go hand in hand”

More to the point of what we will be discussing next, here is a quote from the former Information and Privacy Commissioner from one of her last reports:
“Access to information rights can only exist when public bodies create the conditions for those rights to be exercised”

Records Management does not exist solely for the benefit of FOI – there are a **number of reasons** why Records Management benefits us both internally and externally. **However**, without strong Records Management practices, it is very hard to effectively manage FOI.

It is one of the key “conditions” that allows Access to Information rights to be exercised.

Next, I am going to remind you of your obligations in responding to an FOI request and supporting government’s commitment to Access.



British Columbia | Ministry of Citizens' Services

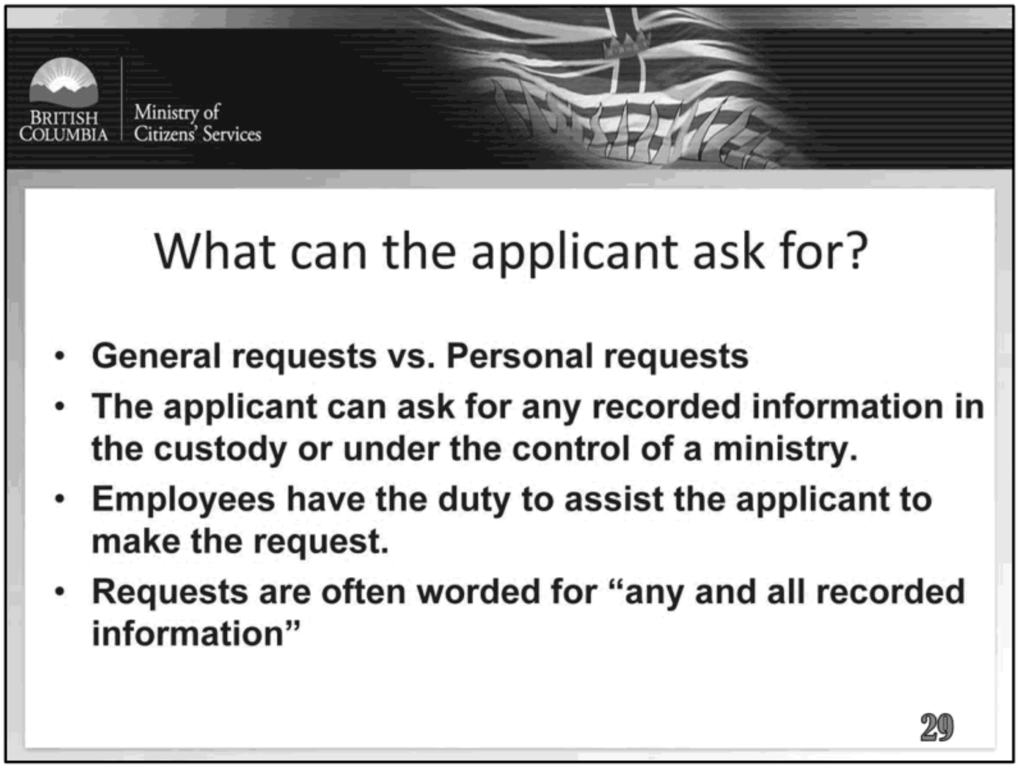
Who makes FOI requests?

28

Many of you may already know what an FOI request is, and may have experienced them already in your role. In simple terms, however, it is simply, an individual exercising their right to access government information. To become an "**FOI applicant"** an individual must submit a written request for access to a record. The request wording has to be **clear enough** and contain **enough detail** to enable an employee to identify the records sought.

An FOI request is **usually** submitted to IAO – although, if an employee outside of IAO receives a request it is still considered an FOI request. If this happens to you, you need to forward the request to IAO on the applicant's behalf – particularly because there are tight legislated time restrictions that have probably already started!

I have here a breakdown of the types of requesters that we get, but you should know, that none of this makes a difference as to what they receive, unless they are requesting their own personal information, which is the case with most of the individuals represented in this chart. Political parties get the same information media, researchers, interest groups or lawyers get.



BRITISH COLUMBIA | Ministry of Citizens' Services

What can the applicant ask for?

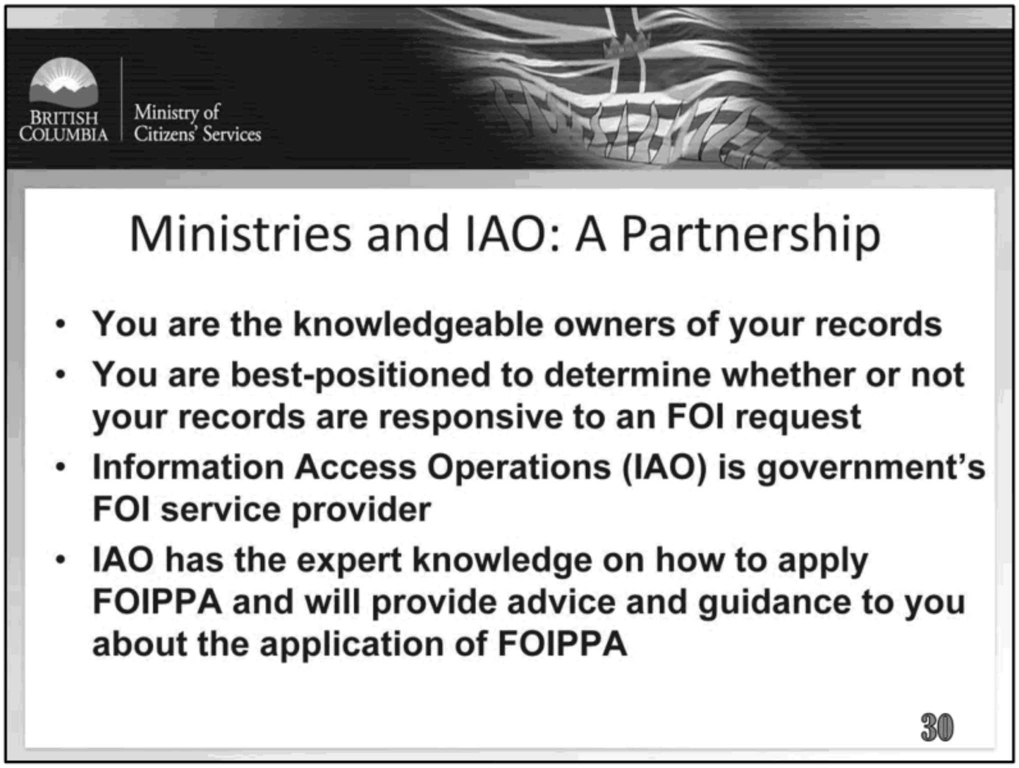
- **General requests vs. Personal requests**
- **The applicant can ask for any recorded information in the custody or under the control of a ministry.**
- **Employees have the duty to assist the applicant to make the request.**
- **Requests are often worded for "any and all recorded information"**

29

So what can an applicant ask for? To be honest, this is a bit of a trick question. An FOI applicant can ask for **any** record. They have the right to request any record, but this does not mean they have a right to **access** every record. To this effect, IAO will conduct a line by line review of any responsive records to ensure that information that is **legally appropriate** to be severed - or in other words, removed - prior to release has been highlighted as such.

Further, applicants must request **specific** records – because FOI is not built to **answer** questions, instead it is built to provide the records **that may answer** a question. What this means is you will find requests that are often worded as: "I want any and all records regarding the costs incurred constructing the 6-mile bridge" and not, "How much did the 6-mile bridge cost?". We will talk in a moment about duty to assist, but it is worth noting here, that if you do receive a request asking how much did the bridge cost, that just because they didn't "ask the question correctly" doesn't mean we are going to deny them records. We have a responsibility to be open and to connect people with the records to which they have a right to access.

I should point out, government does not need to rely on the FOI system to respond to questions from the public. If you are asked how much the 6-mile bridge cost, and you have that number readily available – an FOI request is not needed. FOI should be viewed as a last resort to support the objectives of an accountable and transparent government. There are other mechanisms for supporting these goals – like responding to a question directly and releasing records proactively.



BRITISH COLUMBIA | Ministry of Citizens' Services

Ministries and IAO: A Partnership

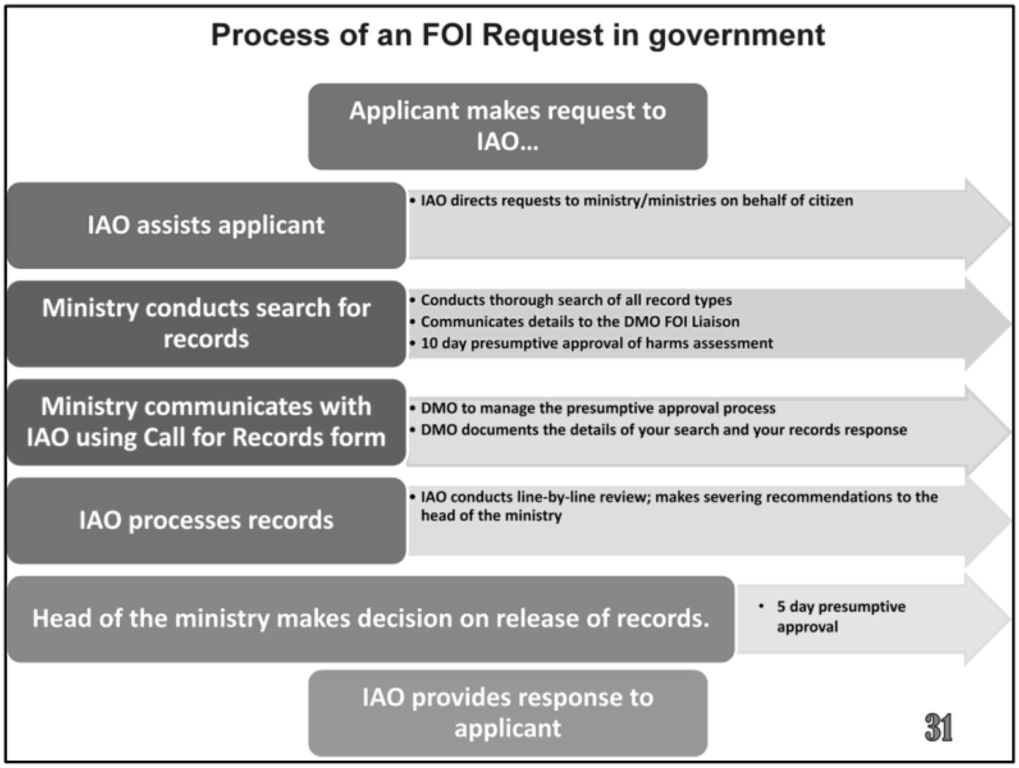
- **You are the knowledgeable owners of your records**
- **You are best-positioned to determine whether or not your records are responsive to an FOI request**
- **Information Access Operations (IAO) is government's FOI service provider**
- **IAO has the expert knowledge on how to apply FOIPPA and will provide advice and guidance to you about the application of FOIPPA**

Ministries and Information Access Operations work in concert to respond to FOI requests. As a member of the public service, you are the subject matter expert of your records. You know what you have and whether or not what you have is responsive to an FOI request. You also know what information may be harmful if released.

To be very clear, you are not expected to know what section of FOIPPA may apply in terms of removing that information, but you are in the best position to identify information if something may be harmful if it were released. You are responsible for ensuring that this information is communicated back to IAO. What IAO needs to hear, is "if this information about the location of spirit bear' dens was released, I would be worried that hunters and curious well-wishers would both go out looking for them and disrupt the habitat". You don't need to know that there is a legislative exception that may exempt that information from release.

IAO is the expert when it comes to processing FOI requests. They have the expertise required to apply FOIPPA , to manage the legislated timelines and to communicate with the applicant with a customer focus. IAO also possesses the technology required to effectively sever records.

Your DMO FOI Liaison is just that – your liaison to support communication between IAO and the Minister's Office.



Process of an FOI Request in government

Applicant makes request to IAO…

IAO assists applicant
- IAO directs requests to ministry/ministries on behalf of citizen

Ministry conducts search for records
- Conducts thorough search of all record types
- Communicates details to the DMO FOI Liaison
- 10 day presumptive approval of harms assessment

Ministry communicates with IAO using Call for Records form
- DMO to manage the presumptive approval process
- DMO documents the details of your search and your records response

IAO processes records
- IAO conducts line-by-line review; makes severing recommendations to the head of the ministry

Head of the ministry makes decision on release of records.
- 5 day presumptive approval

IAO provides response to applicant

31

This graphic provides a high-level overview of the FOI process for government. I'll go through this for you in a moment, but first I want to underline that the whole point of this process is to create a system that will ensure an effective, customer focused information access process.

When a ministry receives a request they have thirty days to respond to that request (unless an extension is requested and approved), so as I move through this process keep that tight timeframe in mind.

1. and 2: Those thirty days start the moment the FOI applicant makes a request to IAO, who acts on behalf of ministries. Next, IAO assists the applicant to direct the request to the correct ministries – For the Minister's office, your requests are communicated to you through your designated DMO FOI Liaison.

3 and 4: Next, your office has ten days to conduct a thorough and accurate search for records. We'll get into what is required of you in more detail as we move through the presentation. For now, know you are required to communicate your search details, the harms that you perceive, and the records - or a "no records" response to your DMO FOI Liaison.

Your DMO FOI Liaison will document all of that information on the Call for Records form and relay that back to IAO. To be clear, you are responsible for conducting your own search for records. Your DMO FOI Liaison is responsible for overseeing the search process, including directing, monitoring, confirming and reporting on progress.

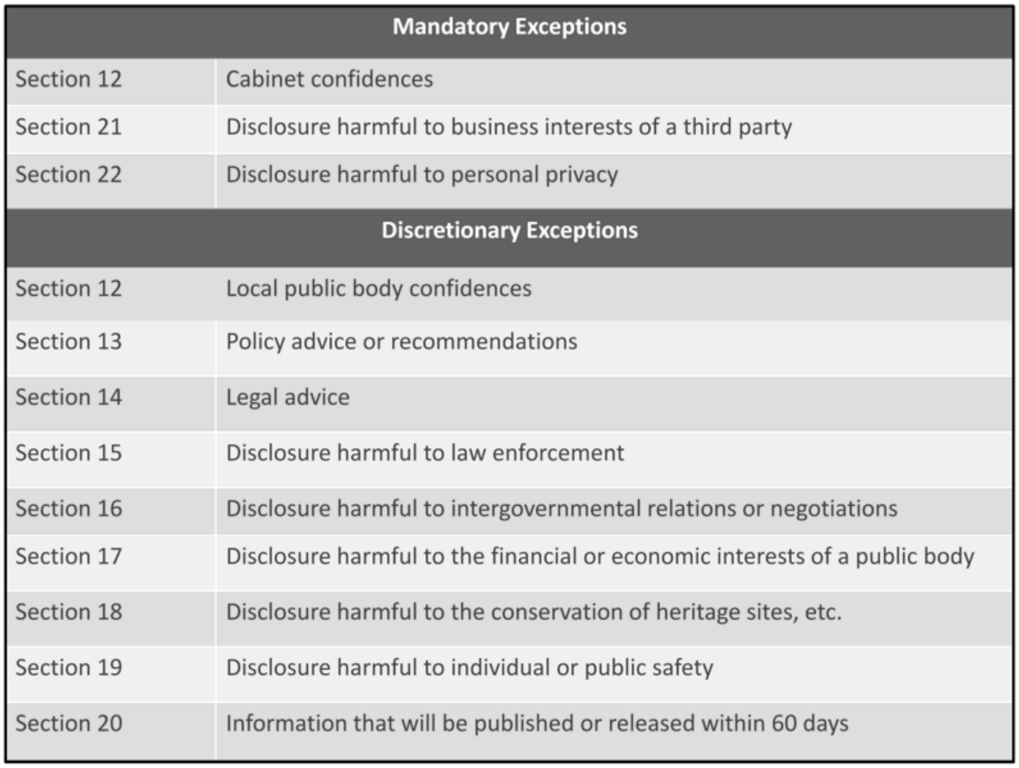
I want to flag something new for you here, and that is the presumptive approval process. Basically, that means that if you have provided records but have not provided formal harms or a formal approval within the ten days allotted by your DMO FOI Liaison, that person has the authority to proceed with the FOI process, presuming approval from your office.

It may seem senseless to provide records knowing that harms recommendations or approval is not achievable within the allotted 10 days. I would recommend that your office provide responsive records in any case, to avoid triggering the newly implemented escalation process, which I will explain in a moment.

5. Getting back to the process, IAO then has 10 days to use the information to assess and conduct a line by line review of the record with the harms you provided, keeping Part 2 of FOIPPA in mind. In order to do a harms assessment, IAO needs to understand your concerns related to the potential sensitivity of records. IAO will assess the potential application of the legislation to the areas you have flagged as potentially harmful.

6. Next, your DM, the ultimate decision maker when it comes to Access requests, has 6 days to make a decision on releasing information based on IAO's recommendations. Should records need to be reviewed or approved by your office within this timeframe, MOs will be given 5 days before the DMO FOI Liaison will presume approval.

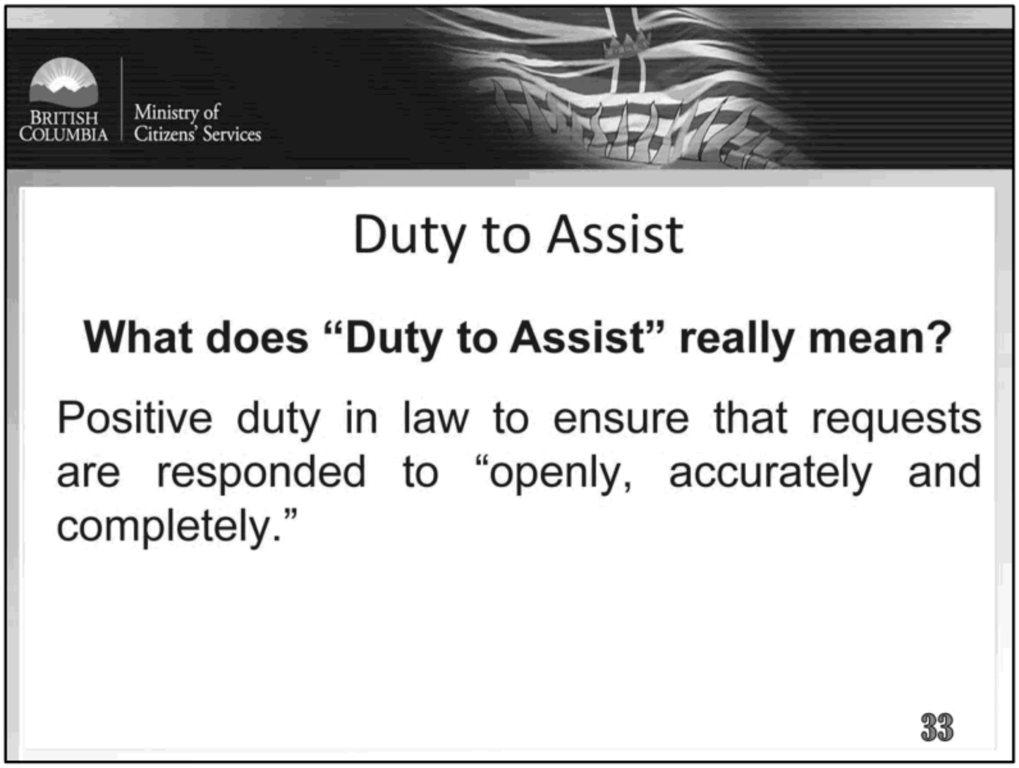
7. At this point, IAO has one day to release the appropriate records to the applicant.



Mandatory Exceptions	
Section 12	Cabinet confidences
Section 21	Disclosure harmful to business interests of a third party
Section 22	Disclosure harmful to personal privacy
Discretionary Exceptions	
Section 12	Local public body confidences
Section 13	Policy advice or recommendations
Section 14	Legal advice
Section 15	Disclosure harmful to law enforcement
Section 16	Disclosure harmful to intergovernmental relations or negotiations
Section 17	Disclosure harmful to the financial or economic interests of a public body
Section 18	Disclosure harmful to the conservation of heritage sites, etc.
Section 19	Disclosure harmful to individual or public safety
Section 20	Information that will be published or released within 60 days

Two of the steps I just mentioned – IAO conducting a line by line review of records, and the Deputy exercising their discretion about what information will be withheld and what information will be released – those steps are based on FOIPPA's legislated exceptions to disclosure. In other words, what you see on the slide are the reasons that a ministry can take out – or in other words, sever information prior to release. The first three items you see there, sections 12, 21 and 22 are **mandatory** exceptions. That means that the ministry must never release records that meet the rules of the sections related to cabinet confidences, third party business information or personal information that would represent an unreasonable invasion of a person's privacy.

The list of discretionary items you see there represent the other reasons a ministry may remove information prior to release. Sections 13 to 20 are discretionary – which means that you don't have to sever them. In fact, the default position **should be** to release that information. The question shouldn't be 'can we sever' but instead we should ask 'should we' or 'do we really need to' sever. Ultimately, this is a recommendation that will come from the experts at IAO and it is a decision that will be made by the DM.



British Columbia | Ministry of Citizens' Services

Duty to Assist

What does "Duty to Assist" really mean?

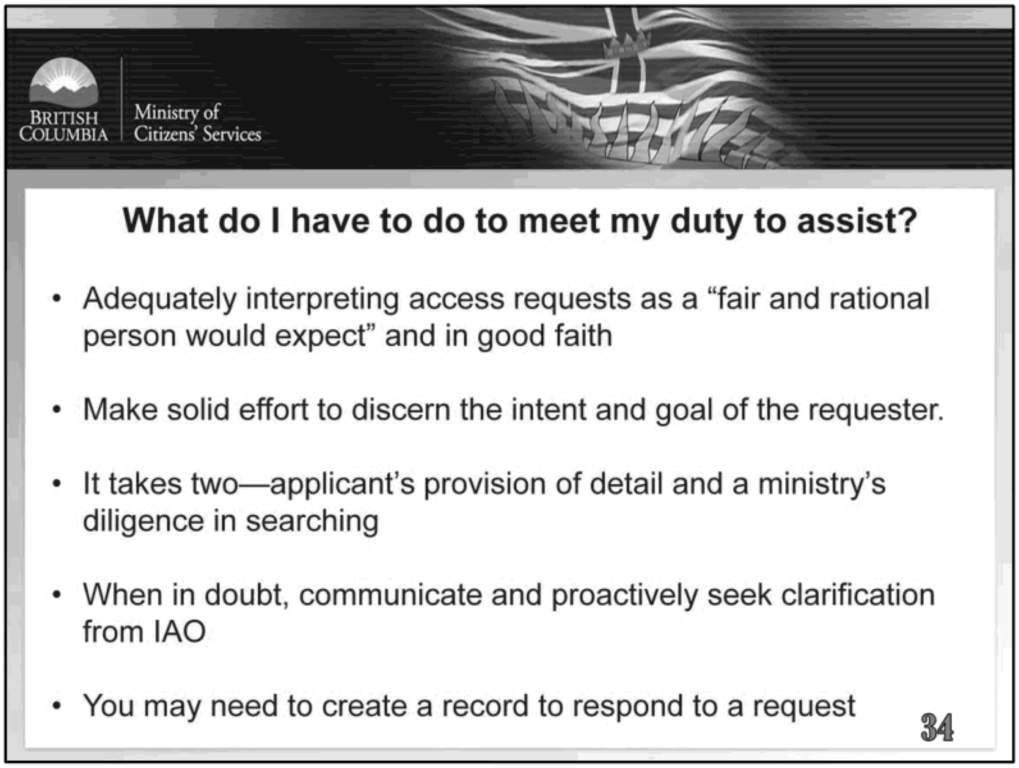
Positive duty in law to ensure that requests are responded to "openly, accurately and completely."

33

So, coming back to this term I used – duty to assist – all **government employee's** must make every reasonable effort to assist applicants and to respond to each applicant openly, accurately and completely in a timely way. After all, access to information is a foundational democratic principle.

The "duty to assist" goes beyond just meeting the letter of the law; it involves providing an excellent service experience to each applicant.

Take a moment and think about what **you** would like as a response if **you** were requesting your information from a publicly funded organization. I'm sure you can imagine that if you were the applicant you would appreciate a thoughtful, respectful and thorough customer service approach. You would want to feel that you **could** get the information that you needed. You know you have a right to access your information, and government wants to support that right with responsive customer service. Our legislated duty to assist provides us with an obligation to ensure we are embodying this perspective.



BRITISH COLUMBIA | Ministry of Citizens' Services

What do I have to do to meet my duty to assist?

- Adequately interpreting access requests as a “fair and rational person would expect” and in good faith
- Make solid effort to discern the intent and goal of the requester.
- It takes two—applicant’s provision of detail and a ministry’s diligence in searching
- When in doubt, communicate and proactively seek clarification from IAO
- You may need to create a record to respond to a request

34

To meet your duty to assist an FOI applicant, you need to adequately and liberally interpret access requests. This means steering clear of narrow interpretations, it’s about getting to the underlying intent of a request and understanding the request from the applicant’s point of view. You need to interpret requests in a manner that a “fair and rational person would expect”. You can be proactive and seek clarification from your DMO FOI Liaison if you are unsure about a request. What I mean by this is that if someone asks for a report authored by John Smith in 1998 and there isn’t one - but there is one for 1999 – Through your DMO FOI Liaison, you can request that IAO contact the applicant to ask if they actually wanted the 1999 report – or, to speed up the whole process, you could just provide the 1999 report. Similarly, if you know of records that exist in a different office, you should be indicating what those offices are.

I want to tie this concept of duty to assist back to something I mentioned earlier. You’ll remember that I noted that an applicant has to provide sufficient detail for an employee to be able to actually understand a request – And that’s true, but I think our duty to assist the applicant means that the burden doesn’t rest **solely** with the applicant. If we don’t understand something, let’s have a conversation. Let’s try to find out what the applicant is **actually** looking for. For you, that means you are going to relay your concerns or questions to your DMO FOI Liaison. They can work with IAO who can communicate that conversation directly to the FOI applicant.

We also have an obligation under FOIPPA to create a record in response to a request, where feasible. There are some conditions – for instance, creating the record shouldn't interfere with the operations of the ministry, but the test for that is pretty high in government. To show you what I mean – you can imagine that someone has asked for a record that doesn't exist exactly as they have requested it – but to create it all you would need to do is filter a few columns out of a spreadsheet. This is definitely an instance where you would create the record for the applicant. Alternatively, you can imagine that if someone requests access to millions of lines of metadata – this might not be something that your ministry could easily create or provide to an applicant.

The last thing I want to point out is that we need to use our common sense when a single ministry receives a request within government. If the applicant has directed it to the wrong ministry, let's tell them that. FOIPPA provides a mechanism for a ministry to transfer a request to another. So if someone has asked your office for records and you don't have them – but you know, or think another ministry does – let your DMO FOI Liaison know, they can contact IAO who is able to reach out to the other ministry and see if they do have records and in turn can support the applicant by getting the request to the right place.

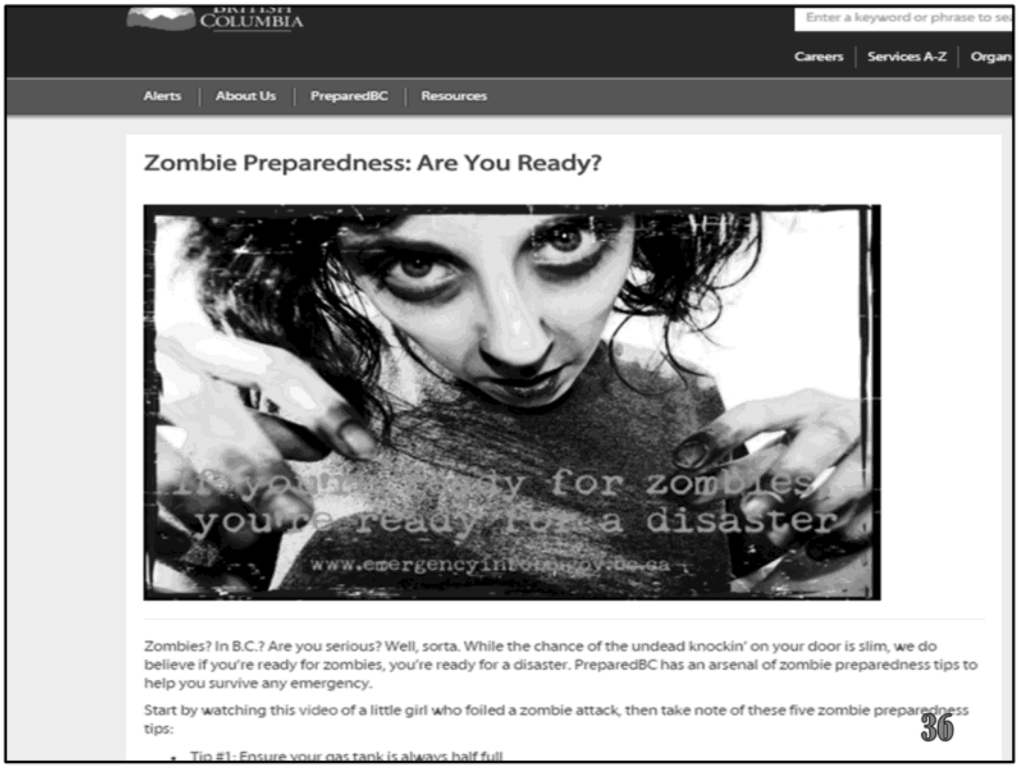
Copyright

This is a real life example of an FOI request that demonstrates how we can exercise our duty to assist an FOI applicant.

An FOI applicant wrote:
“Dear Leicester City Council,
Can you please let us know what provisions you have in place in the event of a zombie invasion? Having watched several films it is clear that preparation for such an event is poor and one that councils throughout the kingdom must prepare for.
Please provide any information you may have,
Yours faithfully.
Concerned citizen”

The Leicester FOI co-ordinator said “To you it might seem frivolous and a waste of time…but to different people it actually means something. Everybody has their own interests and their own reasons for asking these questions.”

This example illustrates how we can demonstrate our duty to assist and support citizens who are requesting information respectfully and in good faith. Regardless of how we may feel about this request. We do have a duty to assist. This request may seem laughable and like the individual is not taking things seriously, but let’s consider for a moment, that we receive this request in BC.


British Columbia
Enter a keyword or phrase to se
Careers
Services A-Z
Organ
Alerts
About Us
PreparedBC
Resources
If you're ready for zombies,
you're ready for a disaster
www.emergencyinfobc.gov.bc.ca

Zombie Preparedness: Are You Ready?

Zombies? In B.C.? Are you serious? Well, sorta. While the chance of the undead knockin' on your door is slim, we do believe if you're ready for zombies, you're ready for a disaster. PreparedBC has an arsenal of zombie preparedness tips to help you survive any emergency.

Start by watching this video of a little girl who foiled a zombie attack, then take note of these five zombie preparedness tips:

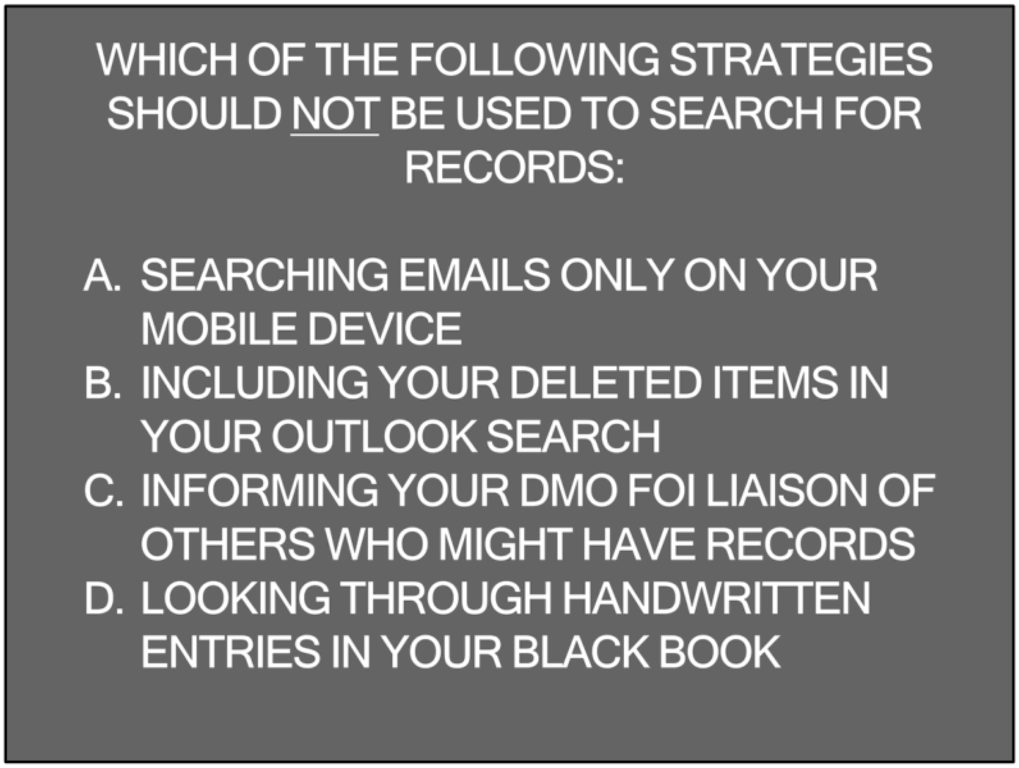
- Tip #1: Ensure your gas tank is always half full

If we were to ignore it, or not treat it seriously, we would be at risk of being offside our duties.

In BC, if someone were to make that same request they would receive real, zombie-related records. In fact, in 2012 there was a real request directed to Government Communications and Public Engagement for records related to Emergency Management BC's Emergency Preparedness campaign centred on zombies! As they say: If you're ready for zombies, you're ready for a disaster.

It is important to respectfully treat each request in good faith – we need to be thoughtful, respectful and helpful when we respond to FOI requests.

Source: https://www.emergencyinfobc.gov.bc.ca/zombie-preparedness-week-are-you-ready/



WHICH OF THE FOLLOWING STRATEGIES SHOULD NOT BE USED TO SEARCH FOR RECORDS:

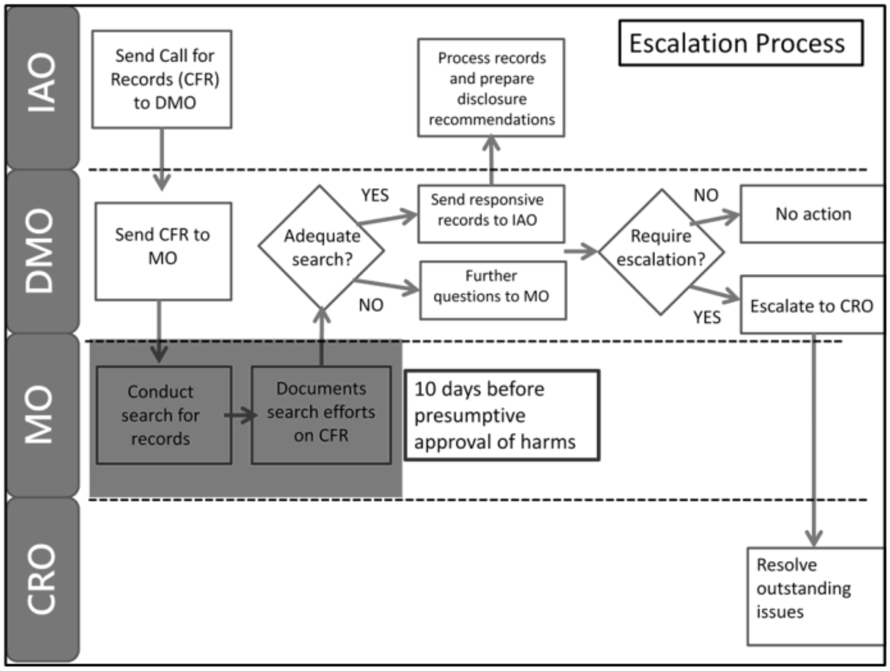
A. SEARCHING EMAILS ONLY ON YOUR MOBILE DEVICE
B. INCLUDING YOUR DELETED ITEMS IN YOUR OUTLOOK SEARCH
C. INFORMING YOUR DMO FOI LIAISON OF OTHERS WHO MIGHT HAVE RECORDS
D. LOOKING THROUGH HANDWRITTEN ENTRIES IN YOUR BLACK BOOK

Read before quiz: One of the ways that we can **really demonstrate** that we are working to support applicants and meet our duty to assist is when it comes to searching for "responsive records". "Responsive records" – when we're talking about FOI - just means the records that respond to an FOI request.

Which of the following strategies should not be used to search for records?

- Searching emails on your mobile device
- Include your deleted items in your Outlook search
- Inform your FOI coordinator of other people you think might have records
- Look through handwritten entries in your "black book" for responsive records

The answer here is A – it is not a complete search if it was only conducted on your mobile device. You also need to search on your desktop and any personal device you may have conducted government business on. It is simply ineffective at doing a complete search. This means that the other options are TRUE. You do have to search your deleted items in your Outlook folder.
You are obliged to provide handwritten notes in response to an FOI request. **and**
You should inform your DMO FOI Liaison of others who may have records – whether that means colleagues in your office, division or ministry – or if you know another ministry would have records.


Escalation Process
IAO
DMO
MO
CRO
Send Call for Records (CFR) to DMO
Process records and prepare disclosure recommendations
Send CFR to MO
Adequate search?
YES
NO
Send responsive records to IAO
Further questions to MO
Require escalation?
NO
YES
No action
Escalate to CRO
Conduct search for records
Documents search efforts on CFR
10 days before presumptive approval of harms
Resolve outstanding issues

As I just mentioned, an adequate search for records is one of the most important things you can do to support government in meeting our Access obligations.

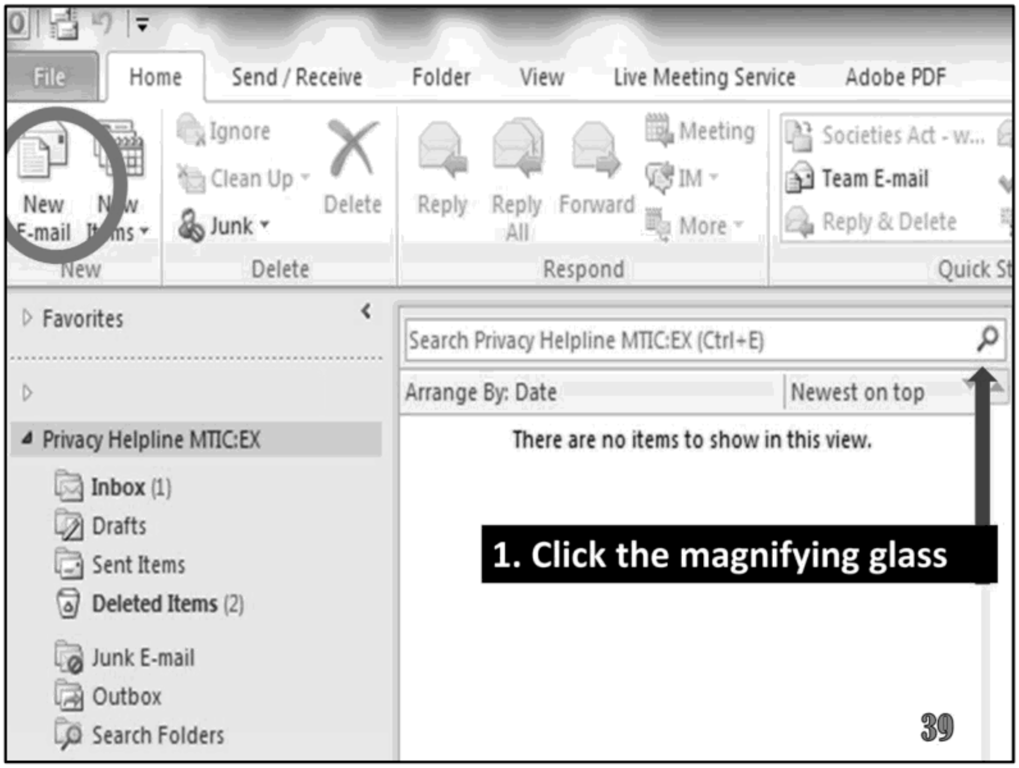
You are responsible for searching anywhere you or your office has stored recorded information, that includes your email, any SharePoint sites, your network drive, your electronic systems and devices and physical storage such as your desk, cabinet or notebook. You are the expert, you should **know** where the records are kept. And if you don't know you should ask someone who would. You also should be able to take a common sense approach here – if you don't have records, but you know your colleague does – document that detail so that your DMO FOI Liaison is able to ensure your colleague receives the request for records.

It is your responsibility to communicate your search efforts **clearly** to your DMO FOI Liaison. Your DMO FOI Liaison is responsible for overseeing the search process and must be able to clearly **document** who has received and who has responded to the request and all the search details on the Call for Records form that is sent back to IAO. The details on searching – including, the search terms that were used and the search methodology - need to move clearly through the chain of command to ensure that we aren't playing a game of broken telephone.

The swimlane you see on the screen represents the various roles and some of the responsibilities of the players involved in responding to one of your FOI requests. As we know, IAO receives the request from the applicant. The DMO FOI Liaison is the role that will liaise between your office and IAO. They are your point of contact for supporting you in ensuring you have a clear understanding of the request and of what is required of you in responding to the request. They also are available to support IAO in ensuring they have the information they need from your office. This includes getting your records of course, but also includes documenting the details of your searches and information that explains why there are no records if you submit a no records response.

It is an expectation across government that IAO be able to provide evidence that a thorough and comprehensive search has been conducted – if you don't relay the details of your efforts this becomes very challenging for IAO. It is also important that if you are submitting a response that indicates there are no records, you need to clearly communicate why there are no records, other sources for the records and other available records that are similar to what the applicant has requested. There is a big difference between "the Minister's Office has no records on this issue" and "the Minister's Office has no records on this issue, **because** it arose when the Minister was in Ottawa, so issues were addressed by the Deputy".

In the event your office responds to an FOI Request with a no records response, you should know that your DMO FOI Liaison is responsible for engaging in a formal escalation of that file. The DMO FOI Liaison will review the request and the no records response. There are times when a no records response may be appropriate, like in the example I just gave – or if the Minister for Children and Family Development receives a request for records related to the numbers of hunted Bear in BC - it is likely that they would reply by explaining that they have a 'no records response' . The DMO FOI Liaison would reach back to you in the Minister's Office for more information. In this case it is likely that you could avoid escalation by providing a more fulsome response explaining that the applicant should be redirected to the Natural Resource Sector. However, in a more complicated file, if the Minister's Office did not include an explanation as to why there are no records, or a recommendation for where records may be located, the DMO FOI Liaison will initiate an escalation process. This process would raise the profile of the file from the DMO FOI Liaison to your ministry's Deputy Minister. Your DM may bring that file to the Chief Records Officer, who may in turn escalate the process directly to the Minister of Citizens' Services.



There are no items to show in this view.

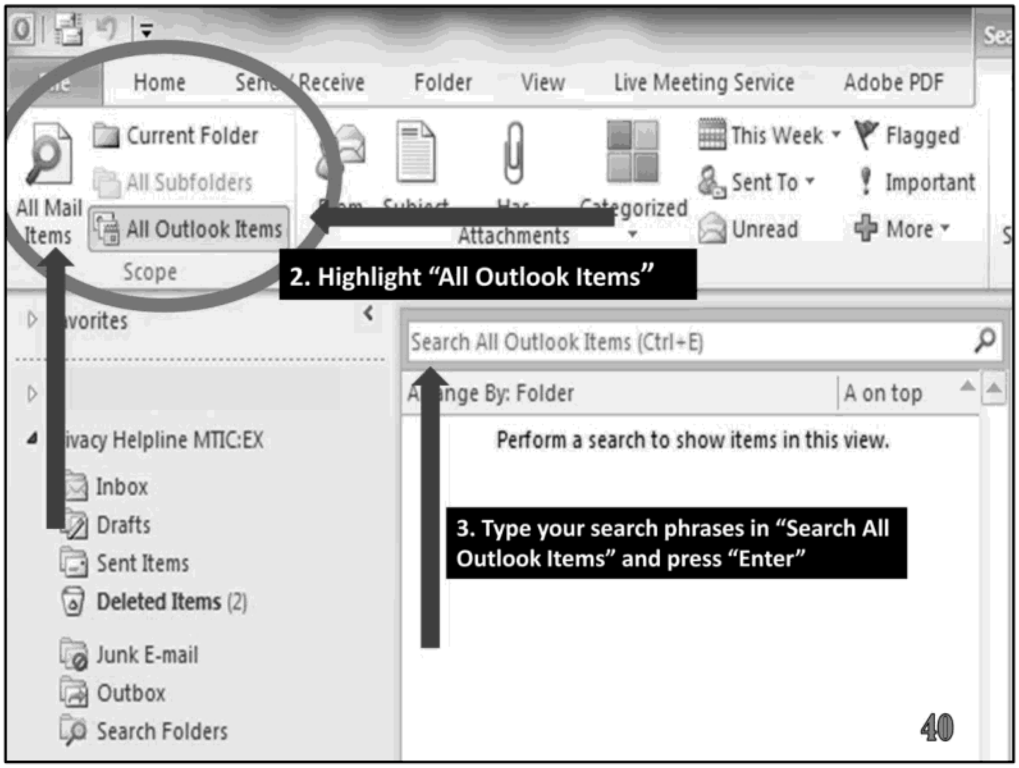
1. Click the magnifying glass

To help you get a leg up on an email search, I'm going to walk you through what a proper search in your Outlook folder should look like. To be clear, your email is only one place you need to search for records. But, I think this is a useful tip that not everyone necessarily knows about. It also demonstrates the attention that needs to be paid when you are conducting your search in other areas – like your LAN, your technical systems and your physical records.

I know we have talked about this, but I want to reiterate that searching your Outlook cannot be done only from your mobile device and must also be done from your computer. An Outlook search must include **all of your folders**, not just your inbox. And, you do need to search the deleted items folder that is contained within your Outlook account.

Okay, so getting technical for a moment - I'll draw your attention to the "New E-mail" button – just take note of it because it will change in a moment.

The first thing you need to do for a thorough search is to click the magnifying glass, which you can see in the top right of the screen here.



2. Highlight “All Outlook Items”

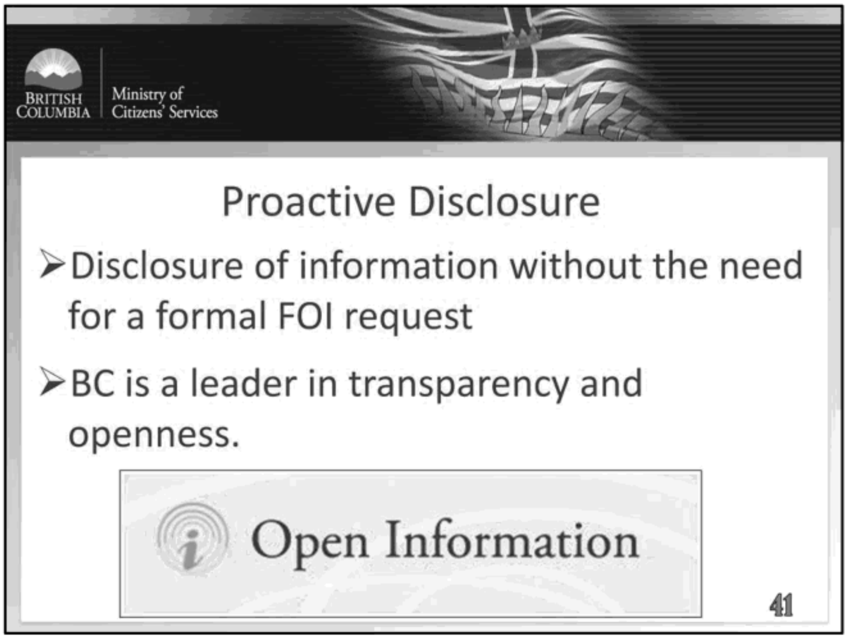
3. Type your search phrases in “Search All Outlook Items” and press “Enter”

When you click the magnifying glass, you can see (in the top left corner), the “New E-mail” button changes to “All Mail Items”.

Next, you need to ensure you have “All Outlook Items” - again in the top left, is selected. This is not the default selection, so you have to manually select it. Now you can type your search phrases in to the “Search All Outlook Items” field and press “Enter”.

This type of search will produce all the Outlook items responsive to the request – not just the items in your inbox!

Remember, you should be using a set of fulsome search terms. Don’t just search what the applicant has asked. You need to use your expertise and insider knowledge of your own records to find everything that may respond to a given FOI request. If you are searching for records relating to an event that took place in New Zealand, maybe include “Kiwi” “paradise” or “NZ” as search terms, and not just “New Zealand”, because that won’t necessarily bring up all the responsive records. Make sure you document the search terms you used and communicate that to your DMO FOI Liaison.



BRITISH COLUMBIA | Ministry of Citizens' Services

Proactive Disclosure

- ➢Disclosure of information without the need for a formal FOI request
- ➢BC is a leader in transparency and openness.

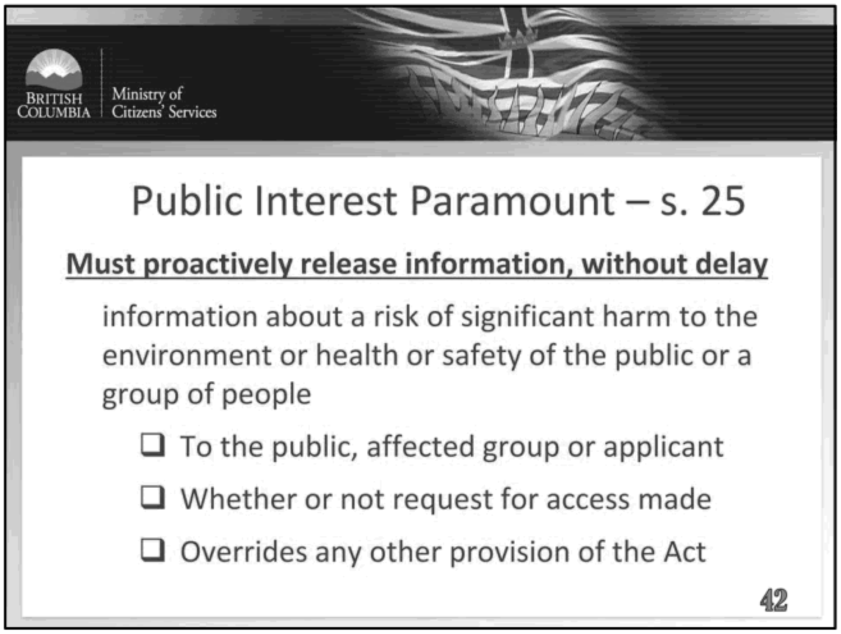
Open Information

41

We’ve talked a little about some very granular practices with respect to FOI, but it is important not to lose sight of the government-wide context.

- Proactive disclosure is the disclosure of information without the need for a formal FOI request. You may have also heard this referred to as “routine release”.
- There are lots of examples of proactively disclosed information. For one, BC’s Open Information site, which contains thousands of proactively disclosed records. There is also the BC Data catalogue which contains thousands of high-quality datasets.
- Corporately, we currently proactively release summaries of community gaming grants, Minster’s receipted travel expense information, and summaries of FOI requests, calendars, summaries of contracts over $10,000 and direct awards, and more.
- FOIPPA requires all ministers to establish additional categories of recorded information that can be proactively disclosed.

Other disclosures are more casual – you might give the general public non-personal and non-sensitive information over the phone, or via a website. Not all disclosures are repeatable -- and that’s okay. Sometimes a disclosure is a one-off. Any information a ministry makes available on its website, or when citizens call a hotline or come to a service counter is a proactive disclosure. Each time we do this, we contribute to citizens receiving the information they’re interested in, more efficiently.



BRITISH COLUMBIA | Ministry of Citizens' Services

Public Interest Paramount – s. 25

Must proactively release information, without delay

information about a risk of significant harm to the environment or health or safety of the public or a group of people

- □ To the public, affected group or applicant
- □ Whether or not request for access made
- □ Overrides any other provision of the Act

42

- While we are on the topic of proactively releasing information, it is important to address s.25 of FOIPPA. Section 25 is a public interest override which dictates that despite anything else, and regardless of whether it has been requested, the head of a ministry must disclose information about a risk of significant harm to the environment; or to the health or safety of the public or a group of people; and any other information which is clearly in the public interest. This release must happen without delay.

- Examples include, records that would indicate:
  - The accidental release of a pesticide into a stream, which will affect fish and other aquatic life.
  - The presence of a norovirus in the public drinking water.
  - A natural gas leak which could cause an explosion in a populated area.

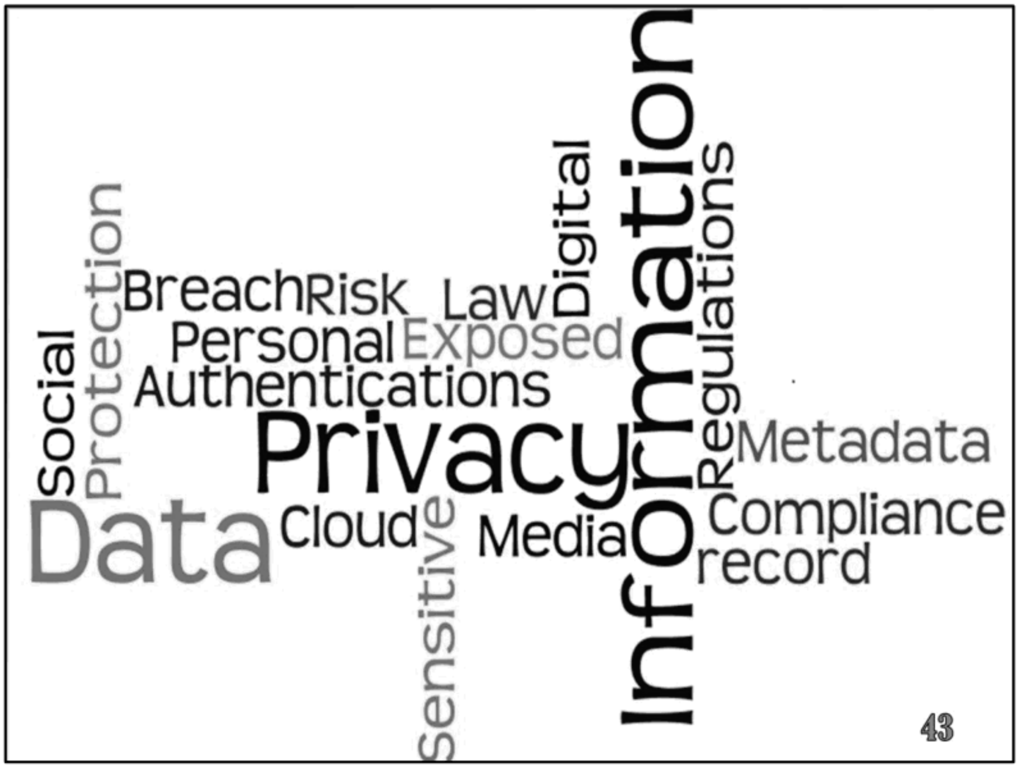
- Past interpretations by the OIPC and government of this section included a requirement for urgency. This meant that government was disclosing information via section 25 only when the information related to an imminent matter. "This bridge is about to collapse" vs. "This bridge may collapse in the next 5 years".

- Following the Commissioner's 2015 investigation into the lack of information released regarding the Mount Polley mine tailings pond, the Commissioner released a report which stated that section 25 should not be interpreted to require an element of urgency in order to require the disclosure if it is clearly in the public interest.

- The standard now is: where a disinterested and reasonable observer, **knowing what the information is** and **knowing all of the circumstances**, would conclude that disclosure is obviously in the public interest.

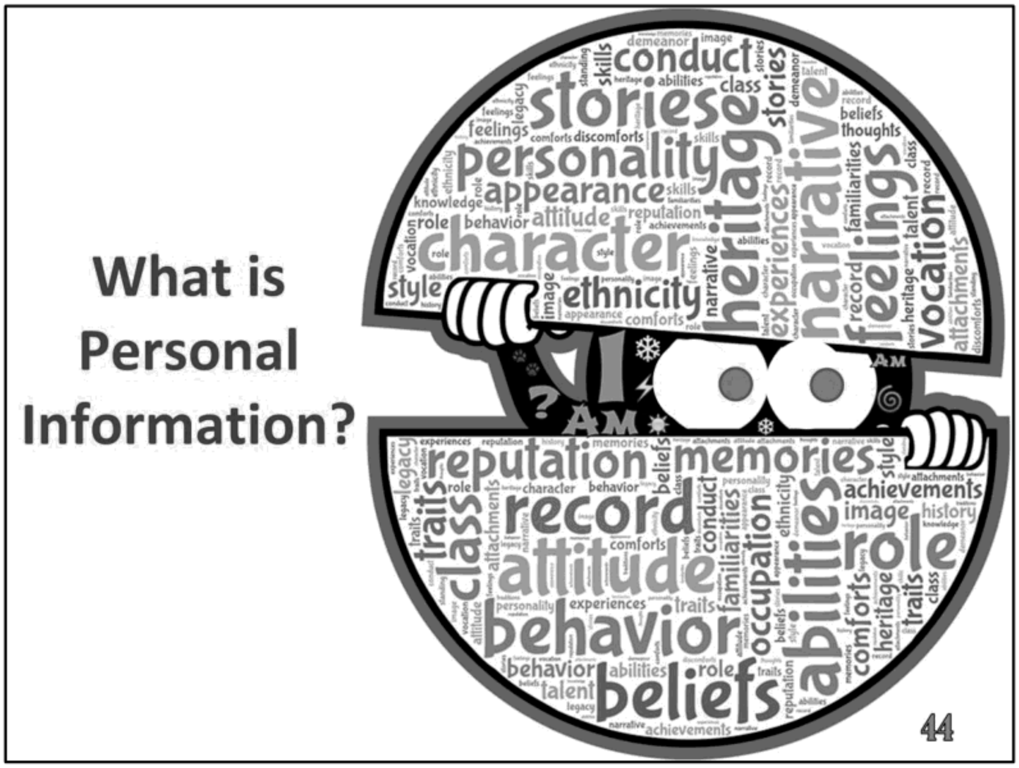
- Following a recent 2016 OIPC Investigation into the lack of records released regarding nitrate levels in the Hullcar aquifer in Spallumcheen, it is clear from the Commissioner that the requirement is not just that the public be notified of an issue in the public interest, but also that the records that relate to the issue be publically released.

- This is important for you to know as you may be asked to approve of this kind of release and need to know the robust legal impetus for you to release those records.



We have spent the last little bit focusing on openness and transparency as a means of demonstrating accountability, but protecting personal information or personal privacy is another way we need to demonstrate accountability. Accountability to citizens and their information.

Part 3 of FOIPPA is the part of the Act that addresses the privacy and the protection of personal information. It does this by restricting the purposes for which you can collect, use or disclose personal information.



What is Personal Information?

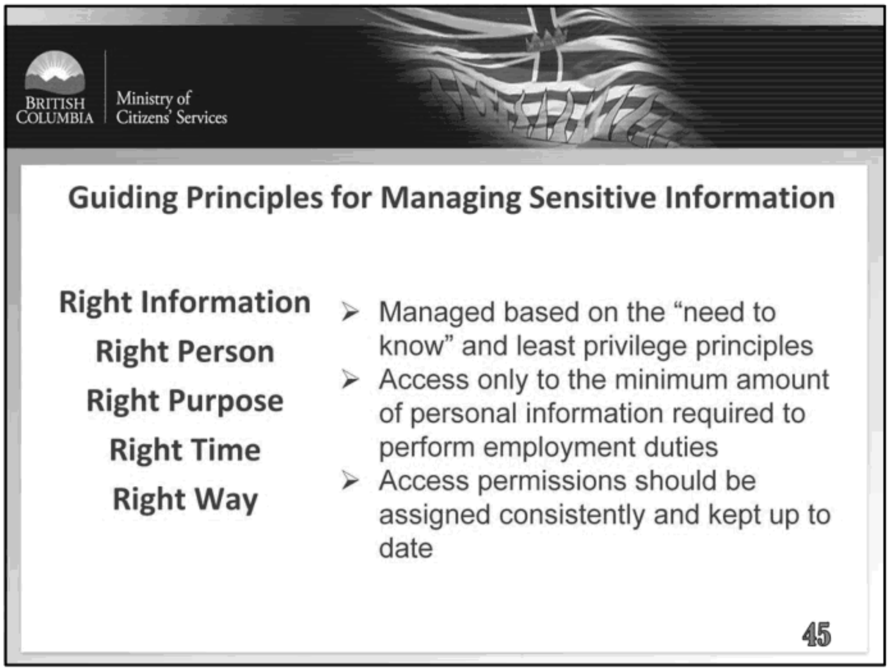
Personal information is an important term to have a clear understanding of, as privacy is all about the protection of personal information.

Personal information is defined as recorded information about an identifiable individual other than "contact information" A citizen's contact information is considered their business contact, when that information is used to connect with them in their business capacity. Essentially, their business card, as long as they are handing it out for business reasons.

But everything else about the citizen as an identifiable individual is their personal information. This would include their name, their home address, their voting habits and their DNA – perhaps the obvious examples. But it would also include information about their educational history, employment history, health history **and even their personal opinions**. In the context of your work, you're most likely to come across personal information of a constituent or person seeking government services and, the employee information of the people in your office.

There are two caveats here, first, if you have a bunch of disparate, non-personal elements of information that individually don't identify you, but taken as a whole could work to identify you, then those would become personal information. This is what we call the mosaic effect. **For example,** information about what kind of car an individual drives, their age or their hometown may not identify anyone if they are 30 and drive a Civic in Vancouver. However, if they are 80, and drive a Rolls Royce in Spuzzum, BC, then it is more likely to be able to identify them – so, context is important.

Second, it is important to consider context, because in a different context, information can be either personal or business contact. For instance, if I run a professional day care out of my home, then my address could be both personal and business related. If I use my address to order a shipment of diapers for the daycare, then it is business contact, but if I use my address to register for a home owner grant, then it is personal.



BRITISH COLUMBIA | Ministry of Citizens' Services

Guiding Principles for Managing Sensitive Information

Right Information
Right Person
Right Purpose
Right Time
Right Way

- ➢ Managed based on the "need to know" and least privilege principles
- ➢ Access only to the minimum amount of personal information required to perform employment duties
- ➢ Access permissions should be assigned consistently and kept up to date

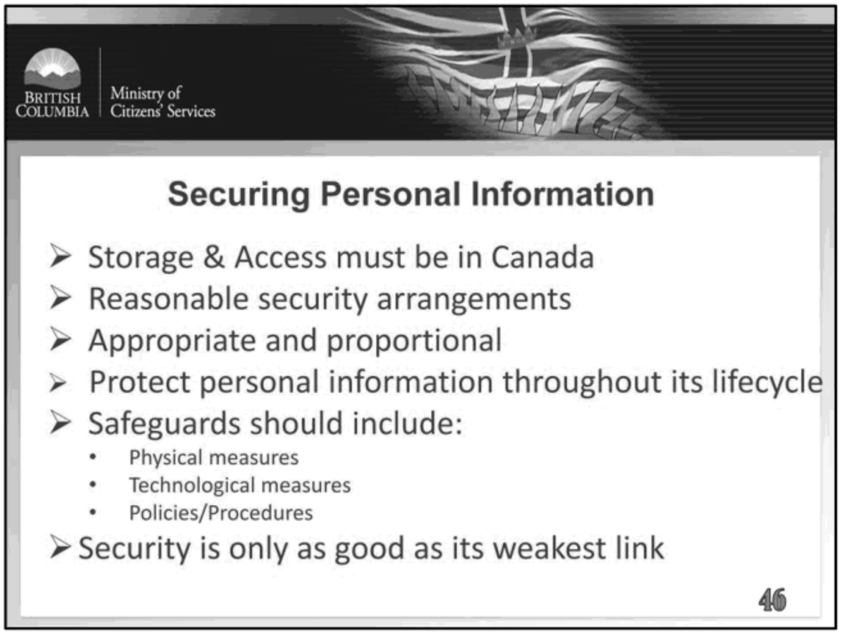
45

We don't have time to do a walk through of every provision of FOIPPA – that would take a week. But we can discuss, and more importantly, you can remember, this very simply mantra – Right Information; Right Person; Right Purpose; Right Time; and Right Way. These are the things you need to consider when you are collecting, using, and disclosing personal information. Am I sharing it with the right people, and only the right people? Should I be sharing this information over Facebook, or is it more appropriate that I share it over email?

Some of the practices that we can pull out of this mantra would include managing information on a need to know – not a nice to know basis. Accessing, using, or disclosing the minimum amount of personal information necessary, and managing and auditing access permissions.

An example that I like to use to demonstrate these guiding principles is that of a border agent that I read about. Generally speaking, he was a good worker and accepted passports and other information in order to process people through customs. He did this securely, while at his booth at the border in order maintain border security. All good according to these principles. However, one fateful day, a very attractive citizen came through his booth, and he did the same thing he always did….with one notable exception. He took the information he had from that interaction and used it after hours in order to message the citizen on Facebook. Dating was not the right purpose. Facebook was not the right way. After hours was not the right time. He basically failed on each of these guiding principles. He was not the right person, for the citizen or for that job apparently. Now, not every example of wrong is going to be wrong for each principle, so consider each principle here when you are collecting, using or disclosing personal information.

If you need support in determining in applying these guiding principles – your ministry has an MPO – Ministry Privacy Officer – who can support you.



BRITISH COLUMBIA | Ministry of Citizens' Services

Securing Personal Information

- Storage & Access must be in Canada
- Reasonable security arrangements
- Appropriate and proportional
- Protect personal information throughout its lifecycle
- Safeguards should include:
  - Physical measures
  - Technological measures
  - Policies/Procedures
- Security is only as good as its weakest link

46

FOIPPA's security provisions are fairly straightforward. There are two things you need to know:

1. Storage and access to personal information must be within Canada. There are exceptions to this rule, but you will want to take as a default that personal information needs to stay within Canada. This has implications with some cloud services like DropBox, Slackmail or social media platforms. There are cases where it is okay to use these services, but you should get your privacy sense tingling, and you should dial in the Privacy Helpline to make sure you are on side. Further, these services may complicate the FOI process and so you should remember that these records are still FOIable.

2. Next, you have to ensure reasonable security arrangements. What does reasonable mean? It means that the security around personal information must be appropriate and proportional to its sensitivity. So, if the personal information in question is someone's lunch order, it would probably be sufficient to simply put it in your pocket and not share it. However, if the information is someone's health information, including a drug screen and a list of all of their current medical conditions, then that is information that needs to be encrypted, password protected, locked up with controlled access and ensuring access is logged and audited.

When you are thinking about security, you want to think about it in 3 different ways – what physical security measures have you taken, what technical measures have you taken and what policy or procedural measures have you taken?

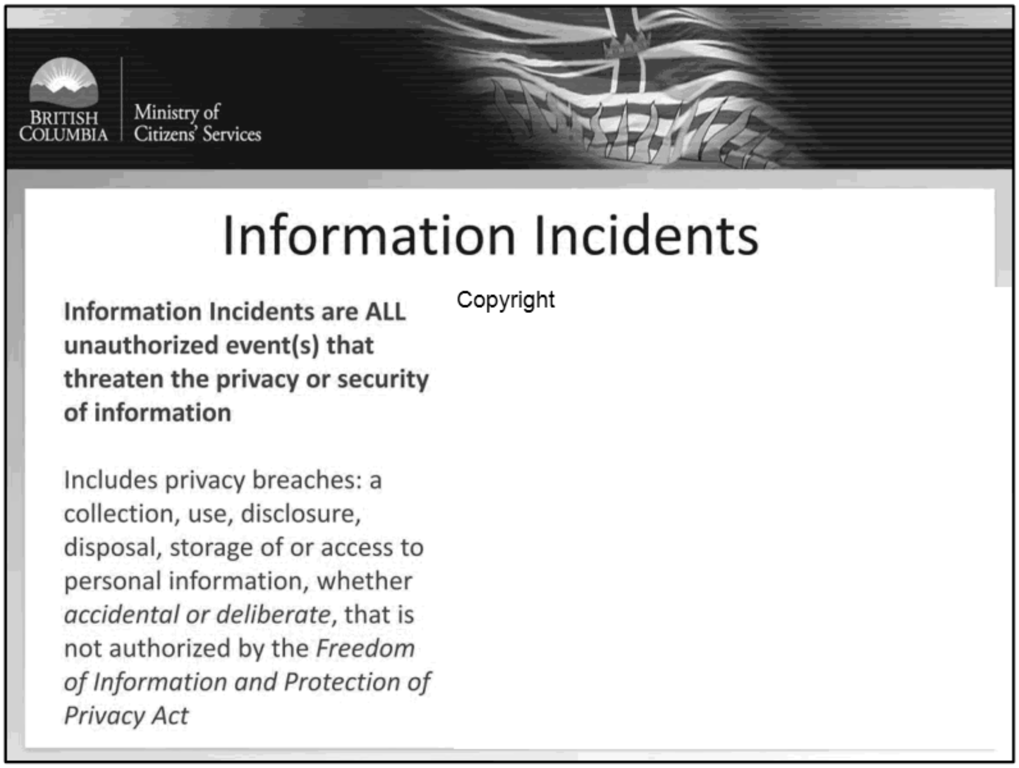
In terms of physical security, think of locking cabinet doors, having a security guard, locked offices, and privacy screens.

With respect to technical security, think about encryption, passwords, audit logs and access controls.

For policy or procedural security, this is where you try to fill in the gaps between technical and physical security. Perhaps a policy that requires you to not leave your keys in your locked cabinet, and to not tape your password to your desk.

Many overarching policies around securing and managing government information are set at the corporate level through the Core Policy and Procedures Manual, the Appropriate Use policy, and other related policies. You should contact the IM IT Policy email inbox if you need help in applying these policies. There may be additional need to develop intra-office policies specific to your work, and these should align with and enhance the “motherhood” corporate policies requirements.

For example, the corporate policies make general statements but don’t tend to go into specifics about procedure. So, if your office receives and saves a lot of correspondence, are you using personal information in the document titles or document names when saving them? This is something you should avoid, and can do so by setting a document naming policy.



BRITISH COLUMBIA | Ministry of Citizens' Services

Information Incidents

Information Incidents are ALL unauthorized event(s) that threaten the privacy or security of information

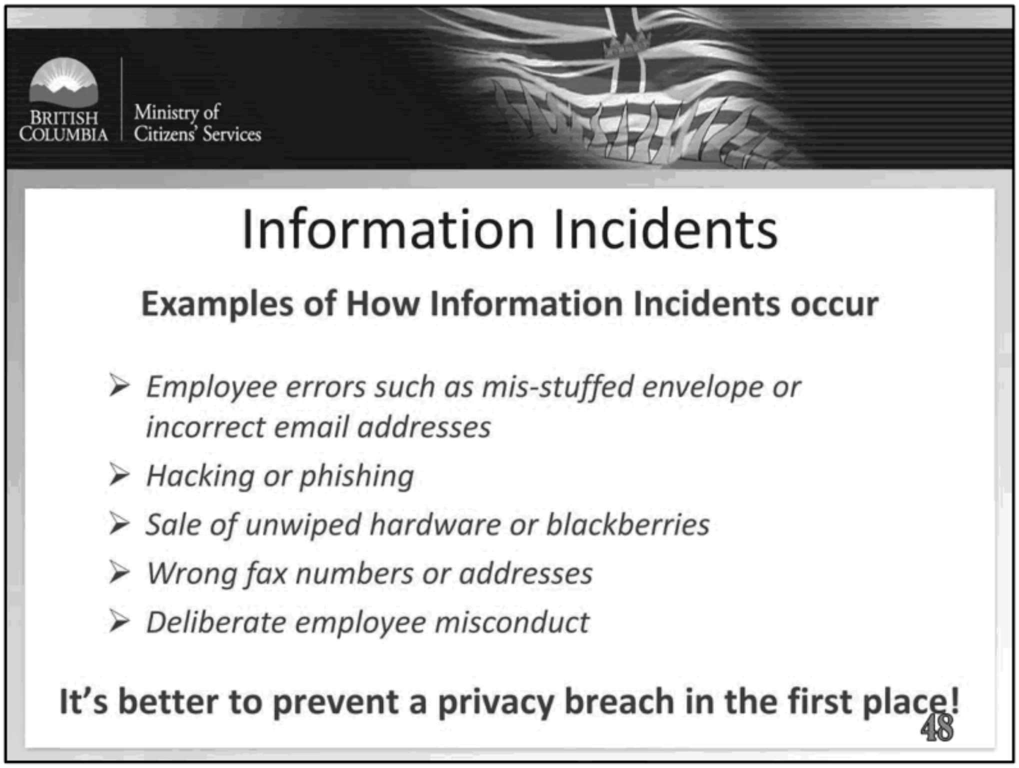
Includes privacy breaches: a collection, use, disclosure, disposal, storage of or access to personal information, whether *accidental or deliberate*, that is not authorized by the *Freedom of Information and Protection of Privacy Act*

Copyright

Information Incidents are ALL unauthorized event(s) that threaten the privacy or security of information

Information incidents include privacy breaches: a collection, use, disclosure, disposal, storage of or access to personal information, whether *accidental or deliberate*, that is not authorized by the *Freedom of Information and Protection of Privacy Act*

You can consider an event as a privacy breach, anytime someone sees some personal information they shouldn't have. This can be minor, such as receiving an email by mistake, or this can be more significant, like someone snooping around a system to find out information on their daughter's sketchy new boyfriend. You can't quite predict what the impact of a breach is going to be, regardless of whether it is small or large, accidental or deliberate. So we have to treat them all as incidents to start.



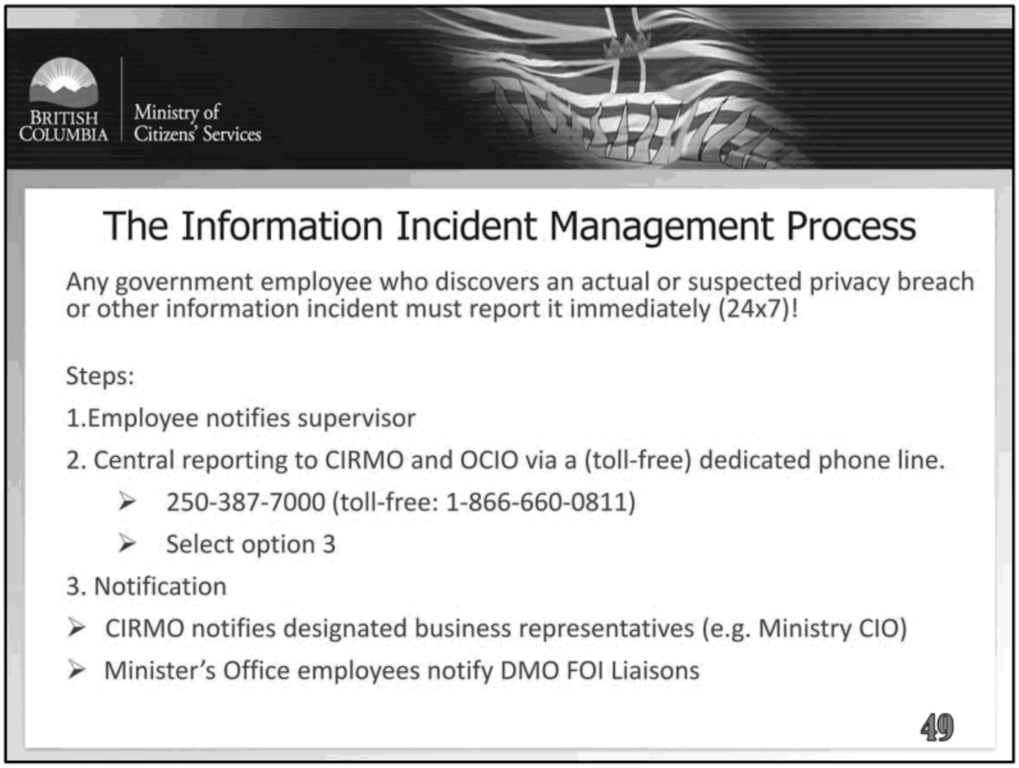
BRITISH COLUMBIA | Ministry of Citizens' Services

Information Incidents

Examples of How Information Incidents occur

- ➢ *Employee errors such as mis-stuffed envelope or incorrect email addresses*
- ➢ *Hacking or phishing*
- ➢ *Sale of unwiped hardware or blackberries*
- ➢ *Wrong fax numbers or addresses*
- ➢ *Deliberate employee misconduct*

It's better to prevent a privacy breach in the first place!



BRITISH COLUMBIA | Ministry of Citizens' Services

The Information Incident Management Process

Any government employee who discovers an actual or suspected privacy breach or other information incident must report it immediately (24x7)!

Steps:

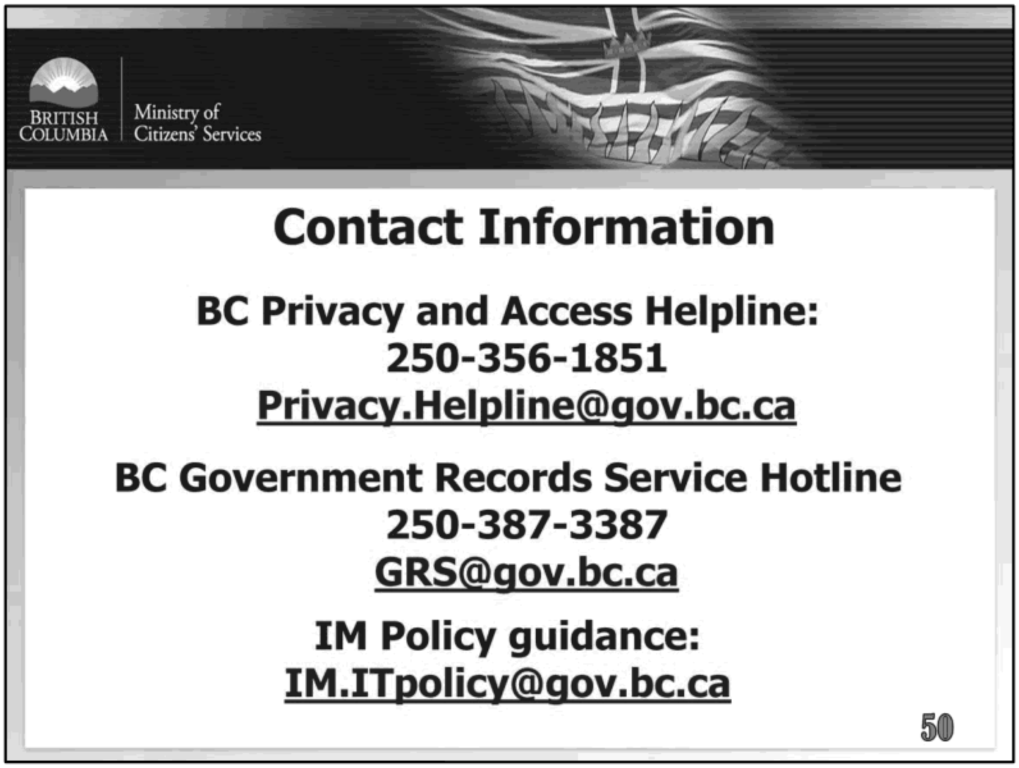
1.Employee notifies supervisor

2. Central reporting to CIRMO and OCIO via a (toll-free) dedicated phone line.

   - 250-387-7000 (toll-free: 1-866-660-0811)
   - Select option 3

3. Notification

- CIRMO notifies designated business representatives (e.g. Ministry CIO)
- Minister's Office employees notify DMO FOI Liaisons



BRITISH COLUMBIA | Ministry of Citizens' Services

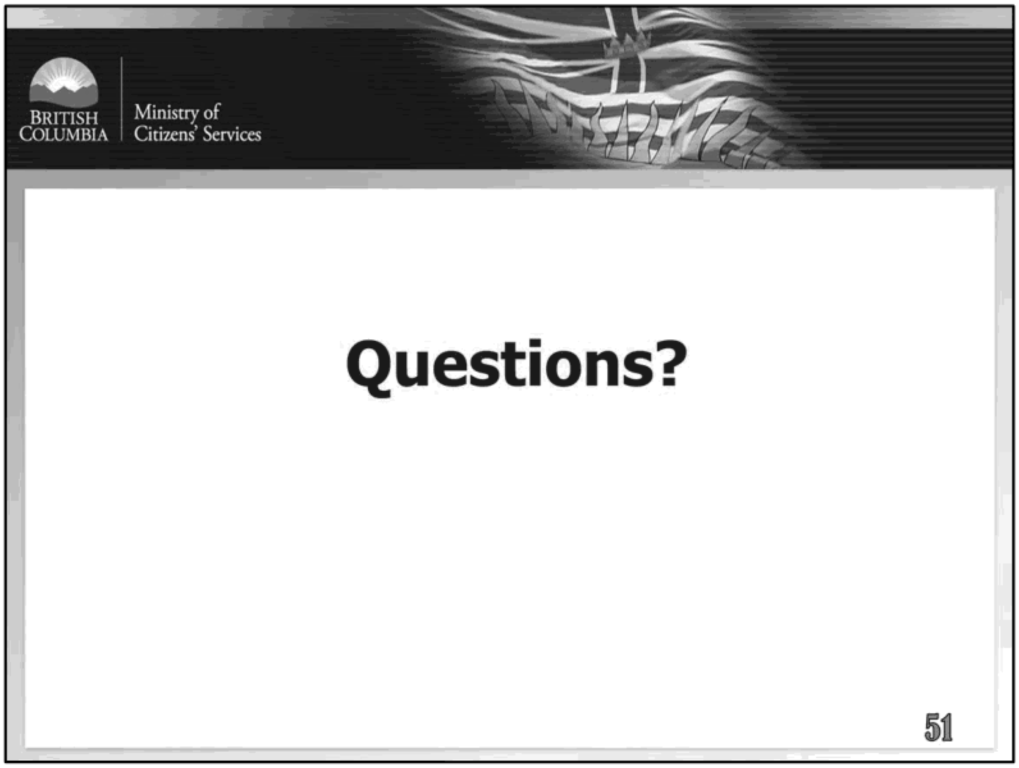
Contact Information

BC Privacy and Access Helpline:
250-356-1851
Privacy.Helpline@gov.bc.ca

BC Government Records Service Hotline
250-387-3387
GRS@gov.bc.ca

IM Policy guidance:
IM.ITpolicy@gov.bc.ca

50



BRITISH COLUMBIA | Ministry of Citizens' Services

Questions?

51

British Columbia

Ministry of Citizens' Services

British Columbia

From: Curtis, David FIN:EX
To: Hoskins, Chad FIN:EX; Reed, Matt FIN:EX
Subject: MO Guides & Training Links
Date: Tuesday, July 25, 2017 5:38:03 PM
Attachments: Managing Government Calendars.pdf
Managing Minister s Office Records - Updated 2017-07-11.pdf
Best Practices when Leaving a Ministers Office.pdf

Hi,
I would appreciate your review of the following training materials from GRS – to make sure we are consistent with the emerging training materials. If possible I would appreciate the return of any comments, concerns that you might have by 10:00am tomorrow.
Thanks and sorry for the tight timeline.

Regards,

David
****

Guides

GRS has two published guides specifically for Ministers' Offices (both attached):
Managing Ministers' Office Records, and
Best Practices when Leaving a Ministers' Office
I have also attached a "Managing Government Calendars" document that covers best practices for managing calendars.
Numerous additional guides can be found on the Government Records Service website.

Courses

Several online, self-directed courses are available via the PSA's Learning System, including:

- IM 117: Protection of Privacy, Access to Information and Records Management (ITEM-652)
- IM 110: Managing Our Information Assets (ITEM-56)
- IM 112: Managing Government Records (ITEM-41)
- LAN Organization (ITEM-158)
- Email and Records Management Best Practices (ITEM-570)

These courses can be taken at any time and we would recommend starting with IM117.
To learn more about these courses and to register, visit the Learning System and search for a course by its title or item number.
In addition, we are more than happy to deliver custom, in-person training.
For more information, visit the Government Records Service website or contact Richelle Wright, the Ministry of Citizens' Services Records Officer.

GOVERNMENT RECORDS SERVICE GUIDE

BEST PRACTICES WHEN LEAVING A MINISTER'S OFFICE

This material complements the more detailed *Departing or Transferring Employees Guide.*

Overview

Government information created and used by British Columbia's cabinet ministers and their staff is a valuable public asset and must be managed in a manner consistent with policy, information schedules and Standards of Conduct.

All of the official records, that are required to be retained, must be retained by the responsible authority (office of primary responsibility) when individuals transfer to another office or leave government. Managing all digital and physical information appropriately as part of regular office practice will make it easy to transition when you leave.

Six Key Practices

1. **Manage government information separately from non-government information.** When you leave, you can take personal records with you. If you are an MLA, you may also take your MLA records (i.e., constituency records). Government records must be retained according to information schedules and continue to be available to serve the ongoing needs of the ministry.

2. **Ensure official records are sent to the appropriate responsibility centre or filed appropriately.** What does this mean? See the following bullets and check out *Appendix A: Minister's Office Records Processes*.

   - **Official records** are those that document substantive activities, decisions and decision making processes of the office. They include the master or file copies of records documenting the performance of minister's office functions or the running and administration of the office itself (e.g., email and attachments, other executive correspondence, final reports, minutes).

What can you take with you?

- Personal records
- Constituency records (if you are the MLA)
- Records that relate to a function or program that is moving with you to a different ministry.

Not sure what to do with your MLA records?

Temporary storage is available for records of retiring MLAs. Complete the MLA Records Transfer agreement form available on the Records Management website.

Tips:

- **Check all the places you store government information** to make sure it is properly handled – this includes email folders, twitter accounts, CLIFF, H drive, mobile devices such as laptops and Blackberries, voice mail, and your desk drawers.
- Ensure **Cabinet records** are sent to Cabinet Operations.
- Transfer **expense records** to the Ministry of Finance
- Make sure that **other offices are aware** you are transferring official records, not reference copies.
- **Accessibility**: ensure authorized staff can access the records after you go by sharing encryption passwords and resolving access restrictions.

- A **responsibility centre** is an office or functional area to which the Minister's Office routinely delegates relevant records it generates and receives**.**
- **Regularly transfer** official records to the appropriate responsibility centre – in most cases a Deputy Minister's office.
- **File official records** that belong in the Minister's office in the government's Lan records storage system.

If you've done this on a routine basis, you won't have many other records to deal with when you transition.

3. **Dispose of transitory records.** Delete or otherwise securely destroy redundant copies, working materials no longer needed, ephemeral emails, and other transitory records that you have retained for reference purposes. For more information, see the *Transitory Records Guide* and the *Email Decision Diagram* available on the Records Management website.

4. **Ministers and other staff, with Deputy Minister permission, may retain reference copies of information needed for their new role** (e.g., email, speeches). Keep in mind these may be subject to requests made under the *Freedom of Information and Protection of Privacy Act* (*FOIPPA*).

5. **Minister's office to remove information access for the departing staff member** (i.e. facility and information systems).

6. **Review the checklist for departing employees.** The exit checklist for paper and e-records in the *Departing or Transferring Employees Guide* will help you ensure you haven't forgotten anything.

Governing legislation and policy

This includes:

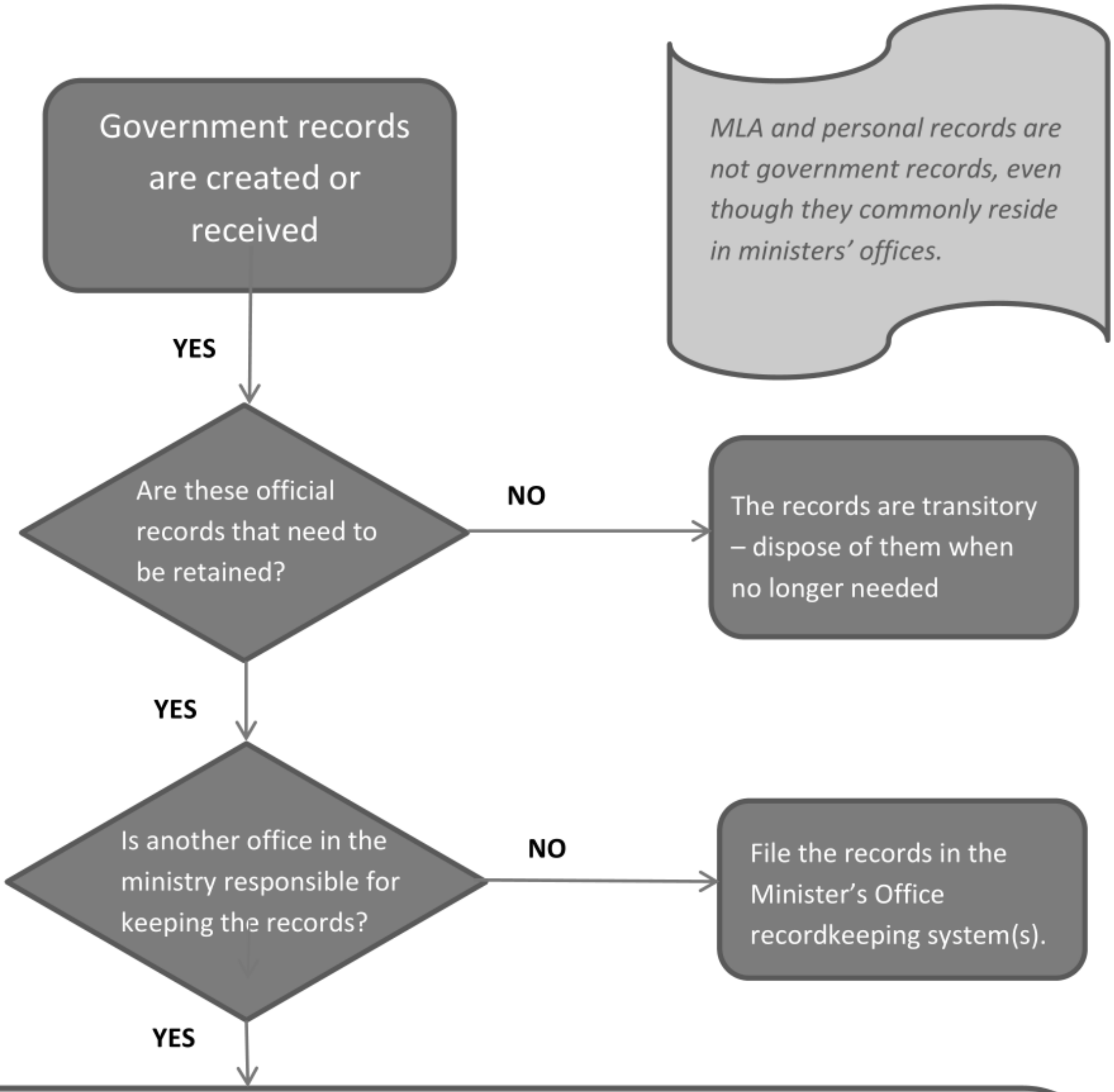
- *Information Management Act* (SBC 2015, c. 27)
- *Core Policy and Procedures Manual* – Chapter 12, IM/IT Management
- *Recorded Information Management (RIM) Manual*
- Oath of Employment for Political Staff
- Oath of Employment for BC Public Service Employees
- Appropriate Use of Government Information and Information Technology Resources (Appropriate Use Policy)

Additional Resources:

- For definitions of key terms (the ones in bold blue font) see the *RIM Glossary*
- Check out the RM Guides on the Records Management website
- Ask your Records Officer team for advice and assistance

Remember: All of the official records needed for government business must remain with the appropriate ministry responsibility centre.

APPENDIX A: MINISTERS' OFFICE RECORDS PROCESSES


Government records are created or received
YES
Are these official records that need to be retained?
NO
The records are transitory – dispose of them when no longer needed
YES
Is another office in the ministry responsible for keeping the records?
NO
File the records in the Minister's Office recordkeeping system(s).
YES
MLA and personal records are not government records, even though they commonly reside in ministers' offices.

Send records to the office identified as the responsibility centre, and maintain a record of their location. Example *(note that offices and locations vary among ministries)*:

TYPE OF RECORD	OFFICE	LOCATION
Cabinet submission drafts	Deputy Minister's Office	LAN (Local Area Network)
FOI request files	Corporate Services	TRIM (Total Records & Information Management System)
Minister's calendar	Minister's Office	Outlook (current month); LAN (previous months)
Minister's speeches	Government Communications & Public Engagement	LAN

Managing Government Calendars

BRITISH COLUMBIA

Ministry of Finance

Trusted financial and economic leadership for a prosperous province

Principles - Goals

To ensure accuracy and consistency in the processing and release of calendar requests

AND

to process calendar requests in a timely and efficient manner

WHILE

retaining the calendar’s functionality for staff

How Do You Use Your Calendar?

☒ Is your calendar your records system?

- Do your calendar entries include attachments such as agendas, documents; and
- Do you rely on the attachments as documentation of decision-making?

How Do You Use Your Calendar?

☑ OR

- Do you use your calendar as an organizational tool; and
- The documentation of decision-making is appropriately maintained elsewhere?

Your Record Keeping Responsibilities

- Create and keep complete and accurate records sufficient to support decision-making and business activities

- Government records, including calendars, must be managed and preserved to remain authentic, reliable, trustworthy, secure, complete and accessible over time and location regardless of media or format.

Your Record Keeping Responsibilities

Calendar records must be accurate and are subject to a formal access request under the *Freedom of Information and Protection of Privacy Act (FOIPPA) (FOI)*

Keeping Calendars Current

Calendar record should always contain current updates

Examples:

Delete meetings that did not occur

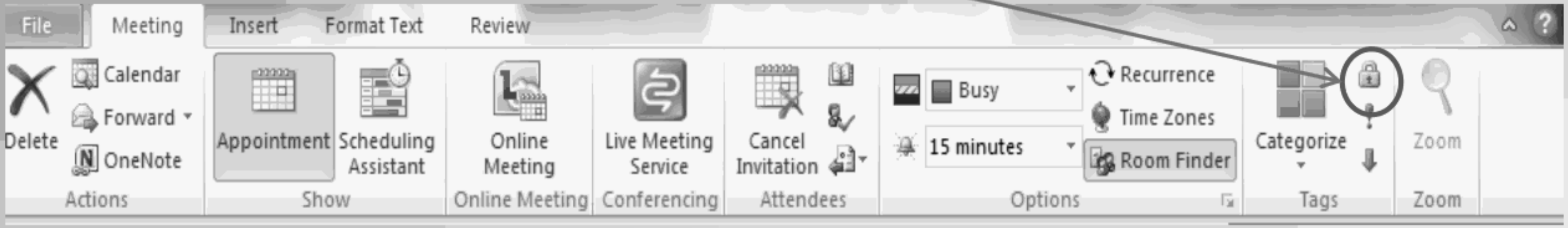
Delete meetings that calendar owner or representative did not attend

OR

Update owner’s calendar to reflect actual attendee and update the representatives calendar

Personal Appointments

Flag personal appointments as personal using the Mark Private icon



Consider deleting personal appointments immediately after they occur

Private Appointments

Use the Private Icon for:

- Sensitive meetings, e.g. personnel issues
- Confidential issues

Where others that normally have view access would be able to discern the meeting's purpose

Recorded Entries

- Ensure that calendar entries are ***CLEAR*** and ***CONSISTENT*** at time of entry.

- Be clear about the *subject* of the meeting and who is expected to attend. Keep the meeting subject ***CONCISE***. More information may lead to unnecessary redaction.

Recording Entries - Example

Unnecessary degree of detail – “**John Smith, EFO, re: cabinet submission on Citizen Engagement**”

- Based on this entry, IAO would be required to make a determination as to whether to redact the entry and it would be necessary to contact the calendar owner’s office, and possibly the Office of the Premier, for further information

Concise entry – “**John Smith, EFO, Citizen Engagement**”

- This entry can likely be released in full

Recording Entries cont'd..

- ***Be consistent*** at the time of entry – all those attending the meeting should have the same calendar entry
- Do not include attachments, send attachments in a separate email; or remove attachments immediately after the event
- If changes are necessary the originator should make changes so that all calendars are updated

Tip: Use the Outlook "new meeting" function to schedule meetings

Calendar Retention

With *some* exceptions, **all** government employee calendars must be managed as follows:

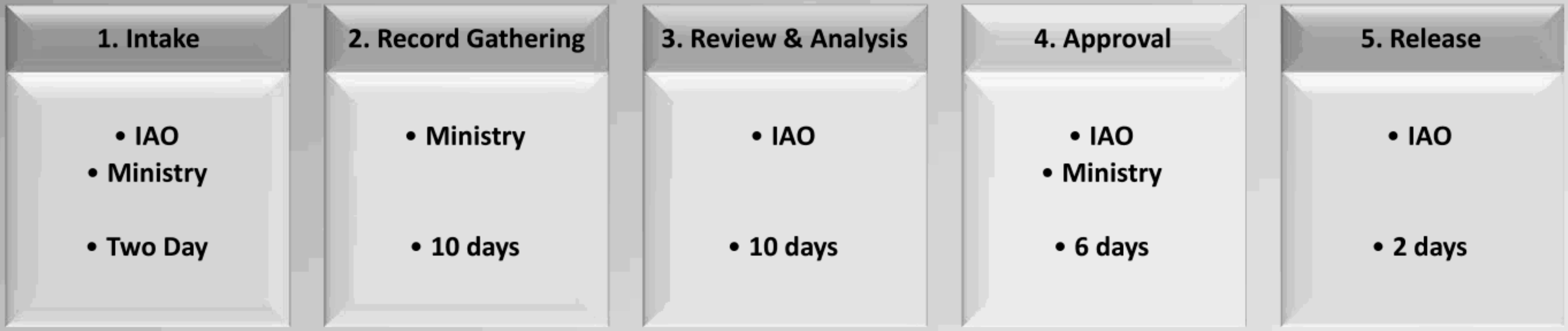
Retain your calendar until:

- A reasonable period of time has elapsed; and
- When no longer needed for operational purposes

Exception: Executive Directors who are regular members of the ministry executive council, ADMs, DMs, Ministers

The FOI Process for Calendars

FOIPPA Request -Timelines 30 Days!



1. Intake
- IAO
- Ministry
- Two Day

2. Record Gathering
- Ministry
- 10 days

3. Review & Analysis
- IAO
- 10 days

4. Approval
- IAO
- Ministry
- 6 days

5. Release
- IAO
- 2 days

Unless…………………

The request necessitates a 30 Day Extension under the Act

The Harms Assessment

What to look for………

Identifying ‘Harms’

‘Harms’– Disclosure of the records would significantly harm the ministry’s position, or a third party’s interest on a given topic

Ministry *must* ensure harms are clearly identified and communicated to IAO (identifying date and time of calendar entries that are of concern)

Ministry *may* need to provide more detail in order for IAO to determine if an exception to disclosure would apply

A Summary of 'Harms' in the Calendar Entries

Meeting / Appointment Date	Time	Potential Concerns
April 15, 2017	10:00 am	Doctor's Appointment
April 17, 2017	3:00 pm	Meeting with legal counsel
April 18, 2017	11:00 am	Cabinet Submission – New School in (SD007)
April 19, 2017	3:00 pm	Drinks with the girls

Severing Guidelines - Calendar Entries

Entry or Description of Entry	Severed or not Severed (sections in FOIPPA)
Blackberry/cell phone numbers for government employees	Severed under section 17 (Disclosure harmful to the financial or economic interests of a public body)
“Cabinet” or “Cabinet Retreat”	Not Severed
“Treasury Board”	Not Severed
Accommodation details	Severed under section 15 (Disclosure harmful to law enforcement)
Meeting location details	Severed under section 15 (Disclosure harmful to law enforcement)
Constituency related – any entries in the Minister’s calendar that relate to his/her duties as a Member of the Legislative Assembly	Out of Scope - under section 3 (Scope of this Act) - As the office of a Member of the Legislative Assembly is not a public body, any entries in a Minister’s calendar that relate to his/her duties as an MLA will be severed as outside the scope of FOIPPA.
360’s (executive performance review), mentoring, EPDP	Severed under section 22 (Disclosure harmful to personal privacy)

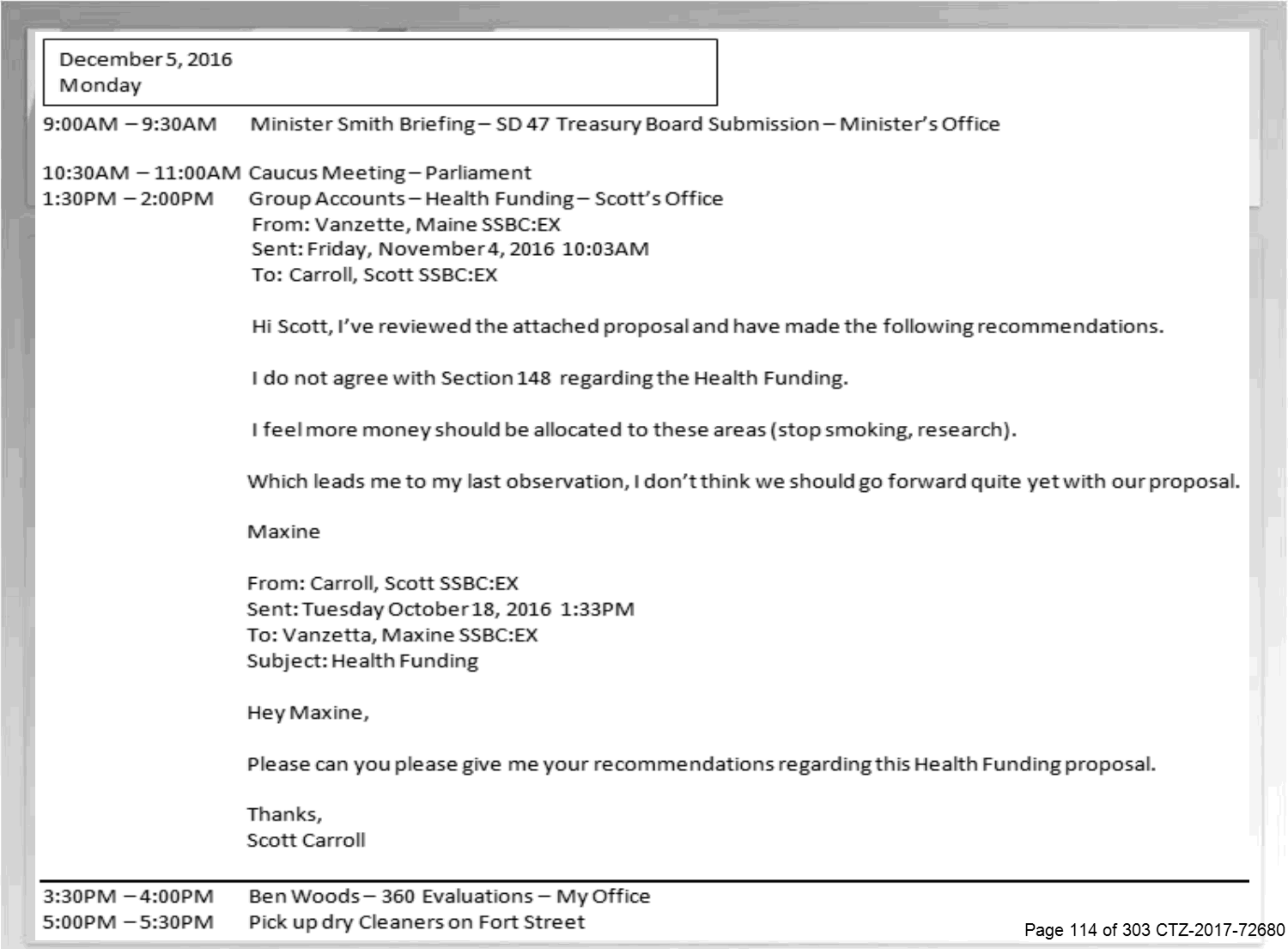
Calendar Entry Sample

Calendar Entry: **“Treasury Board Submission – New School Funding for SD 007”**

- ❖ Based on this entry, an exception would be considered. IAO will confer with the program area and potentially redact

Calendar Entry: **“Treasury Board Submission”**

- ❖ Based on this entry, it does not attract an exception therefore, it wouldn’t be redacted



December 5, 2016
Monday

9:00AM – 9:30AM Minister Smith Briefing – SD 47 Treasury Board Submission – Minister's Office

10:30AM – 11:00AM Caucus Meeting – Parliament
1:30PM – 2:00PM Group Accounts – Health Funding – Scott's Office

From: Vanzette, Maine SSBC:EX
Sent: Friday, November 4, 2016 10:03AM
To: Carroll, Scott SSBC:EX

Hi Scott, I've reviewed the attached proposal and have made the following recommendations.

I do not agree with Section 148 regarding the Health Funding.

I feel more money should be allocated to these areas (stop smoking, research).

Which leads me to my last observation, I don't think we should go forward quite yet with our proposal.

Maxine

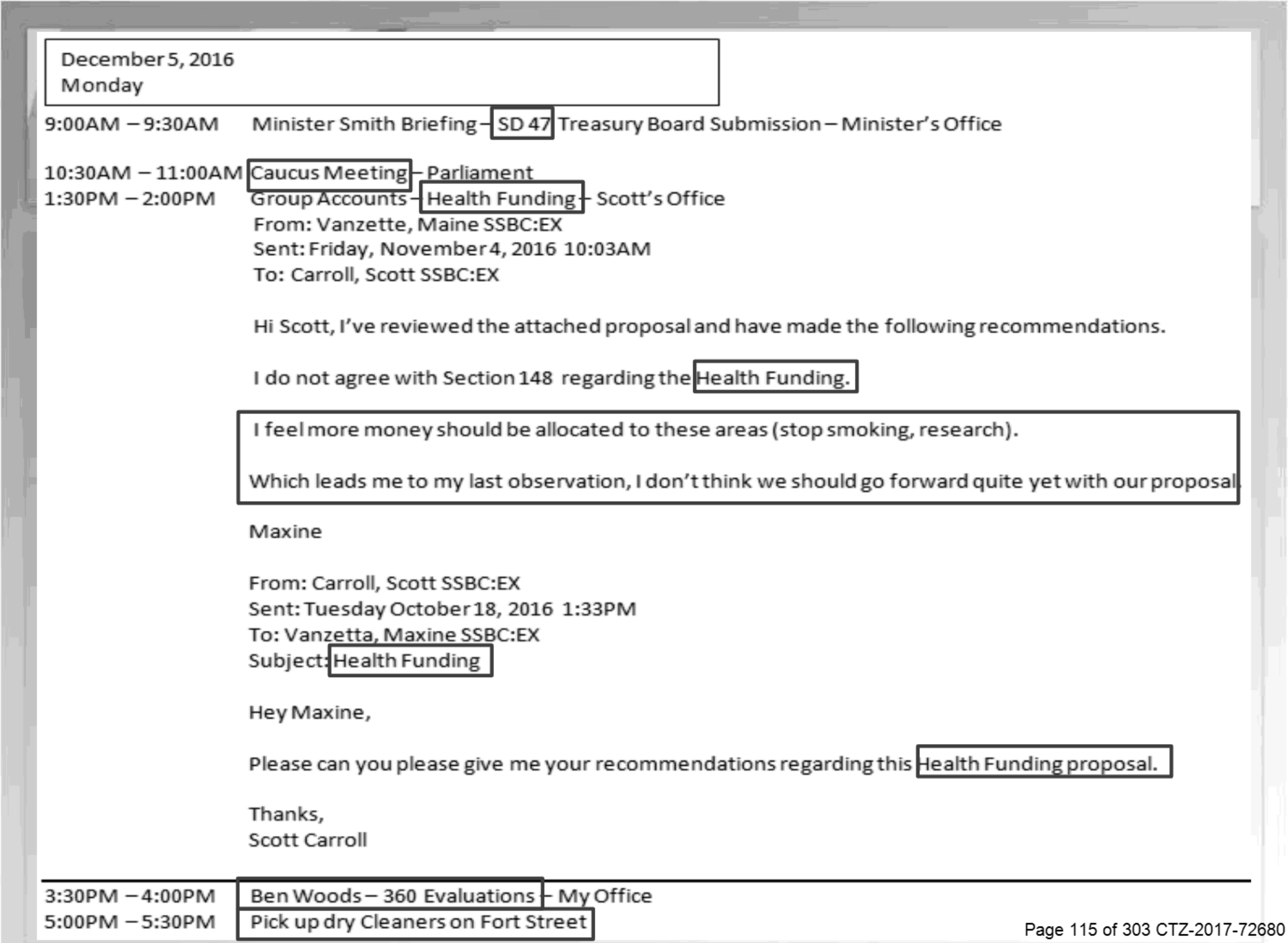
From: Carroll, Scott SSBC:EX
Sent: Tuesday October 18, 2016 1:33PM
To: Vanzetta, Maxine SSBC:EX
Subject: Health Funding

Hey Maxine,

Please can you please give me your recommendations regarding this Health Funding proposal.

Thanks,
Scott Carroll

3:30PM – 4:00PM Ben Woods – 360 Evaluations – My Office
5:00PM – 5:30PM Pick up dry Cleaners on Fort Street



December 5, 2016
Monday

9:00AM – 9:30AM Minister Smith Briefing – SD 47 Treasury Board Submission – Minister's Office

10:30AM – 11:00AM Caucus Meeting – Parliament
1:30PM – 2:00PM Group Accounts – Health Funding – Scott's Office

From: Vanzette, Maine SSBC:EX
Sent: Friday, November 4, 2016 10:03AM
To: Carroll, Scott SSBC:EX

Hi Scott, I've reviewed the attached proposal and have made the following recommendations.

I do not agree with Section 148 regarding the Health Funding.

I feel more money should be allocated to these areas (stop smoking, research).

Which leads me to my last observation, I don't think we should go forward quite yet with our proposal.

Maxine

From: Carroll, Scott SSBC:EX
Sent: Tuesday October 18, 2016 1:33PM
To: Vanzetta, Maxine SSBC:EX
Subject: Health Funding

Hey Maxine,

Please can you please give me your recommendations regarding this Health Funding proposal.

Thanks,
Scott Carroll

3:30PM – 4:00PM Ben Woods – 360 Evaluations – My Office
5:00PM – 5:30PM Pick up dry Cleaners on Fort Street

December 5, 2016
Monday

9:00AM – 9:30AM Minister Smith Briefing – S12 Treasury Board Submission – Minister's Office

10:30AM – 11:00AM S3 – Parliament

1:30PM – 2:00PM Group Accounts – S13, S17 – Scott's Office

From: Vanzette, Maine SSBC:EX
Sent: Friday, November 4, 2016 10:03AM
To: Carroll, Scott SSBC:EX

Hi Scott, I've reviewed the attached proposal and have made the following recommendations

I do not agree with Section 148 regarding the S13, S17

S13, S17

Maxine

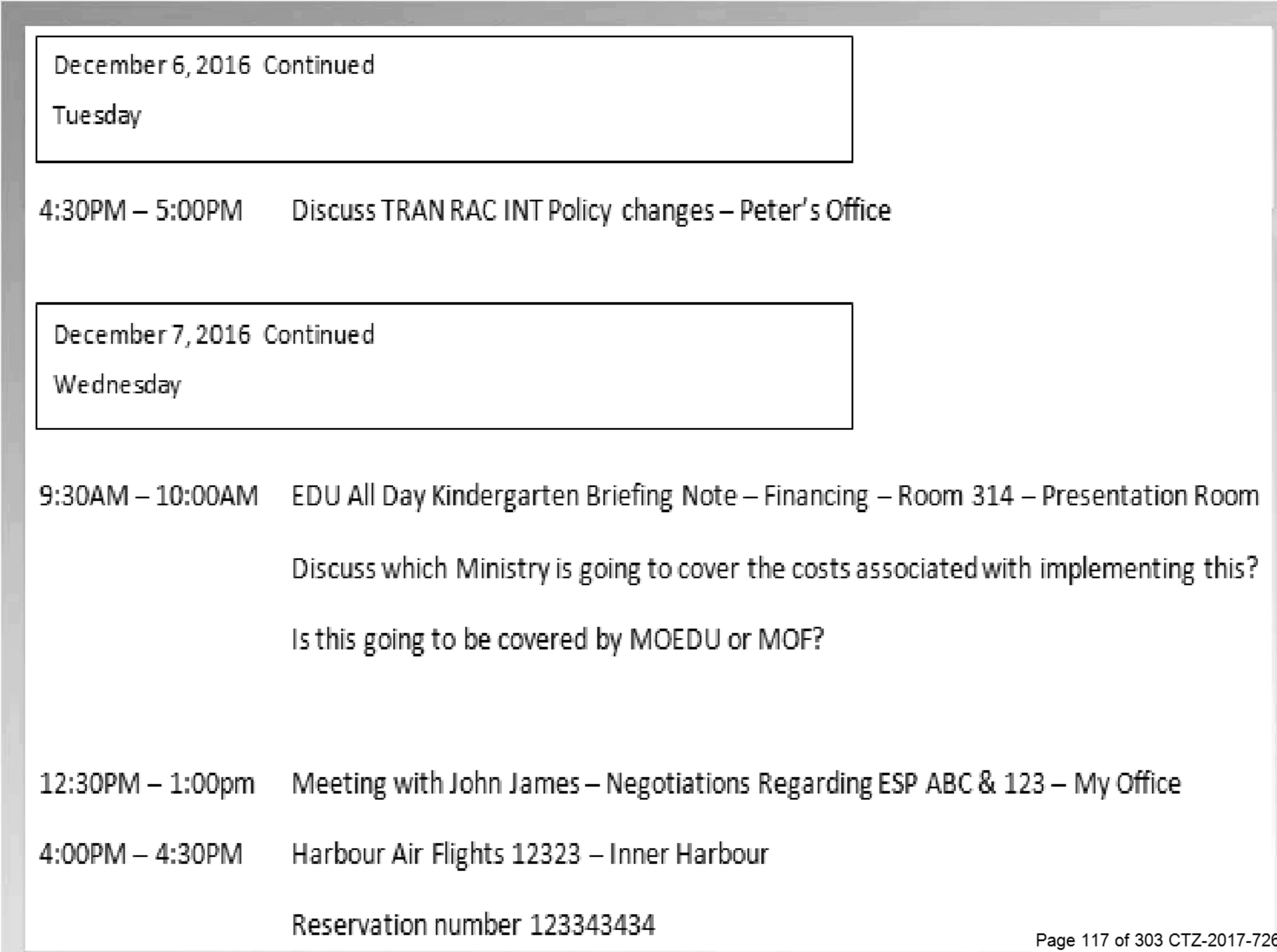
From: Carroll, Scott SSBC:EX
Sent: Tuesday October 18, 2016 1:33PM
To: Vanzetta, Maxine SSBC:EX
Subject: Health Funding

Hey Maxine,

Please can you please give me your recommendations regarding this S13, S17.

Thanks,
Scott Carroll

3:30PM – 4:00PM S22
5:00PM – 5:30PM S22



December 6, 2016 Continued

Tuesday

4:30PM – 5:00PM Discuss TRAN RAC INT Policy changes – Peter's Office

December 7, 2016 Continued

Wednesday

9:30AM – 10:00AM EDU All Day Kindergarten Briefing Note – Financing – Room 314 – Presentation Room

Discuss which Ministry is going to cover the costs associated with implementing this?

Is this going to be covered by MOEDU or MOF?

12:30PM – 1:00pm Meeting with John James – Negotiations Regarding ESP ABC & 123 – My Office

4:00PM – 4:30PM Harbour Air Flights 12323 – Inner Harbour

Reservation number 123343434

December 6, 2016 Continued

Tuesday

Unclear if this needs to be removed

4:30PM – 5:00PM Discuss TRAN RAC INT Policy changes – Peter's Office

December 7, 2016 Continued

Wednesday

S17

9:30AM – 10:00AM EDU All Day Kindergarten Briefing Note – Financing – Room 314 – Presentation Room
Discuss which Ministry is going to cover the costs associated with implementing this?
Is this going to be covered by MOEDU or MOF?

Unclear if this needs to be removed

12:30PM – 1:00pm Meeting with John James – Negotiations Regarding ESP ABC & 123 – My Office

4:00PM – 4:30PM Harbour Air Flights 12323 – Inner Harbour
Reservation number 123343434
17, 22

Overall Gains

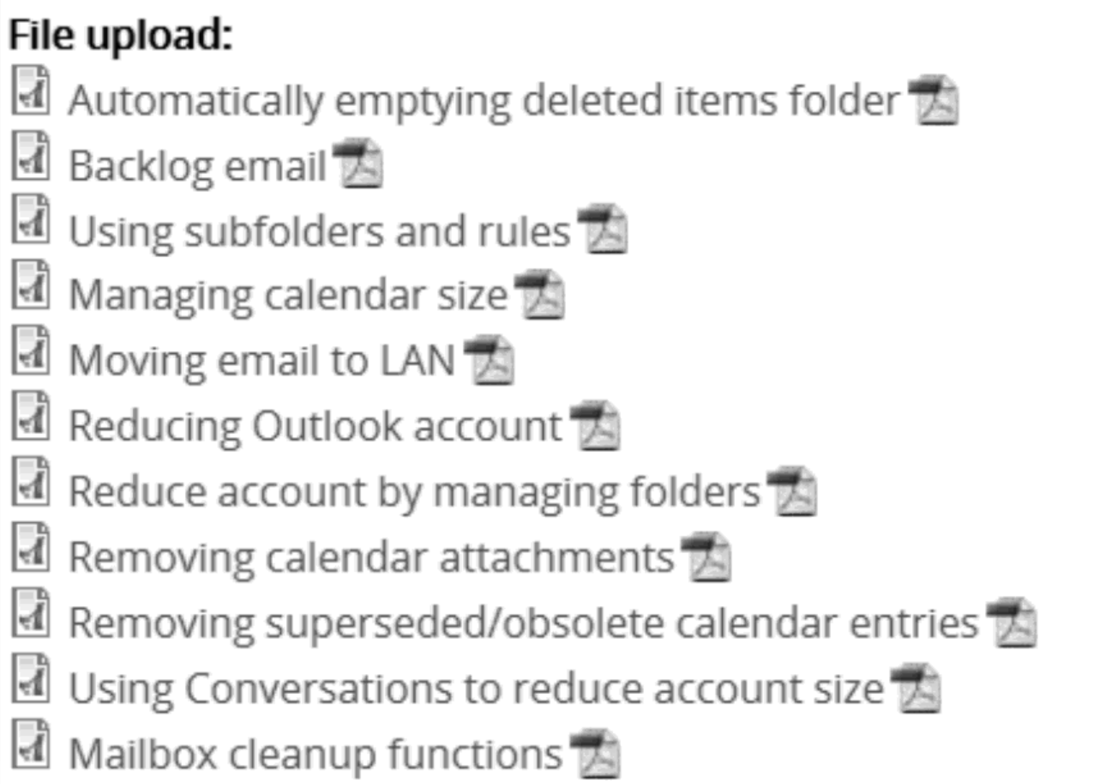
Compliance with Government’s legislated obligations (IMA and FOIPPA)

Ministry-wide coordinated and consistent approach to managing calendars as a government record

Required approach to managing calendars for release

Reference Materials

@ Work – Records Management Community – Articles – Outlook Tips



File upload:

- Automatically emptying deleted items folder
- Backlog email
- Using subfolders and rules
- Managing calendar size
- Moving email to LAN
- Reducing Outlook account
- Reduce account by managing folders
- Removing calendar attachments
- Removing superseded/obsolete calendar entries
- Using Conversations to reduce account size
- Mailbox cleanup functions

Outlook Demonstration

Remember the help function in Outlook

THANK YOU

GOVERNMENT RECORDS SERVICE GUIDE

MANAGING MINISTER'S OFFICE RECORDS

Overview

Records of British Columbia's cabinet ministers and their staff are a valuable public asset. They provide documentation of government policies and programs and are an important part of government's historical record.

Like other government offices, those of ministers are subject to statutory and policy requirements regarding records management, freedom of information, and privacy. They are also subject to the government-wide directive on appropriate use of information and information technology resources ("Appropriate Use Policy"). Employees further must adhere to their Oath and to the Standards of Conduct for Political Staff.

There typically are three categories of records within a minister's office:

- **Personal Records** that relate to the private life and personal interests of the minister and staff**.**
- **Member of Legislative Assembly (MLA) Records,** which are the political and constituency records generated by ministers in their capacity as members of the Legislative Assembly.

  Personal and MLA records should be managed separately from government records, in order to protect privacy and avoid having to separate them later on (an incoming minister and staff would not usually have access to the personal and MLA records of their predecessors).
- **Government Records** that are created or received by ministers and their staff as ministers of the Crown. These include both official and transitory records and are subject to the *Document Disposal Act* (soon to be replaced by the *Information Management Act*) and the *Freedom of Information and Protection of Privacy Act*.

Official Records

Given the level of responsibility of a minister's office, official records of the office must be maintained, including records documenting substantive activities, decisions and decision making processes of the office. In broad terms, official records include the master or file copies of records documenting the performance of minister's office functions or the running and administration of the office itself.

Minister's office records now are increasingly digital (e.g. electronic messages and documents) and are maintained in many locations by multiple responsible bodies. Records typically are received from many offices, acted upon by the minister's office, and then routed to other offices for action and/or retention.

While practices may vary somewhat among offices, the following are typical, best practices:

- **For most records received by or sent from a minister's office, the Office of Primary Responsibility (OPR) is the deputy minister's office** (i.e. with such exceptions as listed below, most records are sent to the deputy minister's office for retention, when no longer needed by the minister's office).

The deputy minister's office is able to provide continuity and appropriate public service administration of the records of successive ministers. In some cases certain minister's office records are best maintained along with other related records within the appropriate functional area.

- **Cabinet records go to Cabinet Operations.**
- **Expense records go the Ministry of Finance.**
- **Other types of records** (e.g. approved decision notes) may go to the **relevant ministry program area OPR** for the subject matter.

Recordkeeping Requirements for Official Records

Since ministers' office records are maintained by a variety of responsibility centres, it is important to establish documentation on which types of records are routed where. Best practice is to maintain this documentation within the deputy minister's office.

Appendix A provides an overview of the basic routing and documentation requirements, which are:

- **Identify the offices responsible for maintaining official records received from the minister's office.** See the records location and types list at the end of Appendix A for an example of an easy way to track designated responsibility centres for various types of records.
- **Ensure that offices identified as responsibility centres are aware of their role.** Offices receiving the master "file copies" of minister's office records need to be aware that they are responsible for maintaining the records for the required length of time, in a secure, accessible manner. (Under current information schedules, official records of minister's offices must be retained at least 10 years). See the Records Management Resources section below for sources of information on appropriate recordkeeping systems and practices.
- **When a freedom of information (FOI) request or litigation search occurs, use the above documentation to provide relevant information about where the requested records are held.**

Transitory Records

Transitory records are records of temporary usefulness that are needed for only a limited period of time in order to complete a routine action or prepare an ongoing record. They are those records that do *not* have ongoing value for supporting or documenting the work of the minister's office, and therefore do *not* need to be maintained as part of the official records of the office.

Note that it is the content and use of a record that determines its value, not its form (e.g. an email may be transitory or official.)

For guidance on identifying transitory records see the Transitory Records Guide. See as well **Appendix B** below for scenarios regarding transitory and official records of minister's offices.

The December 2015 David Loukidelis Report (*Implementing Investigation Report F15-03*) outlines considerations relevant to the identification of transitory records.

> *"1. Is the function or activity for which the record was produced and used significant?*
>
> The significance of the function or activity that the final document supports and of which it is a part is key to determining the retention and preservation of any government record (always assuming, of course, that this is limited to a government function or activity, not a personal matter). However, it is not the goal of a transitory records identification process to determine the relative significance of the function or activity that is being documented. That is the objective of the records management process after the records are captured into the system, with retention and disposition being driven by that analysis. Officials therefore should not need to consider the significance of the function and activity when identifying what is transitory. For example, the activity of routine maintenance of a government building is generally considered less significant than development of new legislation. Yet, because that process is a government activity, some evidence of that activity needs to be captured, with records management schedules determining whether and how long records documenting these activities are retained.
>
> *2. Is the record significant in relation to the transaction or activity for which it was created and used in support?*
>
> If all functions and activities are essentially equal for the purpose of identifying transitory records the next step would be to analyze the relative significance of the document in terms of its contribution to or participation in the function or activity. For practical purposes, it is assumed that, if it is necessary to create or receive a record to further or complete the transaction or activity, the record is significant enough for the limited purposes of a transitory records policy. The real question revolves around the quality, the value, of the record or information in relation to the function and activity.
>
> *3. Does the information, in relation to other captured (or to be captured) records, best document the function or activity it was created or used to support?*
>
> This question helps delineate the boundaries of both the scope and content of a transitory records policy. Regardless of the function or activity, and assuming that the record was created and used for a purpose, it is simply a matter of determining whether it provides unique, or the most effective, evidence of a function or activity. This would mean that information that is irrelevant to a particular activity, or that duplicates information better held elsewhere, is transitory. On the other hand, even if the record, in its format or content, is of poor quality, it should not be considered transitory if it is the only record."

It is good practice for all offices to regularly dispose of transitory records as soon as their value ends. This makes it easier to identify and manage the official records. Transitory records can and should be disposed of as soon as they no longer are of value to the individual holding them (e.g. deleted from the individual's email account), with one important exception:

- ***If the minister's office receives a freedom of information or litigation search request, all relevant records must be provided - whether transitory or not.*** *Transitory records that are subject to such requests must be retained pending completion of the applicable FOI response process and review period or the applicable litigation activities (contact Information Access Operations and Legal Services Branch, respectively, for guidance on particular cases).*

Freedom of Information and Protection of Privacy

Government records within a minister's office are subject to the *Freedom of Information and Protection of Privacy Act*, and must be searched in response to an FOI request. Designated FOI contacts for ministers' offices are located within the deputy ministers' office. Ministers' offices are also subject to government-wide privacy policies.

See the following handouts:

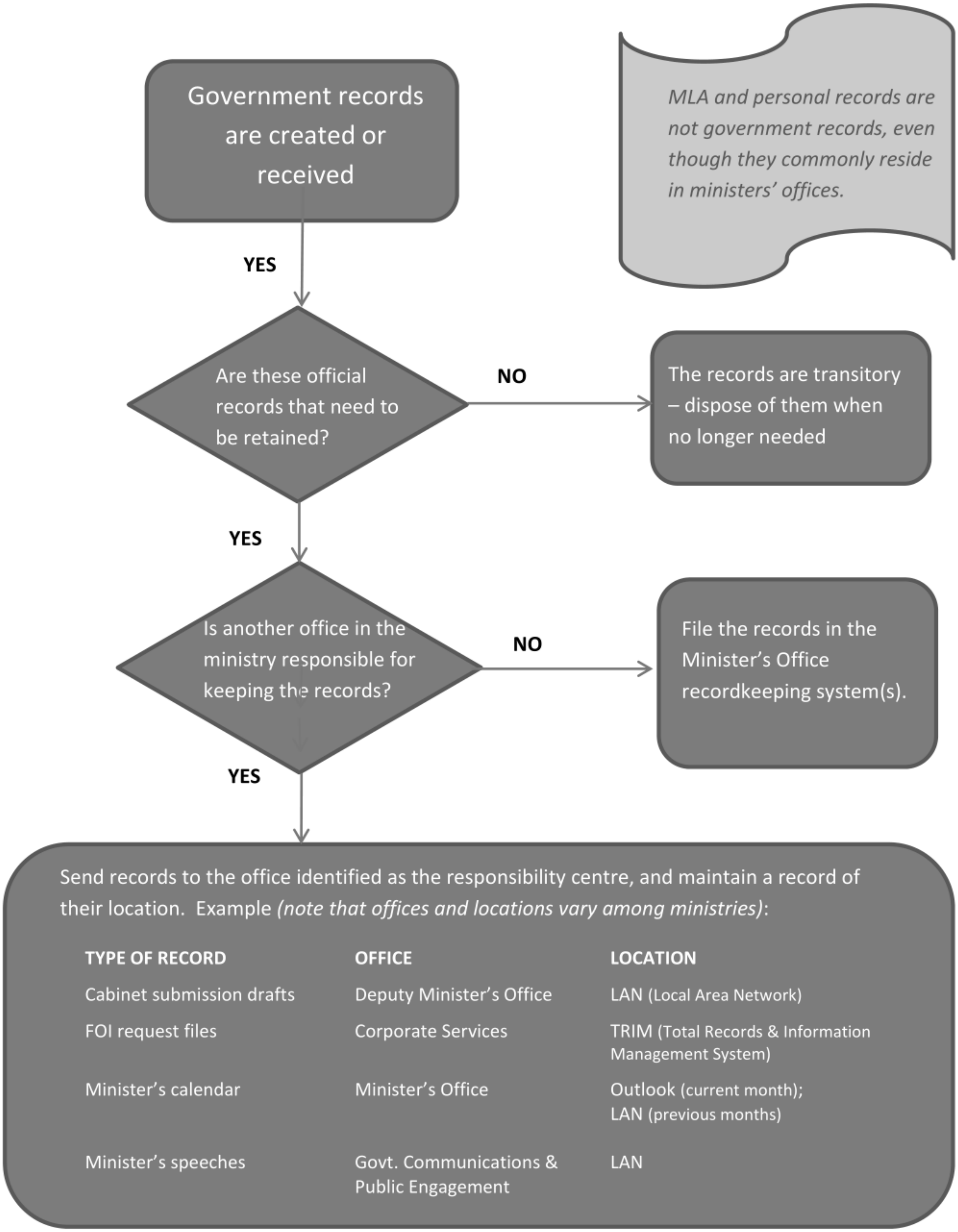
- Minister's Office Search Process
- Clarifying and Interpreting an FOI Request
- Conducting and Documenting a Search for Records
- Providing Explanations when there are No Records to an FOI Request
- The Escalation Process for FOI Requests
- The 10 Privacy Principles
- Privacy Glossary and Resources

Additional Resources

Staff responsible for managing minister's office records will find a wide variety of guides, tools and contacts (e.g. ministry records officers) on Government's records management website.

Note also that in support of implementation of the December 2015 Loukidelis Report recommendations to improve government records management and FOI processes, new training has been provided and will continue to be enhanced and updated, and new policy documentation is under development.

APPENDIX A: MINISTERS' OFFICE RECORDS PROCESSES



Government records are created or received

MLA and personal records are not government records, even though they commonly reside in ministers' offices.

Are these official records that need to be retained?

The records are transitory – dispose of them when no longer needed

Is another office in the ministry responsible for keeping the records?

File the records in the Minister's Office recordkeeping system(s).

Send records to the office identified as the responsibility centre, and maintain a record of their location. Example *(note that offices and locations vary among ministries)*:

TYPE OF RECORD	OFFICE	LOCATION
Cabinet submission drafts	Deputy Minister's Office	LAN (Local Area Network)
FOI request files	Corporate Services	TRIM (Total Records & Information Management System)
Minister's calendar	Minister's Office	Outlook (current month); LAN (previous months)
Minister's speeches	Govt. Communications & Public Engagement	LAN

APPENDIX B: Scenarios Regarding Transitory and Official Records

The following scenarios are illustrative of the variety of functions performed by a minister's office (MO) and the types of records the office receives and creates. These scenarios assume that many of the official records for a minister's office will typically be sent for filing and retention by the deputy minister's office (DMO) or other appropriate responsibility centre. Under this practice, residual copies remaining in the minister's office are transitory and may be disposed of when no longer needed.

Scenario 1 – Speeches and Presentations

The minister has been asked to speak about a new ministry initiative at a conference at UNBC. The MO works with the ministry program area on the speech/presentation.

Function/Process	Records are:
Event planning correspondence (email strings around choices of hotel, flights, government vehicle use)	Transitory
Official invitations and itinerary (e.g. purpose for minister's attendance, background on the event, venue, dates)	Official records • Retain records in MO or DMO. • Any attachments need to be removed from calendar entry and filed separately.
Minister's speech or presentation (e.g. text, audio-video)	Official Records • Government Communications and Public Engagement (GCPE) retains the official record of the minister's speech or presentation • Official copies of presentation material may be retained by the originating program area if they are of continuing value to that program. Transitory • Residual copies may be retained by the MO or DMO for reference purposes until no longer useful.

Scenario 2 – Travel Planning and Expenses

The minister is travelling to Ottawa to attend an annual meeting of Federal/Provincial/Territorial ministers.

Function/Process:	Records are:
Travel planning correspondence (Email strings relating to choice of flights, airport transports, car rentals, hotels etc.)	<u>Transitory</u>
Travel and meeting itineraries (e.g. purpose of trip, planned meetings, dates, venues, attendees)	<u>Official records</u> • Retain records in either MO or DMO. If the official records are retained in the DMO, then residual MO copies are transitory.
Invitation logged in Outlook calendar	<u>Official records</u> • MO will print/pdf calendar each month. • These records will be retained in MO or DMO.
Meeting-related records prepared by ministry (e.g. briefing notes, handouts, slides)	<u>Transitory</u> (residual MO copies) • Official records are retained in DMP and/or other appropriate responsibility centre. • MO copies should be disposed of when no longer needed.
Meeting related records received before or at meeting (agenda, minutes, notes, content provided by other attendees)	<u>Official records</u> • Retain records in either MO or DMO. If the official records are retained in the DMO, then residual MO copies are transitory.
Travel expenses for Minister and accompanying staff (e.g. transportation and accommodation costs, per diem, receipts)	<u>Official records</u> • Travel vouchers and receipts are sent to Ministry of Finance. • Residual MO copies are transitory.
Presentations or speeches by Minister	See Speeches and Presentations scenario

Scenario 3 - House briefing materials

Ministry program areas have been asked to provide the Minister with material for the budget estimates debate in the House.

Function/Process	Records are:
Briefing materials and questions (e.g., hardcopy binders, documents attached in CLIFF)	Transitory (residual MO copies) • Official records are retained in the DMO or other relevant responsibility centre. • Copies in MO should be disposed of when no longer useful.
Correspondence relating to direction on preparation of budget estimates	Transitory (residual MO copies) • Official records are retained in the DMO.

Scenario 4 - Non-Cabinet Committees/Meetings

The minister is attending a meeting with key stakeholders about progress to date on a ministry sponsored project.

Function/Process	Records are:
Meeting invitation in Outlook Calendar	Official records • The MO will print/pdf calendar each month for filing. • These records will be retained in the MO or DMO.
Meeting preparation (includes background/briefing materials and reports developed by the ministry, content prepared for meeting stakeholders)	Transitory (residual MO copies) • Official records are retained in the DMO or other appropriate responsibility centre. • Minister's office copies should be disposed of when no longer useful.
Meeting records (includes agenda, records received from stakeholders, agenda, minutes, notes)	Official records • These records will be retained in the MO or DMO. If the official records are retained in the DMO, then residual MO copies are transitory.

Scenario 5 - Unfiled Minister's Office E-Mail

Due to volume, MO personnel have accumulated e-mail that has not been disposed of over time as clearly transitory or filed in other systems (e.g., TRIM).

Function/Process	Records are:
Accumulation of e-mail messages in Outlook folders	Official records • MO retains these records until they have been either filed in another office system or transferred to the DMO (e.g. when the minister transfers to another portfolio) • MO personnel should continue to dispose of transitory messages (per the Transitory Records Guide), except those identified in FOI and litigation searches, and to remove or dispose of any MLA or personal messages. • DMO will ultimately assume responsibility for these e-mail accumulations.

From: Gillies, Jessica FIN:EX
To: Reed, Matt FIN:EX
Subject: MO training?
Date: Tuesday, July 25, 2017 1:37:33 PM

Hi Matt,

I am the DMO liaison to the MO for their FOI requests. Do you know if CIRM will be providing any training to new MO staff re: FOI requests, records management, etc.? We're going to meet with the new MA tomorrow and I can give them some info but I was wondering if any formal training is planned.

Thank you!

Jessica Gillies
Manager, FOI & Correspondence Unit
FOI & Correspondence Unit | Deputy Minister's Office | Ministry of Finance
FIN FOI SharePoint site | Correspondence intranet page
phone 250 387-3513 | email Jessica.Gillies@gov.bc.ca

Please consider the environment before printing this email | ***VISION: Trusted financial and economic leadership for a prosperous province***

*This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error **please notify the sender immediately**. Any unauthorized copying, disclosure or distribution of the e-mail or the information it contains is strictly forbidden.*

From: Reed, Matt FIN:EX
To: Curtis, David FIN:EX; Laidlaw, Susan FIN:EX
Subject: RE:
Date: Wednesday, July 26, 2017 9:59:00 AM

No problems from Privacy, but there is a reference on the last page to an FOI contact – which may not adequately grab the role of the DMO FOI Liaison, but I would defer to Brad on that front.

-m

From: Curtis, David FIN:EX
Sent: Wednesday, July 26, 2017 9:34 AM
To: Reed, Matt FIN:EX; Laidlaw, Susan FIN:EX
Subject:

Any comments/concerns regarding distribution of this document to the MOs?

From:	Hoskins, Chad FIN:EX
To:	Reed, Matt FIN:EX; Onciul-Omelus, Jamie FIN:EX
Subject:	RE: FOI training session
Date:	Friday, July 28, 2017 1:21:53 PM
Attachments:	image001.jpg

Hi Matt,

s.22 she connect with you on Monday. I believe that she has asked her contact in the DMO there to send you the invite.

It might be best if you bring the deck that you usually use for new leg staff. I think Jamie has been asked to describe some of the processes around FOI and sending calendars for proactive release. I'm not sure we'd have a deck for that as the questions sounded slightly more informal.

Thanks, Chad

From: Reed, Matt FIN:EX
Sent: Friday, July 28, 2017 11:56 AM
To: Onciul-Omelus, Jamie FIN:EX
Cc: Hoskins, Chad FIN:EX
Subject: FOI training session

Hi Jamie,

I understand that I will be heading to the CFD FOI training with you on Monday, and was hoping that you would be able to send me the meeting notice for this session. Also, if possible, it would be helpful to either chat beforehand, or to see the deck that will be used for this session.

Thanks,

-m

Matt Reed

Senior Director, Strategic Privacy and Training

Privacy, Compliance and Training Branch,

250 514-8870

BC logo for sig

From: Reed, Matt FIN:EX
To: Curtis, David FIN:EX; Hoskins, Chad FIN:EX
Subject: RE: MO Guides & Training Links
Date: Wednesday, July 26, 2017 9:23:00 AM

No inconsistencies from my point of view.

Thanks,

-m

From: Curtis, David FIN:EX
Sent: Tuesday, July 25, 2017 5:38 PM
To: Hoskins, Chad FIN:EX; Reed, Matt FIN:EX
Subject: MO Guides & Training Links

Hi,

I would appreciate your review of the following training materials from GRS – to make sure we are consistent with the emerging training materials. If possible I would appreciate the return of any comments, concerns that you might have by 10:00am tomorrow.

Thanks and sorry for the tight timeline.

Regards,

David

****

Guides

GRS has two published guides specifically for Ministers' Offices (both attached):

Managing Ministers' Office Records, and

Best Practices when Leaving a Ministers' Office

I have also attached a "Managing Government Calendars" document that covers best practices for managing calendars.

Numerous additional guides can be found on the Government Records Service website.

Courses

Several online, self-directed courses are available via the PSA's Learning System, including:

- IM 117: Protection of Privacy, Access to Information and Records Management (ITEM-652)
- IM 110: Managing Our Information Assets (ITEM-56)
- IM 112: Managing Government Records (ITEM-41)
- LAN Organization (ITEM-158)
- Email and Records Management Best Practices (ITEM-570)

These courses can be taken at any time and we would recommend starting with IM117.

To learn more about these courses and to register, visit the Learning System and search for a course by its title or item number.

In addition, we are more than happy to deliver custom, in-person training.

For more information, visit the Government Records Service website or contact Richelle Wright, the Ministry of Citizens' Services Records Officer.

From: Reed, Matt FIN:EX
To: Gillies, Jessica FIN:EX; Hoskins, Chad FIN:EX
Subject: RE: MO training?
Date: Tuesday, July 25, 2017 7:44:00 PM

Hi Jessica,

I believe that training has been offered (both FOI training, and the IM training that I normally deliver). I can speak for the IM training – and that we haven't confirmed any sessions yet. Chad (CCed here) can speak for the FOI training offer.

Thanks,
-m

From: Gillies, Jessica FIN:EX
Sent: Tuesday, July 25, 2017 1:38 PM
To: Reed, Matt FIN:EX
Subject: MO training?

Hi Matt,

I am the DMO liaison to the MO for their FOI requests. Do you know if CIRM will be providing any training to new MO staff re: FOI requests, records management, etc.? We're going to meet with the new MA tomorrow and I can give them some info but I was wondering if any formal training is planned.

Thank you!

Jessica Gillies
Manager, FOI & Correspondence Unit
FOI & Correspondence Unit | Deputy Minister's Office | Ministry of Finance
FIN FOI SharePoint site | Correspondence intranet page
phone 250 387-3513 | email Jessica.Gillies@gov.bc.ca

Please consider the environment before printing this email | ***VISION: Trusted financial and economic leadership for a prosperous province***

This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error ***please notify the sender immediately****. Any unauthorized copying, disclosure or distribution of the e-mail or the information it contains is strictly forbidden.*

From:	Reed, Matt FIN:EX
To:	Fairbairn, Joel FIN:EX
Subject:	RE: Updated Ministerial Office Deck - For Staff
Date:	Thursday, July 20, 2017 3:51:00 PM

Thanks Joel.

No problem on your requests – mostly just an oversights between all of our drafts. We will work with Melissa if any of the proposed changes can't be immediately accepted as-is.

-m

From: Fairbairn, Joel FIN:EX
Sent: Thursday, July 20, 2017 11:13 AM
To: Reed, Matt FIN:EX
Subject: RE: Updated Ministerial Office Deck - For Staff

Hey Matt,

Comments embedded. Also, just a couple of requests.

From an editorial standpoint I'd leave most things to PCT. However, can you please make sure your staff make requested changes where it would clearly be our call. There are examples of a couple of things that we had asked to have changed and were not.

Also, from a collaboration/work flow standard, please have staff redline edits.

Thx

-J

From: Reed, Matt FIN:EX
Sent: Friday, July 14, 2017 2:53 PM
To: Williams, Brad M FIN:EX; Fairbairn, Joel FIN:EX; Laidlaw, Susan FIN:EX; Sherwood, David FIN:EX
Subject: Updated Ministerial Office Deck - For Staff

Hi all,

Attached for your review (if you can stand another), is the refreshed IM training deck for Ministerial staff. This the original deck that we used last year, with updates coming from the changes we made for IM117, and the changes we made for the most recent review of the Minister's deck (very little unvetted content). I'm sending this in Word format so that it is easier to comment on. If you could get comments in by Tuesday or Wednesday at the latest that would be great.

Thanks,

-m

Slide 1

Privacy, Access and Records Management Refresher

For Ministerial Staff

Privacy, Compliance & Training Branch
Corporate Information and Records Management Office
Ministry of Finance

British Columbia
Ministry of Finance
Trusted financial and economic leadership for a prosperous province

Good morning/good afternoon.   [personal introduction].

I am here representing the Corporate Information and Records Management Office, or CIRMO for short. This is the division that is responsible for **information management** in government. CIRMO was established in December 2015 to consolidate government's critical information management functions in order to enhance government practices - **including** leadership in the implementation of all 27 of David Loukidelis' recommendations. CIRMO is led by the Chief Records Officer, Associate Deputy Minister Cheryl Wenezenki-Yolland.

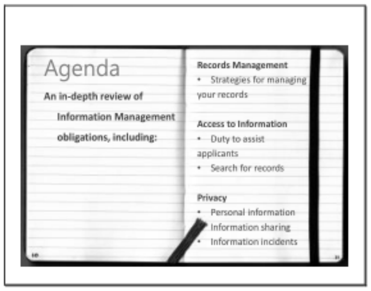
Comment [MS1]: New administration not so keen on Loukidelis.

Comment [MS2]:

Comment [MS3]: Needs to be removed.

As someone who works in Information Management - Privacy and FOIPPA in particular –I am very enthusiastic about this content and so my goal for the next 2 hours will be to share some of that passion with you. I know that you'll come away from today with a greater understanding of your information management obligations. But I also hope that you will gain some of my enthusiasm for information management too.

Slide 2



Agenda

An in-depth review of Information Management obligations, including:

Records Management
- Strategies for managing your records

Access to Information
- Duty to assist applicants
- Search for records

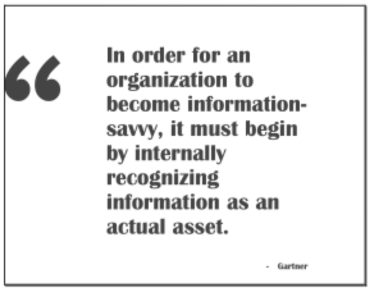
Privacy
- Personal information
- Information sharing
- Information incidents

We are here today to get a bit of a refresher on our information management requirements and introduce new practices and controls that will improve information management practices and accountability. You have all received training on access, **or** said another way, on FOI - and you have all taken training on privacy and information sharing. However, as we all know, these are areas that have developed very quickly, given the massive increase in the volume of records we all hold. This is a result of digitization, email, and nearly unlimited electronic storage.

Today's training will focus on areas that have received the most attention, both from government officials, and the Information and Privacy Commissioner. We'll touch on **records management** requirements, **duty to assist** an FOI applicant and **proper search** for records, and then finish with a reminder of our

collective privacy obligations, including what to do in the event of an information incident or **privacy breach**.

Slide 3



“ In order for an organization to become information-savvy, it must begin by internally recognizing information as an actual asset.

- Gartner

- We in the Ministry of Finance often speak of extending the culture that currently exists around protecting our financial resources to the informational resources we have in government. The measures that are in place to monitor the expenditure of dollars are extensive. We have to take that same culture and discipline and apply it to the protection of private information.

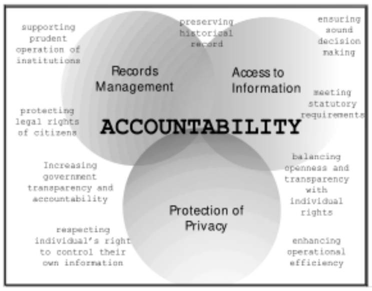
- For me, this means that information is an asset and just like money, property or other more tangible government assets, we need to apply the rules and procedures to protect it.

[additional material]

- …information is not recognizable as a balance sheet asset — even though information meets all the criteria… -Douglas Laney, VP, Gartner

Comment [MS4]: CITZ

Slide 4



supporting prudent operation of institutions

preserving historical record

ensuring sound decision making

Records Management

Access to Information

meeting statutory requirements

protecting legal rights of citizens

ACCOUNTABILITY

Increasing government transparency and accountability

balancing openness and transparency with individual rights

Protection of Privacy

respecting individual's right to control their own information

enhancing operational efficiency

Which leads me to the foundations for today's material, or the three central areas of relevance – Records Management, Access to Information, and Protection of Privacy.

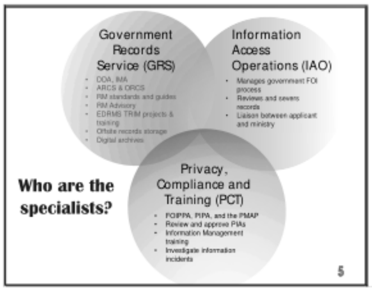
- Generally, these are codified in legislation including the *Freedom of Information and Protection of Privacy Act* (or FOIPPA) and the *Information Management Act* (the IMA)
- These responsibilities fall into three general areas:
  - Records Management which is primarily governed by the IMA; and
  - Access to Information and Privacy which fall~~s~~ under FOIPPA.

- Collectively, these three disciplines drive the outcomes we see here – and which British Columbians expect:
  - supporting prudent operation of institutions
  - preserving our historical record
  - ensuring sound decision making
  - balancing openness and transparency with individual rights
  - enhancing operational efficiency
  - respecting individual's right to control their own information
  - Increasing government transparency and accountability
  - protecting the legal rights of citizens; and,
  - meeting other statutory requirements

Comment [MS5]: Same comment as in June: This does not match the version of the slide that was used in the staff training. CIRMO worked together on the refined "objectives" for that slide, and those ought to be reflected here.

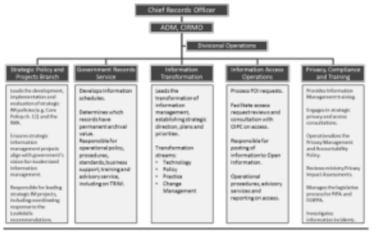
Comment [MS6]: We have repeatedly requested that this word be removed and would appreciate this advice being accepted. Records Management is no more "primarily" governed by the IMA than privacy and access are "primarily" governed by FOIPPA. This modifier is inaccurate and misleading.

Slide 5


Government Records Service (GRS)
DOA, IMA
ARCS & ORCS
RIM standards and guides
RIM Advisory
EDRMS TRIM projects & training
Offsite records storage
Digital archives
Information Access Operations (IAO)
Manages government FOI process
Reviews and severs records
Liaison between applicant and ministry
Privacy, Compliance and Training (PCT)
FOIPPA, PIPA, and the PMAP
Review and approve PIAs
Information Management training
Investigate information incidents
Who are the specialists?
5

Each of these three branches, all within CIRMO, provide a lot of **services** that we will **not talk about today** – but **for today**, we can boil it **down to rough terms** for the topic at hand.

So the Privacy branch is responsible supporting ministries in operationalizing ~~for~~ the privacy portions of the Freedom of Information and Protection of Privacy Act - FOIPPA for short. Information Access Operations, or IAO, manages the Access to Information, or FOI requirements of FOIPPA. And Government Records Service, or GRS, is supporting ministries in operationalizing the~~responsible for records management policy and the operations of the forthcoming~~ Information Management Act.

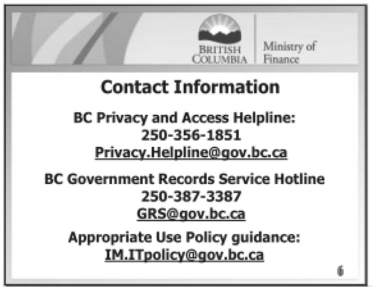

Chief Records Officer
ADM, CIRMO
Divisional Operations
Strategic Policy and Projects Branch
Leads the development, implementation and evaluation of strategic IM policies (e.g. Core Policy ch. 12) and the IMA.
Ensures strategic information management projects align with government's vision for modernized information management.
Responsible for leading strategic IM projects, including coordinating response to the Loukidelis recommendations.
Government Records Service
Develops information schedules.
Determines which records have permanent archival value.
Responsible for operational policy, procedures, standards, business support, training and advisory service, including on TRIM.
Information Transformation
Leads the transformation of information management, establishing strategic direction, plans and priorities.
Transformation streams:
Technology
Policy
Practice
Change Management
Information Access Operations
Process FOI requests.
Facilitate access request reviews and consultation with OIPC on access.
Responsible for posting of information to Open Information.
Operational procedures, advisory services and reporting on access.
Privacy, Compliance and Training
Provides Information Management training.
Engages in strategic privacy and access consultations.
Operationalizes the Privacy Management and Accountability Policy.
Reviews ministry Privacy Impact Assessments.
Manages the legislative process for PIPA and FOIPPA.
Investigates information incidents.

Comment [MS7]: Where is SPL in this diagram. Our recollection is that there have been discussion about replacing with the indented org chart we use in other training?

Comment [MS8]: SPL is responsible for FOIPPA

Comment [MS9]: Not true. This is SPL's role

Slide 6



BRITISH COLUMBIA | Ministry of Finance

Contact Information

BC Privacy and Access Helpline:
250-356-1851
Privacy.Helpline@gov.bc.ca

BC Government Records Service Hotline
250-387-3387
GRS@gov.bc.ca

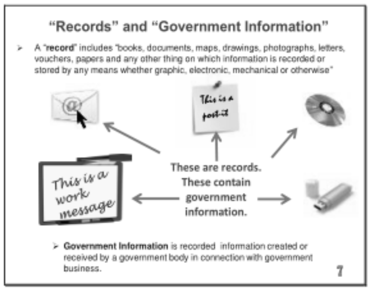
Appropriate Use Policy guidance:
IM.ITpolicy@gov.bc.ca

6

In the event that you have any questions at all, either based on this training, or on the topic areas generally, then we have 3 great resources for you. You can direct any general privacy or access question through the Privacy and Access Helpline – if it is a question specific to a request, then you can direct your question to your DMO FOI Liaison – which is a new role that will function as your primary contact on access matters and liaise between IAO and your office. For any records management questions, about transitory records, records retention, disposition, ARCS/ORCS, etc., then you can call the GRS Hotline. ~~Finally, we will touch on Appropriate Use Policy and if you have any questions about that, you can contact the email noted here.~~ Finally, if you have any questions about how to interpret or apply any IM policies, including core policy or the appropriate use policy, You will see this slide again, just to remind you of how important and great of a resource these are.

Comment [MS10]: We have also repeatedly asked that "Appropriate Use Policy Guidance" be corrected here to refer to any IM policies. Apprecte you making the change in this round of revisions.

Slide 7



“Records” and “Government Information”

- A “**record**” includes “books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by any means whether graphic, electronic, mechanical or otherwise”

This is a post-it
This is a work message

These are records. These contain government information.

- **Government Information** is recorded information created or received by a government body in connection with government business.

7

- So now, we can jump into our actual content and start getting **refreshed** on information management.

- Most of what we need to know in the area of information management focuses around the concepts of a “record” and “government information”, so it is important that we share a common understanding of these terms.

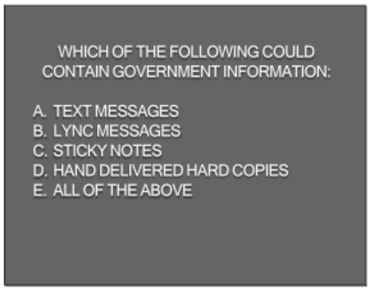
- A "record" is defined in ~~legislation~~ FOIPPA to include: books, documents, maps, drawings, e-mails, and any other places where you have put pen to paper, or typed something into a computer program. This definition is broad enough to include less obvious things like post-it notes stuck to your computer, text messages, and even Lync messages. So for the purposes of access to information or the protection of privacy, it’s this concept that you should keep in mind.

- Government Information is defined in the IMA as information created or received by a government body in connection with government business. When you’re thinking about records management, this is the concept to bear in mind.

- These two terms — “record” and “government information” are sometimes used interchangeably, and they are pretty similar.

- What’s important to understand is that in both cases it is the content and not the medium that matters.

Slide 8



WHICH OF THE FOLLOWING COULD CONTAIN GOVERNMENT INFORMATION:

A. TEXT MESSAGES
B. LYNC MESSAGES
C. STICKY NOTES
D. HAND DELIVERED HARD COPIES
E. ALL OF THE ABOVE

We’ll start with a bit of a knowledge test here… Which of the following could contain government information? Text messages, Lync Messages, Sticky Notes, hand delivered hard copies or all of the above.

The answer here is E - all of these could contain government information. it’s important that we understand that It doesn’t matter what medium is used to produce a record. What makes it government information is the context and, perhaps most importantly, the content - and that the information in the record relates to government business.

This is a great time to emphasize that **ownership** of media or hardware doesn’t determine the ownership of the record – or **whether** something is ~~a record~~government information for records management purposes or a record of the purpose of FOI, for that matter. What I mean is, if you use your personal iPad ~~because~~because you're unexpectedly asked to comment urgently on a document while you’re on vacation without your government-issued device ~~your laptop battery just died –~~ the ~~records~~ work you produce on the iPad are still ~~considered records– in fact they are still~~ considered **government** information for records management purposes and they may still be subject to FOI, security and confidentiality protections, and other policy requirements ~~records~~. So, regardless of the fact that you used your own device. You need to treat that record just as you should any other containing

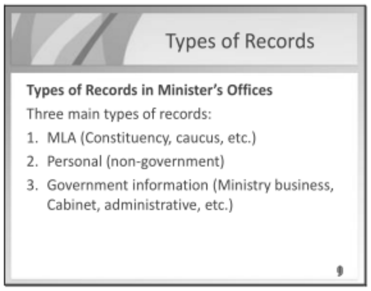
Comment [MS11]: This would not likely be the kind of extenuating circumstance App Use contemplates.

Formatted: Font: Not Bold

Formatted: Font: Not Bold

government information – with the first step being to get it back on the government network and ~~removing~~ remove it from your personal iPad as soon as you have done that. There is more guidance on situations where it **is** and **is not** appropriate to use your own device in managing records, and that is in the Appropriate Use Policy. You need to know that ~~it~~ this is only permitted in extenuating circumstances, and should be avoided where possible.

Slide 9



Types of Records

Types of Records in Minister's Offices

Three main types of records:

1. MLA (Constituency, caucus, etc.)
2. Personal (non-government)
3. Government information (Ministry business, Cabinet, administrative, etc.)

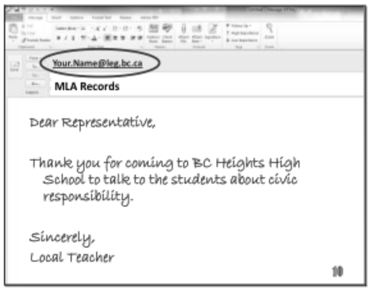
9

- In order to best understand our records management and ~~our~~ access obligations we need to review the different types of record that your offices hold.

- In a Minister's Office there are three main types of records that you will deal with. I'm going to go into the details for each of these separately, but to start, in your work you likely deal with MLA, records that are strictly personal, and then those that are considered government records.

- Of course, these types of records may overlap – say, when your office receives a constituent email to the MLA but the email is then acted upon in the capacity of the Minister. It's important that these two distinct roles are reflected as such in your record keeping practices. However, if records blend – your government records obligations will apply, including provisions under FOIPPA including responsibilities to protect privacy and provide access to these records, and your obligations under IMA to manage them appropriately.

Slide 10



Your.Name@leg.bc.ca

MLA Records

Dear Representative,

Thank you for coming to BC Heights High School to talk to the students about civic responsibility.

Sincerely,
Local Teacher

10

- MLA records are records created, accumulated or used by when the Minister is acting in his or her MLA capacity. MLA records can include communications, speeches and meeting records with constituents about MLA business, Caucus committee meetings or records produced for Committees of the Legislative Assembly.

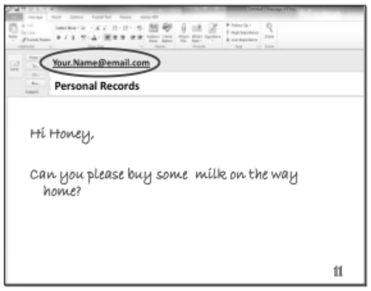
- Considering the purpose for the communication can support you in determining which type of record is appropriate. For instance, when a constituent asks a Minister to support them with an issue that is outside of the Ministerial portfolio, this would be an MLA record. If the question is within the Ministerial portfolio or the Minister moves from an advocacy role to that of an official decision making role, this same original record should be viewed as government information. You should also consider how the materials are received, for example, whether it was received to your legislative email account.

- Use of letterhead, titles and salutations in correspondence should also be considered to ensure that the record is being appropriately actioned in either an MLA or Minister capacity.

- This means that this thank you note we see here from the School District would be an MLA record. And due to the material's content and distribution through the dedicated leg.bc.ca email account, it would not be covered by the Information Management Act or FOIPPA.

- Finally, care should also be exercised to ensure that MLA records in your office are not inappropriately distributed through the government email system as again they may become subject to FOIPPA's specific privacy and access provisions.

Slide 11



Your.Name@email.com

Personal Records

Hi Honey,

Can you please buy some milk on the way home?

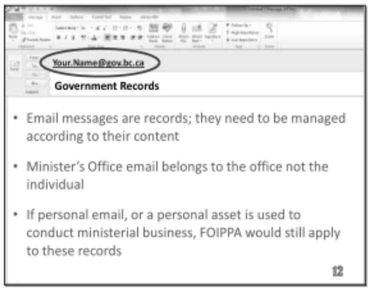
11

- Personal records are records that are, as the name suggests, personal in nature. They relate to your private life or personal interests and are not received or created as part of your daily ministry or constituent business activities. Examples would include personal invitations, communications with family or friends (on non-government business), etc. These records, similarly **are not** covered by records management rules or privacy and access legislation, so we will again not linger on this type of record either, except to say that these records must be maintained separately from other records as much as possible. It is important to recognize here that not only will you be required to manage your own personal records, but may also encounter the personal records of the Minister, especially if in your capacity you deal with the Minister's calendar or correspondence (mail/email).

- I would also like to stress that it is not the medium, the device or the format that dictates that something is personal, it is the **content** and **context**. For example, we understand that you can't restrict an individual from sending a work-related email to your personal account. It's important that we are clear that email, or any other work-related records produced on personal email or personal devices **are not** considered personal records, those are considered government records.

- Further, personal email accounts should never be used to carry out government business, except in extenuating circumstances. When it is used, there are rules you need to follow. This includes copying emails to your government email address, deleting the information from your personal account as soon as you can, and ensuring you have shared the least amount of sensitive information that is necessary in the circumstance.

Slide 12



Your.Name@gov.bc.ca

Government Records

- Email messages are records; they need to be managed according to their content
- Minister's Office email belongs to the office not the individual
- If personal email, or a personal asset is used to conduct ministerial business, FOIPPA would still apply to these records

12

- What that leaves us with, after we remove personal and MLA records from the conversation is **"Government records",** which is essentially everything else.

- **Government** records, **including all those records that are produced in a Ministerial Office**, are covered by the IMA's records management requirements and FOIPPA's access and privacy requirements.

- It is also important to point out that government records belong to your ministry and not to the person who sent or received them.

- Lastly, it is important that I emphasize that triple deleting email is never permitted.

I'm going to dig a bit deeper into a **few of these following examples** in a moment, but to get your minds around what we mean when we say government records, think about all of the types of records one might accumulate in the course of the daily administration of a ministry:

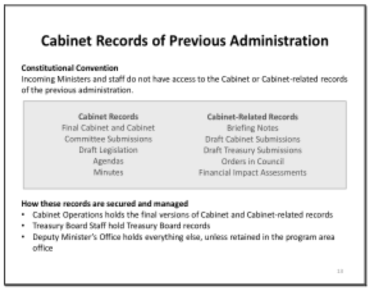
- Cabinet and Treasury Board submissions
- CLIFF records, emails, calendars
- Meeting minutes, agendas and handouts
- Planning and performance reviews and evaluations

- Texts and instant messages
- briefing notes, backgrounders, presentations and speaking notes.

This would also include both official records and transitory records – which we will discuss a little later.

For the moment, we are going to talk about three specific types of records that you will encounter frequently, and then discuss a few tips around how to manage these types of records.

Slide 13



Cabinet Records of Previous Administration

Constitutional Convention
Incoming Ministers and staff do not have access to the Cabinet or Cabinet-related records of the previous administration.

Cabinet Records
Final Cabinet and Cabinet Committee Submissions
Draft Legislation
Agendas
Minutes

Cabinet-Related Records
Briefing Notes
Draft Cabinet Submissions
Draft Treasury Submissions
Orders in Council
Financial Impact Assessments

How these records are secured and managed
- Cabinet Operations holds the final versions of Cabinet and Cabinet-related records
- Treasury Board Staff hold Treasury Board records
- Deputy Minister's Office holds everything else, unless retained in the program area office

13

- Given the recent election, I first want to call your attention to a specific protocol that applies during and after the transition to all new administrations. This protocol applies to Cabinet records and Cabinet-related records. While these types of records are highly confidential and are always protected, additional rules around how they are secured and managed come into play after an election.

- **Cabinet Records** are those that have been prepared for submission to or circulated for consideration by Cabinet or a Cabinet Committee. Cabinet records may include agendas, minutes, final versions of Cabinet and Cabinet Committee submissions, decision letters of Cabinet and its committees, staff analysis, draft legislation, regulations and Orders in Council circulated for consideration by Cabinet, presentation decks and papers.

- **Cabinet-Related Records** are records held by public bodies that are created or received by the public body, which may reveal the substance of deliberations of Cabinet or a Cabinet Committee. This may include: correspondence including email correspondence, briefing notes, drafts of Cabinet or Treasury Board submissions, draft regulations and Orders in Council, financial impact assessments, and memoranda regarding confidential work for the consideration of Cabinet.

- **Constitutional convention -** Established Constitutional convention requires that all records which may reveal the substance of deliberations of a prior Cabinet or its committees are treated as privileged information of that government. This means an incoming administration (i.e., incoming Ministers and political staff) does not have access to these documents without the express consent of the outgoing administration (during/after transition, by approval of the DM responsible and the outgoing Premier or delegate)

- So what happens to these records? Cabinet Operations or Treasury Board Staff hold the final versions of Cabinet Records and Cabinet-Related Records. Where the Cabinet record or Cabinet-related record is an integral part of ministry business files, a copy should be retained in the relevant operational/business unit files. These copies of Cabinet confidential records must be kept secure to ensure no unauthorized access, and must only be accessed by members of the public service, and on a need-to-know

- In responding to requests of a new government, the proper procedure is for staff to paraphrase the information in the records and/or prepare new reports and submissions, rather than simply providing copies of old ones. Previous Cabinet submissions and materials used in their preparation may continue to be used as resource documents by Public Service staff preparing new submissions .

[content below for reference and to be used as needed]

- Although a new administration is precluded from viewing the records of a previous administration, it is generally permissible for a new administration to obtain information about decisions made by a previous administration, particularly where the information is necessary to ensure that government business will be carried out effectively.

- After a change in administration occurs, in providing advice to the new Executive Council, where the continuity of administration requires reference to records prepared for previous Executive Councils, it may be appropriate to paraphrase the contents of those materials.

- However, in disclosing information about the decisions made by a prior administration, employees must take care to continue to protect information about the options presented to the Executive Council in making the decision and any information related to the opinions

Slide 14

Cabinet Submission - Request for Decision

Minister:

Ministry:

Date:

Title:

New Cabinet Records

Manage Cabinet records separately (i.e. don't mix them in with other types of records), in accordance with Cabinet Operations directions

Final versions of Cabinet records are retained by Cabinet Operations

Cabinet submissions and draft submissions must be kept and disposed of securely (i.e., no unauthorized access).

14

While we have spoken about how Cabinet records from previous administrations are treated, we must also speak about how Cabinet records created by the new government should be managed.

It's important that you **have**, or develop a system to manage Cabinet records separately from other government records. Cabinet records should not be mixed in with other types of records. **Final versions** of Cabinet records are retained by Cabinet Operations. So, you should follow Cabinet Operations directions on how you should manage these records.

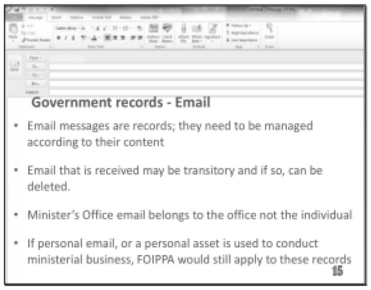
It is important that you keep and dispose of draft and final Cabinet submissions **securely**. This is true of all government records, but there is an inherent need to protect Cabinet integrity that may require **additional** security measures.

This also seems like an important time to highlight that these types of records – as with the other types of government records we have discussed - **are** responsive to FOI requests. This means that if you have cabinet records that respond to an FOI request, you would provide them to your DMO FOI Liaison. It is **your** responsibility to ensure that when providing cabinet records to DMO FOI Liaison that they are made aware of this sensitivity. They will ensure IAO is made aware of this sensitivity so they are able to review the records and apply severing recommendations that will protect any cabinet confidences. You ~~have to~~can rely on **FOIPPA exceptions** to dictate what records can be withheld from release and IAO will guide you here. In general, Cabinet confidential information is mandatorily withheld from disclosure, with a few exceptions, e.g. here the record has been in existence for over 15 years.

We are going to move from talking about specific record types or concepts that can be applied to all records – namely the record lifecycle.

Comment [MS12]: This is not what the next slide does.

Slide 15



Government records - Email

- Email messages are records; they need to be managed according to their content
- Email that is received may be transitory and if so, can be deleted.
- Minister's Office email belongs to the office not the individual
- If personal email, or a personal asset is used to conduct ministerial business, FOIPPA would still apply to these records

15

The next record example I'll walk you through is government email. It is important to remember that work emails contain government information. How you manage email depends on its content. You may have heard the misconception in public that all emails are transitory. We'll deal with this concept of transitory in a moment – but for now, just remember that an email **is** a record. This is important because it is actually the content of that email that determines its value. The form of the record – the fact that it is an email - isn't a factor in determining whether or not you need to keep it.

I also want to reiterate the point that your email records that pertain to government business, are government records no matter the email account you are using, but you should also avoid using your personal email account to do your work. In the extenuating circumstance when you absolutely must do so, there are rules you have to follow, which include "cc-ing" your government email account, deleting the emails from your personal email account as soon as possible, and ensuring you share the least amount of sensitive information that is necessary in the circumstance. Where that sensitive information is someone's personal information, use additional caution to ensure that it is adequately protected. In general, personal information cannot be shared outside of Canada. We will review data residency requirements later in this material.

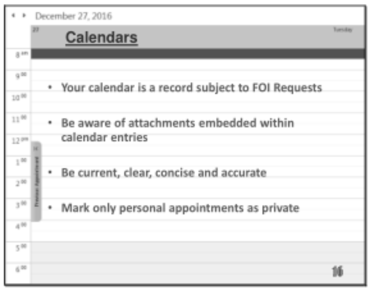
I want to share some email management tips here. These are not mandatory requirements, but instead are strategies that you can implement to support you in creating records that are more manageable when responding to an FOI request. You know your work and therefore you are able to determine which emails are important to that work. If you have emails with information that will either be useful to document the work of your office or for others in doing their work, then you should file those emails in your office recordkeeping system. Likely, for most of you, this won't be a significant number of your emails. Most of the information we share by email is repeated in other documents and is already stored elsewhere. But if you think the email contains the only copy of an important piece of information, you should save a copy, or use the email to prepare a formal document and then dispose of it.

It can be challenging to manage emails when they contain a lot of different topics or move into overlapping and lengthy threads. If you can, try to be specific, to limit the content of your email to one subject area, and to clean up email chains and lengthy threads. You should also try to stay on top of tasks like regularly deleting transitory email. Many emails are only of temporary use and are therefore considered transitory.

For example, a ministry-wide notice to all employees can usually be disposed of as transitory. It is the responsibility of the initiating office to file and maintain an official copy, in their office recordkeeping system.

Lastly, it is important that I emphasize that triple deleting email is never permitted. If you don't know what triple deleting is, then don't worry, this is not something you can accidentally do.

Slide 16



Calendars

- Your calendar is a record subject to FOI Requests
- Be aware of attachments embedded within calendar entries
- Be current, clear, concise and accurate
- Mark only personal appointments as private

16

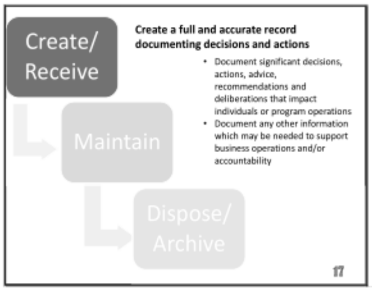
The final records example I wanted to highlight is Outlook calendars. As you may know, A Ministerial Directive under FOIPPA requires the monthly disclosure of calendars of Minister, Deputy Ministers, Associate Deputies, and Ministers of State. To facilitate consistency and ensure security in making these disclosures, certain practices need to be maintained within your offices

Calendars should be maintained so that entries are consistent, clear and current. You can do this by keeping the subject heading for meetings informative and concise. You can keep your calendar current by updating the calendar as changes occur. This means removing meetings that did not occur or were not attended and by updating the calendar entry to reflect who actually attended a meeting. And as for **personal** appointments - like a dentist appointment or a reminder to pick up the kids from school, mark these as **private** – that way details will not show up in a printed copy or to anyone other than the calendar owner or a delegate. However, you need to ensure that **only personal appointments** that are labeled as "private".

If you are interested in receiving a dedicated training session on how to maintain calendars contact your DMO FOI Liaison – their contact information is in your resource package.

We are now going to move from talking about specific record types or concepts that can be applied to all records – namely the record lifecycle.

Slide 17



Create/ Receive

Maintain

Dispose/ Archive

Create a full and accurate record documenting decisions and actions

- Document significant decisions, actions, advice, recommendations and deliberations that impact individuals or program operations
- Document any other information which may be needed to support business operations and/or accountability

17

Now it's time to talk about what to do with government information, from the beginning to the end of its lifecycle. The lifecycle of government information is simple - information is created or received, you use and maintain it, and then the information is either disposed of or sent to the government archives. Some information only lives for a few minutes or hours, and some is never disposed of, but rather is permanently preserved in the government archives.

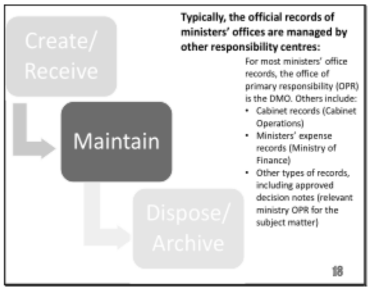
Comment [MS13]: As we have previously advised, this cannot say "full and accurate" as the legal obligation refers to 'Adequate" as the test.

Always ensure that you are creating a full and accurate account of decisions and actions that support business operations. We will now walk through each stage of the lifecycle of government information in order to learn more about it. We'll use an example to make these stages easier to understand. Think about a project where your office is leading a large project involving several offices across different divisions of your ministry.

Create/Receive

As you work on the project, you naturally create and receive government information, such as a project charter, meeting agendas and minutes, email correspondence, and project plans and reports. To have a full and accurate record of the project, you need to have documentation of significant project activities, decisions and results.

Slide 18



Create/ Receive

Maintain

Dispose/ Archive

Typically, the official records of ministers' offices are managed by other responsibility centres:

For most ministers' office records, the office of primary responsibility (OPR) is the DMO. Others include:

- Cabinet records (Cabinet Operations)
- Ministers' expense records (Ministry of Finance)
- Other types of records, including approved decision notes (relevant ministry OPR for the subject matter)

18

As you create and receive government information, it is important to ensure that you maintain the information so that it is available to those who need it and is kept for the required length of time. You should always retain information that details significant activities of your unit, as well as changes to existing programs or the establishment of new ones.

Going back to our example, any information that is needed by your office to perform or document project activities must be filed in your office recordkeeping system. You can file these temporarily, in a collaboration system such as SharePoint, but be sure to transfer them to the recordkeeping system when you have wrapped up the project.

A recordkeeping system is a shared system organized according to government information schedules. Two examples of office recordkeeping systems are an appropriately organized office network drive, sometimes called your "LAN", or the government Enterprise Document and Records Management System (EDRMS), known as TRIM. This office recordkeeping system does not include locations that are only available to you, such as your desktop, home drive or the hard drive of your computer.

Your office may also use other information systems for recordkeeping, such as SharePoint. This is fine, as long as they have appropriate information management controls, including use of information schedules. These schedules specify how long each category of information must be kept. Within the office recordkeeping system for government we use ARCS, which stands for the Administrative Records Classification System, and ORCS, which stands for Operational Records Classification System.

Comment [MS14]: This contradicts what you have just said, above, about moving records off of SP once a project is wrapped up.

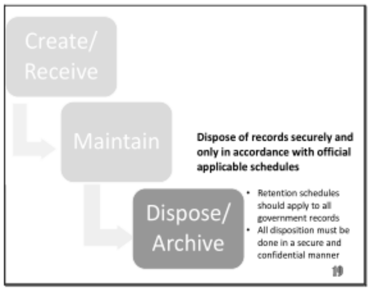
In our example, project information would be categorized according to the ARCS classification for large administrative projects. Of course, not all government information has to be kept - and this will be discussed later.

Since your project involves multiple offices of your ministry, you will need to be clear about which office is the office of primary responsibility (or "OPR") for the project. The OPR maintains the official file copy of government information. For most records involving the minister's office, the OPR is the Ministry's DMO. The DMO is able to provide continuity and appropriate public service administration of the records of successive ministers.

Minister's office official records need to be retained at minimum for 10 years (under the Executive records schedule), after which they are reviewed by an archivist before archival selection. Other examples of OPRs include Cabinet Operations as OPR for Cabinet records; and Ministry of Finance as OPR for Minister's Office expense records.

In our example, you are the project lead and your Ministry's DMO is the OPR. If other offices in your ministry need to keep copies of project information for their own business purposes, they can keep them as "non-OPR" copies and dispose of them when they no longer need them.

Slide 19



Dispose of records securely and only in accordance with official applicable schedules

- Retention schedules should apply to all government records
- All disposition must be done in a secure and confidential manner

19

So, now that we know with whom and where records are maintained, we can talk about disposition. Information schedules provide timetables which tell us how long different types of information is needed and when the information may be disposed of or sent to the government archives.

This is important because you cannot dispose of information unless there is an information schedule to authorize it. Some information schedules identify information that must never be disposed of, but rather must be maintained until it is ready to be transferred to the government archives. Transitory information has its own information schedule that allows you to dispose of the information when it is no longer useful. You will learn more about transitory information shortly.

All disposals must be carried out in a secure and confidential manner. The more sensitive information is, the more measures we have to take to ensure it is securely and appropriately disposed of. Your Records Officer in the Government Records Service (GRS) can help with this.

Returning to our example, once the project is completed or cancelled and a further two years have elapsed, your project file can be disposed of. This meets the requirements established in ARCS for large-scale projects.

Slide 20

Transitory Records

tran·si·to·ry

/ˈtransəˌtôrē, ˈtranzəˌtôrē/

adjective

records that are of temporary usefulness and are needed for only a limited period of time in order to complete a routine action or prepare an ongoing record

"transitory records may be deleted when they are no longer useful"

More

Translations, word origin, and more definitions

20

- Good records management dictates that we need to retain records of value and dispose of records of temporary value, once they are no longer useful.

- This is best practice in information management and is essential for appropriately handling the escalating volume of records that government has in its control.

- ~~David Loukidelis' December 2015 report reinforces this best practice and he noted that t~~The province receives 284 million emails annually.

- In his December 2015 report, ~~Mr.~~ David Loukidelis likened~~s~~ good records management practices to ~~that of~~ good household management, saying that retention of all electronic records is an inappropriate practice akin to hoarding, and should be avoided at all cost.

- Information schedules, approved or continued under ~~the Document Disposal Act, or by Chief Records Officer under~~ the Information Management Act , define criteria as to whether a record is an official government record which **must** be retained or is a transitory government record which **may** be disposed of. Even transitory information has its own information schedule that allows you to dispose of information when it is no

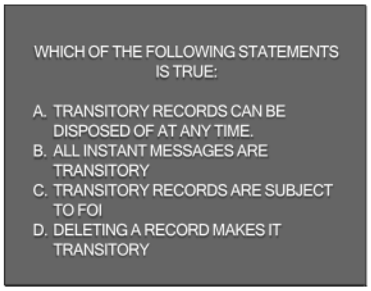
Comment [MS15]: New administration has signalled they are less interested in Mr. Loukidelis and his findings. May be better to present this fact without the context of the report. It remains true regardless of source (in fact, we provided this stat to David in the first place).

longer useful.

- Simply put:
  - **Official** government records **must** be retained within the Minister's Office or an OPR such as the Deputy Minister's Office; and,
  - **Transitory** government records may be disposed of – following an assessment that they are appropriately categorized as transitory.

It may be surprising how something that seems so simple on the surface can become fairly complex. So, let's do a deeper dive into the concept of transitory records. Starting with a test of your knowledge.

Slide 21



WHICH OF THE FOLLOWING STATEMENTS IS TRUE:

A. TRANSITORY RECORDS CAN BE DISPOSED OF AT ANY TIME.
B. ALL INSTANT MESSAGES ARE TRANSITORY
C. TRANSITORY RECORDS ARE SUBJECT TO FOI
D. DELETING A RECORD MAKES IT TRANSITORY

Which of the following statements is TRUE:

- Transitory Records can be disposed of at any time. (FALSE)
- All Instant Messages are transitory. (FALSE)
- Transitory Records are subject to FOI. (TRUE)
- Deleting a record makes it transitory. (FALSE)

So, the correct answer is "c". All transitory records are subject to FOI requests. And because of that, if you receive an FOI request any transitory records that exist at that time, may be responsive to that FOI request. In other words, if you have an FOI request, you **cannot delete** the responsive transitory records. ~~You may have~~While you were ~~**been**~~ **able** to delete them previously, ~~but~~ if you kept them, they are responsive to the request and you must provide them to IAO.

Slide 22

“ It is a record’s content and context that determines whether a record is transitory, rather than its form

- Elizabeth Denham, Information & Privacy Commissioner

One of the things I really want you to take away from our training today is a very clear understanding that it is the **content, context** or **value** of a record, not the record’s form that you need to consider. In other words, **emails** should not be considered transitory. Instead, the content of a specific email may be. Ditto on instant messages. While most people don’t conduct serious business over Lync or text message, if they do, those records need to be kept and filed appropriately.

In terms of a definition,

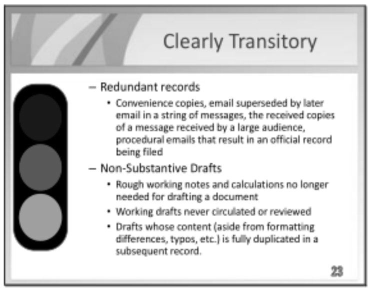
Transitory records are of **temporary** usefulness and are needed for only a **limited period of time** in order to complete a **routine** action or prepare an ongoing record.

- They are not required to **document decisions** and actions or to support ongoing government business.
- They are not **regularly filed** as standard records
- They are not required to meet statutory requirements, **or**
- They are **redundant,** extra copies

This will come up a few times, but I want to reiterate that once an FOI request has been received, transitory records are subject to the request and **cannot be deleted** and must be provided in response to an FOI request. It doesn’t matter that you could have deleted the record. If you have it at the time the request is received, it is responsive to that FOI request and must be provided to IAO through your DMO FOI Liaison.

Comment [MS16]: You’ve just said this, above.

Slide 23



Clearly Transitory

- Redundant records
  - Convenience copies, email superseded by later email in a string of messages, the received copies of a message received by a large audience, procedural emails that result in an official record being filed
- Non-Substantive Drafts
  - Rough working notes and calculations no longer needed for drafting a document
  - Working drafts never circulated or reviewed
  - Drafts whose content (aside from formatting differences, typos, etc.) is fully duplicated in a subsequent record.

23

- So, how does your office determine if something is transitory? I am going to walk you through some examples to try to illustrate the decision making process in the context of the records that are produced in a Ministerial office.

- Duplicated information is a good example of what can be transitory. Imagine a typical email conversation that goes something like this:

  - Email from another office: “Have you considered the proposal that we talked about?”
  - You respond: “Yes, I like the idea, could you please send it in writing?”
  - Other office: “Here it is. Tell me if you need any changes.”
  - You: “Your proposal (attached) is approved.”

- In this simple example, you will end up with four emails, two sent and two received. Each of which contains the previous emails. In this example, you can feel confident deleting the first three emails if you are retaining the fourth, as the fourth contains the entire chain, as well as the decision.

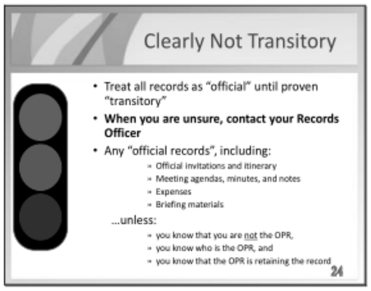
- As another example, if you make a handwritten note while you are listening to a voicemail, and then copy your note into an email, you can delete the voicemail, and dispose of your handwritten note as transitory.

- Non-substantive prior drafts, which can include those that contain changes to elements like the formatting and margins, or corrections to grammatical errors are also transitory. Drafts that were never circulated or reviewed are also considered non-substantive.

- Even though transitory information may be disposed of when it is no longer required, it is unlawful to delete or destroy any transitory record that is the subject of a current FOI request.

- Transitory records also must not be deleted where they may be relevant to a current or an expected future legal action.

Slide 24



Clearly Not Transitory

- Treat all records as “official” until proven “transitory”
- **When you are unsure, contact your Records Officer**
- Any “official records”, including:
  - Official invitations and itinerary
  - Meeting agendas, minutes, and notes
  - Expenses
  - Briefing materials

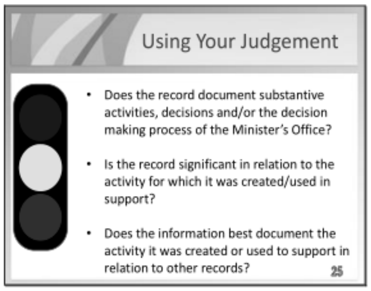
…unless:

- you know that you are not the OPR,
- you know who is the OPR, and
- you know that the OPR is retaining the record

24

- On the other end of the spectrum, there are those records that are clearly **not** transitory.
- Information that is clearly not transitory would include incoming public correspondence, meeting minutes, and case files. You may, however, have copies of information such as meeting minutes that are transitory, provided that:
  - You know that you are not the Office of Primary Responsibility or OPR, and
  - Your office has no need to file your copies for its own business use.

Slide 25



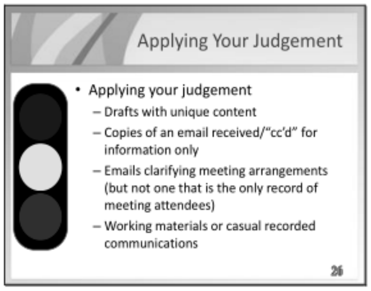
Using Your Judgement

- Does the record document substantive activities, decisions and/or the decision making process of the Minister's Office?
- Is the record significant in relation to the activity for which it was created/used in support?
- Does the information best document the activity it was created or used to support in relation to other records?

25

- When faced with information that is neither clearly transitory or official, you will need to ask yourself these questions:
    - Does the information document an important activity, or decision?
    - To what extent is this already documented somewhere else?
    - Is the information important in relation to the activity for which it was created or which it was used to support?
    - In relation to other information, does this information best document the function or activity for which it was created or which it was used to support?
- If you are unsure as to whether something is transitory or not, you can contact your Records Officer in the Government Records Service (GRS) for assistance.

Slide 26



Applying Your Judgement

- Applying your judgement
    - – Drafts with unique content
    - – Copies of an email received/"cc'd" for information only
    - – Emails clarifying meeting arrangements (but not one that is the only record of meeting attendees)
    - – Working materials or casual recorded communications

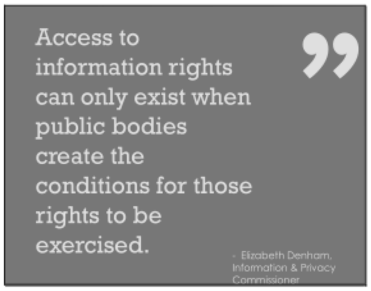
26

I've got a couple examples here that are meant to make you second guess things a little bit and demonstrate that you shouldn't make broad-brushed assumptions about types of records, and that records need to be assessed on a case by case basis.

As I have said, drafts can be transitory, however, some drafts will have unique content. The determination depends on the unique content. If a change is to an editor's comment suggesting a change of one particular word – this would suggest it is transitory. However, if the one particular word that is changed is "approved" from "not approved", then that is definitely not a transitory record. And this is a good example on why "draft" – "or minor edits" does not equal "transitory".

I know that this can seem complicated, but you are all trusted public service employees who have been empowered to make these decisions. If you are not confident that a reasonable, disinterested outsider would agree with you, then you should refer to the transitory records guide, and if you are still unsure it's important that you consult with a Records Officer.

Slide 27



Access to information rights can only exist when public bodies create the conditions for those rights to be exercised.

- Elizabeth Denham, Information & Privacy Commissioner

So why the focus on transitory records? We want to make sure that you are keeping the right records so that those records are available for accountability purposes. As the Commissioner recently said "Good governance and good record keeping go hand in hand"

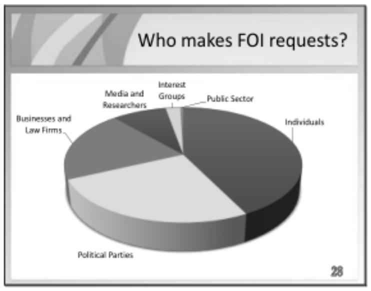
More to the point of what we will be discussing next, here is a quote from the Information and Privacy Commissioner from her most recent report:
"Access to information rights can only exist when public bodies create the conditions for those rights to be exercised"

~~While~~ Records Management does not exist solely for the benefit of FOI – there are a **number of reasons** why Records Management benefits us both internally and externally. **However**, without strong Records Management practices, it is very hard to effectively manage FOI.

It is one of the key "conditions" that allows Access to Information rights to be exercised.

Next, I am going to remind you of your obligations in responding to an FOI request and supporting government's commitment to Access.

Slide 28



Who makes FOI requests?

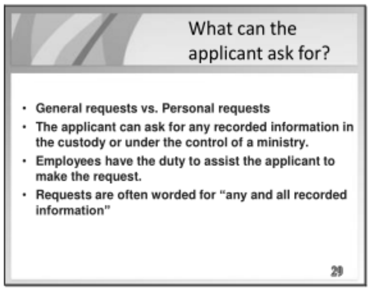
I have to assume that all of you know what an FOI request is, and have likely experienced one, even if you are still quite new. In simple terms, however, it is simply, an individual exercising their right to access government information. To become an "**FOI applicant"** an individual must submit a written request for access to a record. The request wording has to be **clear enough** and contain **enough detail** to enable an employee to identify the records sought.

Comment [MS17]: Really? What about new staff who have never supported a minister's office before?

An FOI request is **usually** submitted to IAO – although, if an employee outside of IAO receives a request it is still considered an FOI request. If this happens to you, you need to forward the request to IAO on the applicant's behalf – particularly because there are tight legislated time restrictions that have probably already started!

I have here a breakdown of the types of requesters that we get, but you should know, that none of this makes a difference as to what they receive, unless they are requesting their own personal information, which is the case with most of the individuals represented in this chart. Political parties get the same information media, researchers, interest groups or lawyers get.

Slide 29



What can the applicant ask for?

- General requests vs. Personal requests
- The applicant can ask for any recorded information in the custody or under the control of a ministry.
- Employees have the duty to assist the applicant to make the request.
- Requests are often worded for "any and all recorded information"

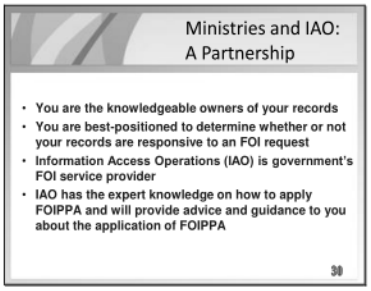
29

So what can an applicant ask for? To be honest, this is a bit of a trick question. An FOI applicant can ask for **any** record. They have the right to request any record, but this does not mean they have a right to **access** every record. To this effect, IAO will conduct a line by line review of any responsive records to ensure that information that is **legally appropriate** to be severed - or in other words, removed - prior to release has been highlighted as such.

Further, applicants must request **specific** records – because FOI is not built to **answer** questions, instead it is built to provide the records **that may answer** a question. What this means is you will find requests that are often worded as: "I want any and all records regarding the costs incurred constructing the 6-mile bridge" and not, "How much did the 6-mile bridge cost?". We will talk in a moment about duty to assist, but it is worth noting here, that if you do receive a request asking how much did the bridge cost, that just because they didn't "ask the question correctly" doesn't mean we are going to deny them records. We have a responsibility to be open and to connect people with the records to which they have a right to access.

I should point out, government does not need to rely on the FOI system to respond to questions from the public. If you are asked how much the 6-mile bridge cost, and you have that number readily available – an FOI request is not needed. FOI should be viewed as a last resort to support the objectives of an accountable and transparent government. There are other mechanisms for supporting these goals – like responding to a question directly and releasing records proactively.

Slide 30



Ministries and IAO:
A Partnership

- You are the knowledgeable owners of your records
- You are best-positioned to determine whether or not your records are responsive to an FOI request
- Information Access Operations (IAO) is government's FOI service provider
- IAO has the expert knowledge on how to apply FOIPPA and will provide advice and guidance to you about the application of FOIPPA

30

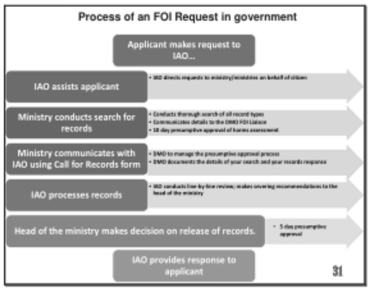
Ministries and Information Access Operations work in concert to respond to FOI requests. As a member of the public service, you are the subject matter expert of your records. You know what you have and whether or not what you have is responsive to an FOI request. You also know what information may be harmful if released.

To be very clear, you are not expected to know what section of FOIPPA may apply in terms of removing that information, but you are in the best position to identify information if something may be harmful if it were released. You are responsible for ensuring that this information is communicated back to IAO. What IAO needs to hear, is "if this information about the location of spirit bear' dens was released, I would be worried that hunters and curious well-wishers would both go out looking for them and disrupt the habitat". You don't need to know that there is a legislative exception that may exempt that information from release.

IAO is the expert when it comes to processing FOI requests. They have the expertise required to apply FOIPPA , to manage the legislated timelines and to communicate with the applicant with a customer focus. IAO also possesses the technology required to effectively sever records.

Your DMO FOI Liaison is just that – your liaison to support communication between IAO and the Minister's Office.

Slide 31



Process of an FOI Request in government

Applicant makes request to IAO...

IAO assists applicant
- IAO directs requests to ministry/ministries on behalf of citizen

Ministry conducts search for records
- Conducts thorough search of all record types
- Communicates details to the DMO FOI Liaison
- 10 day presumptive approval of harms assessment

Ministry communicates with IAO using Call for Records form
- DMO to manage the presumptive approval process
- DMO documents the details of your search and your records response

IAO processes records
- IAO conducts line-by-line review; makes severing recommendations to the head of the ministry

Head of the ministry makes decision on release of records.
- 5 day presumptive approval

IAO provides response to applicant

31

This graphic provides a high-level overview of the FOI process for government. I'll go through this for you in a moment, but first I want to underline that the whole point of this process is to create a system that will ensure an effective, customer focused information access process.

When a ministry receives a request they have thirty days to respond to that request (unless an extension is requested and approved), so as I move through this process keep that tight timeframe in mind.

1. and 2: Those thirty days start the moment the FOI applicant makes a request to IAO, who acts on behalf of ministries. Next, IAO assists the applicant to direct the request to the correct ministries – For the Minister's office, your requests are communicated to you through your designated DMO FOI Liaison.

3 and 4: Next, your office has ten days to conduct a thorough and accurate search for records. We'll get into what is required of you in more detail as we move through the presentation. For now, know you are required to communicate your search details, the harms that you perceive, and the records - or a "no records" response to your DMO FOI Liaison.

Your DMO FOI Liaison will document all of that information on the Call for Records form and relay that back to IAO. To be clear, you are responsible for conducting your own search for records. Your DMO FOI Liaison is responsible for overseeing the search process, including directing, monitoring, confirming and reporting on progress.

I want to flag something new for you here, and that is the presumptive approval process. Basically, that means that if you have provided records but have not provided formal harms or a formal approval within the ten days allotted by your DMO FOI Liaison, that person has the authority to proceed with the FOI process, presuming approval from your office.

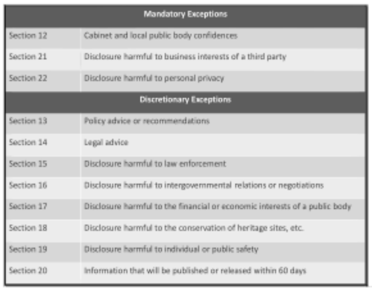
It may seem senseless to provide records knowing that harms recommendations or approval is not achievable within the allotted 10 days. I would recommend that your office provide responsive records in any case, to avoid triggering the newly implemented escalation process, which I will explain in a moment.

5. Getting back to the process, IAO then has 10 days to use the information to assess and conduct a line by line review of the record with the harms you provided, keeping Part 2 of FOIPPA in mind. In order to do a harms assessment, IAO needs to understand your concerns related to the potential sensitivity of records. IAO will assess the potential application of the legislation to the areas you have flagged as potentially harmful.

6. Next, your DM, the ultimate decision maker when it comes to Access requests, has 6 days to make a decision on releasing information based on IAO's recommendations. Should records need to be reviewed or approved by your office within this timeframe, MOs will be given 5 days before the DMO FOI Liaison will presume approval.

7. At this point, IAO has one day to release the appropriate records to the applicant.

Slide 32



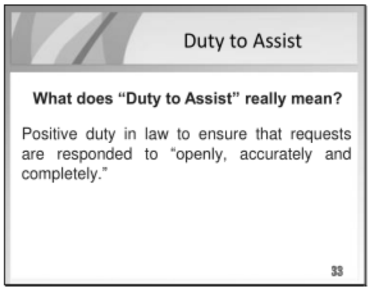
Mandatory Exceptions	
Section 12	Cabinet and local public body confidences
Section 21	Disclosure harmful to business interests of a third party
Section 22	Disclosure harmful to personal privacy
Discretionary Exceptions	
Section 13	Policy advice or recommendations
Section 14	Legal advice
Section 15	Disclosure harmful to law enforcement
Section 16	Disclosure harmful to intergovernmental relations or negotiations
Section 17	Disclosure harmful to the financial or economic interests of a public body
Section 18	Disclosure harmful to the conservation of heritage sites, etc.
Section 19	Disclosure harmful to individual or public safety
Section 20	Information that will be published or released within 60 days

Two of the steps I just mentioned – IAO conducting a line by line review of records, and the Deputy exercising their discretion about what information will be withheld and what information will be released – those steps are based on FOIPPA's legislated exceptions to disclosure. In other words, what you see on the slide are the reasons that a ministry can take out – or in other words, sever information prior to release. The first three items you see there, sections 12, 21 and 22 are **mandatory** exceptions. That means that the ministry must never release records that meet the rules of the sections related to cabinet confidences, third party business information or personal information that would represent an unreasonable invasion of a person's privacy.

Comment [MS18]: Local public body confidence is not mandatorily excepted

The list of discretionary items you see there represent the other reasons a ministry may remove information prior to release. Sections 13 to 20 are discretionary – which means that you don't have to sever them. In fact, the default position **should be** to release that information. The question shouldn't be 'can we sever' but instead we should ask 'should we' or 'do we really need to' sever. Ultimately, this is a recommendation that will come from the experts at IAO and it is a decision that will be made by the DM.

Slide 33



Duty to Assist

What does "Duty to Assist" really mean?

Positive duty in law to ensure that requests are responded to "openly, accurately and completely."

33

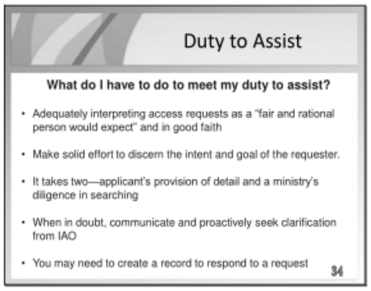
So, coming back to this term I used – duty to assist – all **government employee~~'~~s** must make every reasonable effort to assist applicants and to respond to each applicant openly, accurately and completely in a timely way. After all, access to information is a foundational democratic principle.

The "duty to assist" goes beyond just meeting the letter of the law; it involves providing an excellent service experience to each applicant.

Take a moment and think about what **you** would like as a response if **you** were requesting your information from a publicly funded organization. I'm sure you can imagine that if you were the applicant you would appreciate a thoughtful, respectful and thorough customer service approach. You would want to feel that you **could** get the information that you needed.

You know you have a right to access your information, and government wants to support that right with responsive customer service. Our legislated duty to assist provides us with an obligation to ensure we are embodying this perspective.

Slide 34



Duty to Assist

What do I have to do to meet my duty to assist?

- Adequately interpreting access requests as a "fair and rational person would expect" and in good faith
- Make solid effort to discern the intent and goal of the requester.
- It takes two—applicant's provision of detail and a ministry's diligence in searching
- When in doubt, communicate and proactively seek clarification from IAO
- You may need to create a record to respond to a request

34

To meet your duty to assist an FOI applicant, you need to adequately and liberally interpret access requests. This means steering clear of narrow interpretations, it's about getting to the underlying intent of a request and understanding the request from the applicant's point of view. You need to interpret requests in a manner that a "fair and rational person would expect". You can be proactive and seek clarification from your DMO FOI Liaison if you are unsure about a request. What I mean by this is that if someone asks for a report authored by John Smith in 1998 and there isn't one - but there is one for 1999 – Through your DMO FOI Liaison, you can request that IAO contact the applicant to ask if they actually wanted the 1999 report – or, to speed up the whole process, you could just provide the 1999 report.

I want to tie this concept of duty to assist back to something I mentioned earlier. You'll remember that I noted that an applicant has to provide sufficient detail for an employee to be able to actually understand a request – And that's true, but I think our duty to assist the applicant means that the burden doesn't rest **solely** with the applicant. If we don't understand something, let's have a conversation. Let's try to find out what the applicant is **actually** looking for. For you, that means you are going to relay your concerns or questions to your DMO FOI Liaison. They can work with IAO who can communicate that conversation directly to the FOI applicant.

We also have an obligation under FOIPPA to create a record in response to a request, where feasible. There are some conditions – for instance, creating the record shouldn't interfere with the operations of the ministry, but the test for that is pretty high in government. To show you what I mean – you can imagine that someone has asked for a record that doesn't exist exactly as they have requested it – but to create it all you would need to do is filter a few columns out of a spreadsheet. This is definitely an instance where you would create the record for the applicant. Alternatively, you can imagine that if someone requests access to millions of lines of metadata – this might not be something that your ministry could easily create or provide to an applicant.

The last thing I want to point out is that we need to use our common sense when a single ministry receives a request within government. If the applicant has directed it to the wrong ministry, let's tell them that. FOIPPA provides a mechanism for a ministry to transfer a request to another. So if someone has asked your office for records and you don't have them – but you know, or think another ministry does – let your DMO FOI Liaison know, they can contact IAO who is able to reach out to the other ministry and see if they do have records and in turn can support the applicant by getting the request to the right place.

Slide 35 Copyright

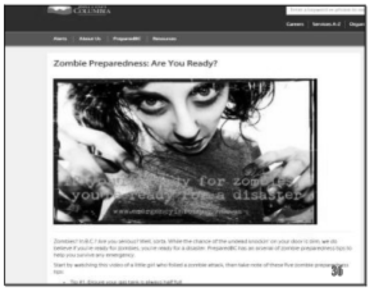
This is a real life example of an FOI request that demonstrates how we can exercise our duty to assist an FOI applicant.

An FOI applicant wrote:
"Dear Leicester City Council,
Can you please let us know what provisions you have in place in the event of a zombie invasion? Having watched several films it is clear that preparation for such an event is poor and one that councils throughout the kingdom must prepare for.
Please provide any information you may have,
Yours faithfully.
Concerned citizen"

The Leicester FOI co-ordinator said "To you it might seem frivolous and a waste of time…but to different people it actually means something. Everybody has their own interests and their own reasons for asking these questions.”

This example illustrates how we can demonstrate our duty to assist and support citizens who are requesting information respectfully and in good faith. Regardless of how we may feel about this request. We do have a duty to assist. This request may seem laughable and like the individual is not taking things seriously, but let’s consider for a moment, that we receive this request in BC.

Slide 36


COLUMBIA
Careers | Services A-Z | Organ
Alerts | About Us | PreparedBC | Resources
If you're ready for zombies, you're ready for a disaster
36

Zombie Preparedness: Are You Ready?

Zombies? In B.C.? Are you serious? Well, sorta. While the chance of the undead knockin' on your door is slim, we do believe if you're ready for zombies, you're ready for a disaster. PreparedBC has an arsenal of zombie preparedness tips to help you survive any emergency.

Start by watching this video of a little girl who foiled a zombie attack, then take note of these five zombie preparedness tips:

- Tip #1: Ensure your gas tank is always half full

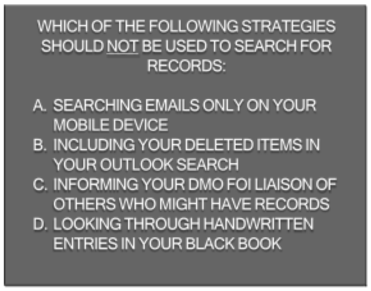
If we were to ignore it, or not treat it seriously, we would be at risk of being offside our duties.

In BC, if someone were to make that same request they would receive real, zombie-related records. In fact, in 2012 there was a real request directed to Government Communications and Public Engagement for records related to Emergency Management BC’s Emergency Preparedness campaign centred on zombies! As they say: If you’re ready for zombies, you’re ready for a disaster.

It is important to respectfully treat each request in good faith – we need to be thoughtful, respectful and helpful when we respond to FOI requests.

Source:
https://www.emergencyinfobc.gov.bc.ca/zombie-preparedness-week-are-you-ready/

Slide 37



WHICH OF THE FOLLOWING STRATEGIES SHOULD NOT BE USED TO SEARCH FOR RECORDS:

A. SEARCHING EMAILS ONLY ON YOUR MOBILE DEVICE
B. INCLUDING YOUR DELETED ITEMS IN YOUR OUTLOOK SEARCH
C. INFORMING YOUR DMO FOI LIAISON OF OTHERS WHO MIGHT HAVE RECORDS
D. LOOKING THROUGH HANDWRITTEN ENTRIES IN YOUR BLACK BOOK

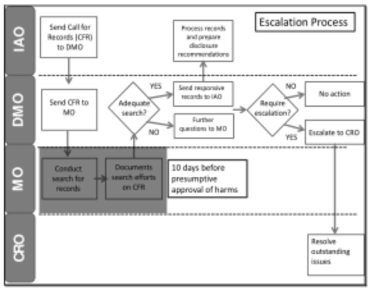
Read before quiz: One of the ways that we can **really demonstrate** that we are working to support applicants and meet our duty to assist is when it comes to searching for "responsive records". "Responsive records" – when we're talking about FOI - just means the records that respond to an FOI request.

Which of the following strategies should not be used to search for records?

- Searching emails on your mobile device
- Include your deleted items in your Outlook search
- Inform your FOI coordinator of other people you think might have records
- Look through handwritten entries in your "black book" for responsive records

The answer here is A – it is not a complete search if it was only conducted on your mobile device. You also need to search on your desktop and any personal device you may have conducted government business on. It is simply ineffective at doing a complete search. This means that the other options are TRUE. You do have to search your deleted items in your Outlook folder.
You are obliged to provide handwritten notes in response to an FOI request. **and**
You should inform your DMO FOI Liaison of others who may have records – whether that means colleagues in your office, division or ministry – or if you know another ministry would have records.

Slide 38



Escalation Process

IAO
DMO
MO
CRO

Send Call for Records (CFR) to DMO

Send CFR to MO

Conduct search for records

Documents search efforts on CFR

10 days before presumptive approval of harms

Adequate search?

YES

NO

Send responsive records to IAO

Further questions to MO

Process records and prepare disclosure recommendations

Require escalation?

NO

YES

No action

Escalate to CRO

Resolve outstanding issues

As I just mentioned, an adequate search for records is one of the most important things you can do to support government in meeting our Access obligations.

You are responsible for searching anywhere you or your office has stored recorded information, that includes your email, your network drive, your electronic systems and devices and physical storage such as your desk, cabinet or notebook. You are the expert, you should **know** where the records are kept. And if you don't know you should ask someone who would. You also should be able to take a common sense approach here – if you don't have records, but you know your colleague does – document that detail so that your DMO FOI Liaison is able to ensure your colleague receives the request for records.

It is your responsibility to communicate your search efforts **clearly** to your DMO FOI Liaison. Your DMO FOI Liaison is responsible for overseeing the search process and must be able to clearly **document** who has received and who has responded to the request and all the search details on the Call for Records form that is sent back to IAO. The details on searching – including, the search terms that were used and the search methodology - need to move clearly through the chain of command to ensure that we aren't playing a game of broken telephone.

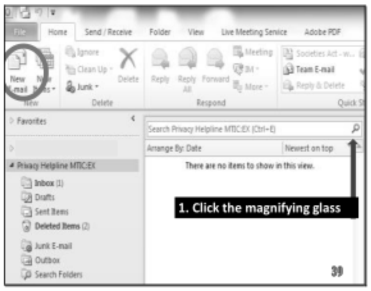
The swimlane you see on the screen represents the various roles and some of the responsibilities of the players involved in responding to one of your FOI requests. As we know, IAO receives the request from the applicant. The DMO FOI Liaison is a new role that will liaise between your office and IAO. They are your point of contact for supporting you in ensuring you have a clear understanding of the request and of what is required of you in responding to the request. They also are available to support IAO in ensuring they have the information they need from your office. This includes getting your records of course, but also includes documenting the details of your searches and information that explains why there are no records if you submit a no records response.

It is an expectation across government that IAO be able to provide evidence that a thorough and comprehensive search has been conducted – if you don't relay the details of your efforts this becomes very challenging for IAO. It is also important that if you are submitting a response that indicates there are no records, you need to clearly communicate why there are no records, other sources for the records and other available records that are similar to what the applicant has requested. There is a big difference between "the Minister's Office has no records on this issue" and "the Minister's Office has no records on this issue, **because** it arose when the Minister was in Ottawa, so issues were addressed by the Deputy".

In the event your office responds to an FOI Request with a no records response, you should know that your DMO FOI Liaison is responsible for engaging in a formal escalation of that file. The DMO FOI Liaison will review the request and the no records response. There are times when a no records response may be appropriate, like in the example I just gave – or if the Minister for Children and Family Development receives a request for records related to the numbers of hunted Bear in BC - it is likely that they would reply by explaining that they have a 'no records response' . The DMO FOI Liaison would reach back to you in the Minister's Office for more information. In this case it is likely that you could avoid escalation by providing a more fulsome response explaining that the applicant should be redirected to the Natural Resource Sector. However, in a more complicated file, if the Minister's Office did not include an explanation as to why there are no records, or a recommendation for where records may be located, the DMO FOI Liaison will initiate an escalation process. This process would raise the profile of the file from the DMO FOI Liaison to your ministry's Deputy Minister. Your DM may bring that file to the Corporate Records Officer, Associate Deputy Minister Cheryl Wenezenki-Yolland, who may in turn escalate the process directly to the Minister of Finance.

Comment [MS19]: Needs to be removed. CWY designation to be rescinded ASAP and new CRO will be designated by Minister in near term .

Slide 39



1. Click the magnifying glass

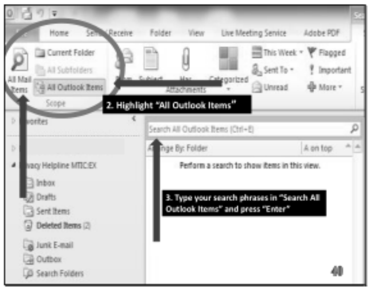
To help you get a leg up on an email search, I'm going to walk you through what a proper search in your Outlook folder should look like. To be clear, your email is only one place you need to search for records. But, I think this is a useful tip that not everyone necessarily knows about. It also demonstrates the attention that needs to be paid when you are conducting your search in other areas – like your LAN, your technical systems and your physical records.

I know we have talked about this, but I want to reiterate that searching your Outlook cannot be done only from your mobile device and must also be done from your computer. An Outlook search must include **all of your folders**, not just your inbox. And, you do need to search the deleted items folder that is contained within your Outlook account.

Okay, so getting technical for a moment - I'll draw your attention to the "New E-mail" button – just take note of it because it will change in a moment.

The first thing you need to do for a thorough search is to click the magnifying glass, which you can see in the top right of the screen here.

Slide 40



2. Highlight "All Outlook Items"

3. Type your search phrases in "Search All Outlook Items" and press "Enter"

When you click the magnifying glass, you can see (in the top left corner), the "New E-mail" button changes to "All Mail Items".

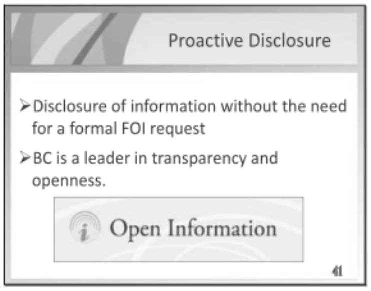
Next, you need to ensure you have "All Outlook Items" - again in the top left, is selected. This is not the default selection, so you have to manually select it. Now you can type your search phrases in to the "Search All Outlook Items" field and press "Enter".

This type of search will produce all the Outlook items responsive to the request – not just the items in your inbox!

Remember, you should be using a set of fulsome search terms. Don't just search what the applicant has asked. You need to use your expertise and insider knowledge of your own records to find everything that may respond to a given FOI request. If you are searching for records relating to an event that took place in

New Zealand, maybe include “Kiwi” “paradise” or “NZ” as search terms, and not just “New Zealand”, because that won’t necessarily bring up all the responsive records. Make sure you document the search terms you used and communicate that to your DMO FOI Liaison.

Slide 41



Proactive Disclosure

- Disclosure of information without the need for a formal FOI request
- BC is a leader in transparency and openness.

Open Information

41

We’ve talked a little about some very granular practices with respect to FOI, but it is important not to lose sight of the government-wide context.

~~One of the more tangible ways that I think government has done a really good job of demonstrating our commitment to access, transparency and accountability is through proactive disclosure.~~

- Proactive disclosure is the disclosure of information without the need for a formal FOI request. You may have also heard this referred to as “routine release”.

- There are lots of examples of proactively disclosed information. For one, BC’s Open Information site, which contains thousands of proactively disclosed records. There is also the BC Data catalogue which contains thousands of high-quality datasets.

- Corporately, we currently proactively release summaries of community gaming grants, Minster’s receipted travel expense information, summaries of FOI requests, calendars, ~~and~~ summaries of ~~directly-awarded~~ contracts over $10,000 and direct awards, and more.

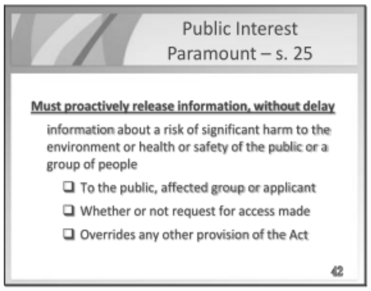
- ~~Several of these disclosures are made on the Open Information site, which contains thousands of proactively disclosed~~

~~records. Others are made through the BC Data catalogue which contains thousands more high-quality datasets.~~

- FOIPPA requires all ministers to establish additional categories of recorded information that can be proactively disclosed.

Other disclosures are more casual – ~~your staff~~you might give the general public non-personal and non-sensitive information over the phone, or via a website. Not all disclosures are repeatable -- and that's okay. Sometimes a disclosure is a one-off. Any information a ministry makes available on its website, or when citizens call a hotline or come to a service counter is a proactive disclosure. Each time we do this, we contribute to citizens receiving the information they're interested in, more efficiently.

Slide 42



Public Interest Paramount – s. 25

Must proactively release information, without delay

information about a risk of significant harm to the environment or health or safety of the public or a group of people

❑ To the public, affected group or applicant

❑ Whether or not request for access made

❑ Overrides any other provision of the Act

42

- While we are on the topic of proactively releasing information, it is important to address s.25 of FOIPPA. Section 25 is a public interest override which dictates that despite anything else, and regardless of whether its been requested, the head of a ministry must disclose information about a risk of significant harm to the environment; or to the health or safety of the public or a group of people; and any other information which is clearly in the public interest. This release must happen without delay.

- Examples include, records that would indicate:
  - The accidental release of a pesticide into a stream, which will affect fish and other aquatic life.
  - The presence of a norovirus in the public drinking water.
  - A natural gas leak which could cause an explosion in a populated area.

- Past interpretations by the OIPC and government of this section included a requirement for urgency. This meant that government was disclosing information via section 25 only when the information related to an imminent matter. “This bridge is about to collapse” vs. “This bridge may collapse in the next 5 years”.

- Following the Commissioner’s 2015 investigation into the lack of information released regarding the Mount Polley mine tailings pond, the Commissioner released a report which stated that section 25 should not be interpreted to require an element of urgency in order to require the disclosure if it is clearly in the public interest.

- The standard now is: where a disinterested and reasonable observer, **knowing what the information is** and **knowing all of the circumstances**, would conclude that disclosure is obviously in the public interest.

- Following a recent 2016 OIPC Investigation into the lack of records released regarding nitrate levels in the Hullcar aquifer in Spallumcheen, it is clear from the Commissioner that the requirement is not just that the public be notified of an issue in the public interest, but also that the records that relate to the issue be publically released.

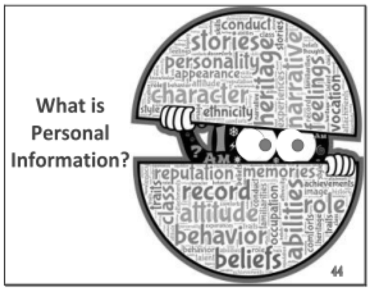
- This is important for you to know as you may be asked to approve of this kind of release and need to know the robust legal impetus for you to release those records.

Slide 43

We have spent the last little bit focusing on openness and transparency as a means of demonstrating accountability, but protecting personal information or personal privacy is another way we need to demonstrate accountability. Accountability to citizens and their information.

Part 3 of FOIPPA is the part of the Act that addresses the privacy and the protection of personal information. It does this by restricting the purposes for which you can collect, use or disclose personal information.

Slide 44


What is Personal Information?

Personal information is an important term to have a clear understanding of, as privacy is all about the protection of personal information.

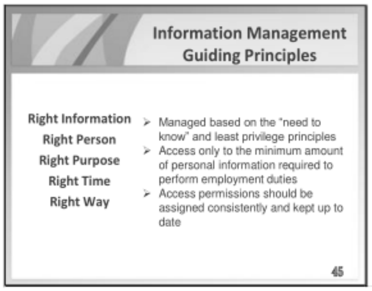
Personal information is defined as recorded information about an identifiable individual other than "contact information" A citizen's contact information is considered their business contact, when that information is used to connect with them in their business capacity. Essentially, their business card, as long as they are handing it out for business reasons.

But everything else about the citizen as an identifiable individual is their personal information. This would include their name, their home address, their voting habits and their DNA – perhaps the obvious examples. But it would also include information about their educational history, employment history, health history **and even their personal opinions**. In the context of your work, you're most likely to come across personal information of a constituent or person seeking government services and, the employee information of the people in your office.

There are two caveats here, first, if you have a bunch of disparate, non-personal elements of information that individually don't identify you, but taken as a whole could work to identify you, then those would become personal information. This is what we call the mosaic effect. **For example,** information about what kind of car an individual drives, their age or their hometown may not identify anyone if they are 30 and drive a Civic in Vancouver. However, if they are 80, and drive a Rolls Royce in Spuzzum, BC, then it is more likely to be able to identify them – so, context is important.

Second, it is important to consider context, because in a different context, information can be either personal or business contact. For instance, if I run a professional day care out of my home, then my address could be both personal and business related. If I use my address to order a shipment of diapers for the daycare, then it is business contact, but if I use my address to register for a home owner grant, then it is personal.

Slide 45



Information Management Guiding Principles

Right Information
Right Person
Right Purpose
Right Time
Right Way

- Managed based on the "need to know" and least privilege principles
- Access only to the minimum amount of personal information required to perform employment duties
- Access permissions should be assigned consistently and kept up to date

45

We don't have time to do a walk through of every provision of FOIPPA – that would take a week. But we can discuss, and more importantly, you can remember, this very simply mantra – Right Information; Right Person; Right Purpose; Right Time; and Right Way. These are the things you need to consider when you are collecting, using, and disclosing personal information. Am I sharing it with the right people, and only the right people? Should I be sharing this information over Facebook, or is it more appropriate that I share it over email?

Some of the practices that we can pull out of this mantra would include managing information on a need to know – not a nice to know basis. Accessing, using, or disclosing the minimum amount of personal information necessary, and managing and auditing access permissions.

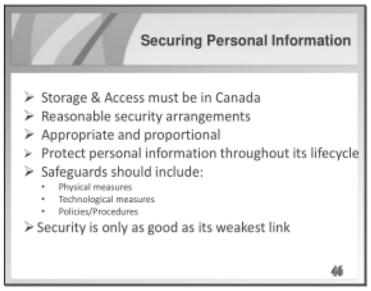
An example that I like to use to demonstrate these guiding principles is that of a border agent that I read about. Generally speaking, he was a good worker and accepted passports and other information in order to process people through customs. He did this securely, while at his booth at the border in order maintain border security. All good according to these principles. However, one fateful day, a very attractive citizen came through his booth, and he did the same thing he always did….with one notable exception. He took the information he

Comment [MS20]: As we also commented in June: As with the staff training, this slide needs to be clarified to make clear that these are the principles for managing sensitive information only and not all information. We would appreciate this change being made in this round of revisions.

had from that interaction and used it after hours in order to message the citizen on Facebook. Dating was not the right purpose. Facebook was not the right way. After hours was not the right time. He basically failed on each of these guiding principles. He was not the right person, for the citizen or for that job apparently. Now, not every example of wrong is going to be wrong for each principle, so consider each principle here when you are collecting, using or disclosing personal information.

If you need support in determining in applying these guiding principles – your ministry has an MPO – Ministry Privacy Officer – who can support you.

Slide 46



Securing Personal Information

- Storage & Access must be in Canada
- Reasonable security arrangements
- Appropriate and proportional
- Protect personal information throughout its lifecycle
- Safeguards should include:
  - Physical measures
  - Technological measures
  - Policies/Procedures
- Security is only as good as its weakest link

46

FOIPPA's security provisions are fairly straightforward. There are two things you need to know:

- Storage and access to **personal information** must be within Canada. There are exceptions to this rule, but you will want to take as a default that personal data needs to stay within Canada. This has implications with some cloud services like DropBox, Slackmail or social media platforms. There are cases where it is okay to use these services, but you should get your privacy sense tingling, and you should dial in the Privacy Helpline to make sure you are on side. Further, these services may complicate the FOI process and so you should remember that these records are still FOIable.

- Next, you have to ensure reasonable security arrangements. What does reasonable mean? It means that the security around personal information must be appropriate and proportional to its sensitivity. So, if the personal information in question is someone's lunch order, it would probably be sufficient to simply put it in your pocket and not share it. However, if the information is someone's health information, including a drug screen and a list of all of their current medical conditions, then that is information that

Formatted: Font: Bold

needs to be encrypted, password protected, locked up with controlled access and ensuring access is logged and audited.

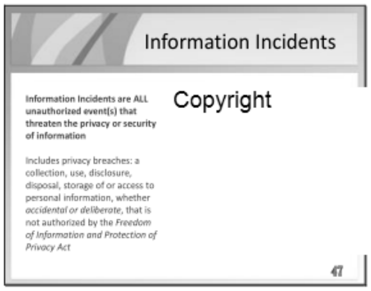
When you are thinking about security, you want to think about it in 3 different ways – what physical security measures have you taken, what technical measures have you taken and what policy or procedural measures have you taken?

In terms of physical security, think of locking cabinet doors, having a security guard, locked offices, and privacy screens.
With respect to technical security, think about encryption, passwords, audit logs and access controls.
For policy or procedural security, this is where you try to fill in the gaps between technical and physical security. Perhaps a policy that requires you to not leave your keys in your locked cabinet, and to not tape your password to your desk.

~~Policy can be big and formal, or simply an intra-office thing to ensure that everyone keeps to their good practices. For example, if you receive and save a lot of correspondence, are you using personal information in the document titles or document names when saving them? This is something you should avoid, and can do so by setting a document naming policy.~~ Many overarching policies around securing and managing government information are set at the corporate level through the Core Policy and Procedures Manual, the Appropriate Use policy, and other related policies. You should contact the IM IT Policy email inbox if you need help in applying these policies. There may be additional need to develop intra-office policies specific to your work, and these should align with and enhance the "motherhood" corporate policies requirements.

For example, the corporate policies make general statements but don't tend to go into specifics about procedure. So, if your office receives and saves a lot of correspondence, are you using personal information in the document titles or document names when saving them? This is something you should avoid, and can do so by setting a document naming policy.

Slide 47



Information Incidents

Information Incidents are ALL unauthorized event(s) that threaten the privacy or security of information

Includes privacy breaches: a collection, use, disclosure, disposal, storage of or access to personal information, whether *accidental or deliberate*, that is not authorized by the *Freedom of Information and Protection of Privacy Act*

Copyright

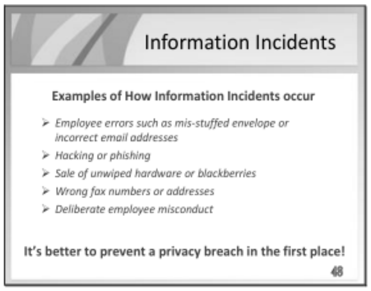
47

Information Incidents are ALL unauthorized event(s) that threaten the privacy or security of information

Information incidents include privacy breaches: a collection, use, disclosure, disposal, storage of or access to personal information, whether *accidental or deliberate*, that is not authorized by the *Freedom of Information and Protection of Privacy Act*

You can consider an event as a privacy breach, anytime someone sees some personal information they shouldn't have. This can be minor, such as receiving an email by mistake, or this can be more significant, like someone snooping around a system to find out information on their daughter's sketchy new boyfriend. You can't quite predict what the impact of a breach is going to be, regardless of whether it is small or large, accidental or deliberate. So we have to treat them all as incidents to start.

Slide 48



Information Incidents

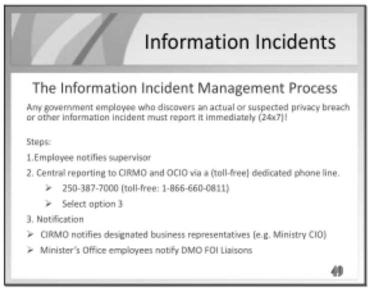
Examples of How Information Incidents occur

- *Employee errors such as mis-stuffed envelope or incorrect email addresses*
- *Hacking or phishing*
- *Sale of unwiped hardware or blackberries*
- *Wrong fax numbers or addresses*
- *Deliberate employee misconduct*

It's better to prevent a privacy breach in the first place!

48

Slide 49



Information Incidents

The Information Incident Management Process

Any government employee who discovers an actual or suspected privacy breach or other information incident must report it immediately (24x7)!

Steps:

1.Employee notifies supervisor

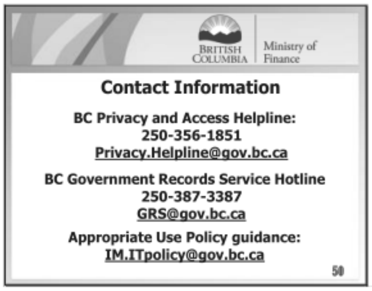
2. Central reporting to CIRMO and OCIO via a (toll-free) dedicated phone line.
   - 250-387-7000 (toll-free: 1-866-660-0811)
   - Select option 3

3. Notification

- CIRMO notifies designated business representatives (e.g. Ministry CIO)
- Minister's Office employees notify DMO FOI Liaisons

49

Slide 50



BRITISH COLUMBIA | Ministry of Finance

Contact Information

BC Privacy and Access Helpline:
250-356-1851
Privacy.Helpline@gov.bc.ca

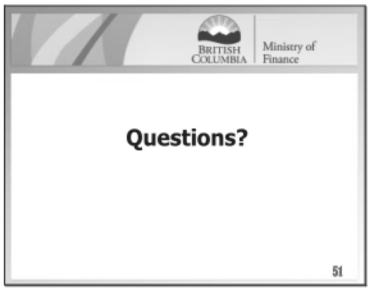
BC Government Records Service Hotline
250-387-3387
GRS@gov.bc.ca

Appropriate Use Policy guidance:
IM.ITpolicy@gov.bc.ca

50

Comment [MS21]: Same comment as above.

Slide 51



BRITISH COLUMBIA | Ministry of Finance

Questions?

51

Slide 52

BRITISH COLUMBIA | Ministry of Finance

BRITISH COLUMBIA

Information Management: Privacy, Access and Records Management

1. Introduction

1.1 Welcome

Where ideas work

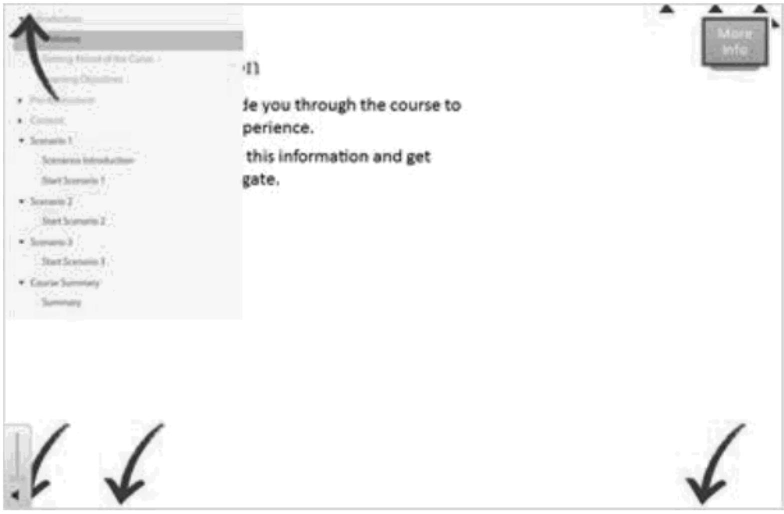
Information Management

Privacy, Access and Records Management

Notes:

Welcome to the *Information Management* eLearning course. This course will familiarize you with the discipline of information management, made up of three related domains: privacy, access to information including proactive disclosure, and records management. This course will introduce practices and controls that will empower employees to act as good stewards of the information they create and receive.

1.2 Course Navigation



de you through the course to
perience.

this information and get
gate.

Notes:

Here are a few tips to guide you through the course to make the most of your experience. Take a moment to review this information and get familiar with how to navigate.

You can navigate from start to finish by using the previous and next buttons at the bottom of the screen. A submit button is located here on question screens.

You can use the progress bar to pause, play, scrub, and replay the audio and screen actions.

Click the audio button to control the sound. Slide the control all the way down to mute the audio.

You can also jump to a specific screen, or go back, by clicking the Menu button in the top left and then selecting the screen you wish from the drop-down menu.

Click the Menu button at the top of the screen to see how far you have progressed in the course. The highlighted section shows where you are in relation to the remaining course content.

You can complete this course over several sessions by exiting and returning to a specific screen by using the menu.

Refer to the glossary in the menu bar for terms or acronyms that you may not be familiar with.

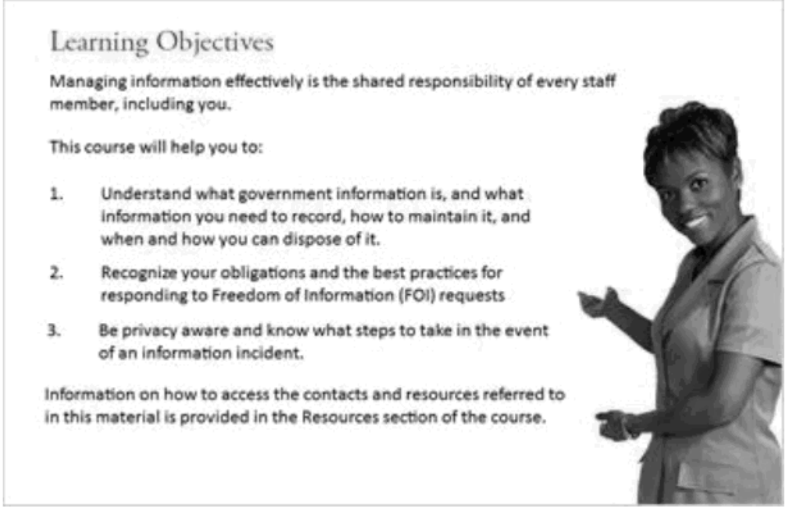
Resources are also available at any time from the menu bar.

A transcript of the entire course is available at the end of the e-course for your future reference.

Whenever you see the More Info button, roll your mouse over it for more information. You can click each link to open the resource in a new browser (this course will stay open). Click the X button on a pop-up to close it.

Click Course Navigation at the top left of the screen for navigation tips at any time throughout the course.

1.3 Learning Objectives



Learning Objectives

Managing information effectively is the shared responsibility of every staff member, including you.

This course will help you to:

1. Understand what government information is, and what information you need to record, how to maintain it, and when and how you can dispose of it.
2. Recognize your obligations and the best practices for responding to Freedom of Information (FOI) requests
3. Be privacy aware and know what steps to take in the event of an information incident.

Information on how to access the contacts and resources referred to in this material is provided in the Resources section of the course.

Notes:

Managing information effectively is the shared responsibility of every staff member, including you.

This course will help you to:

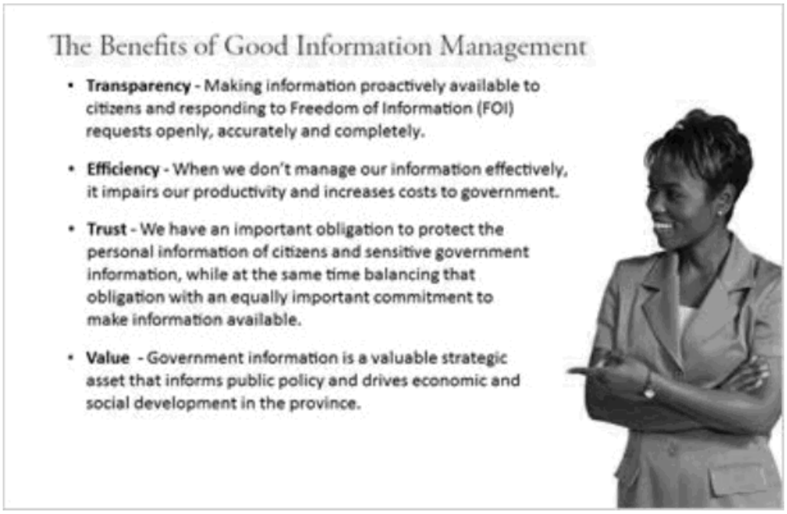
- Understand what government information is, and what information you

need to record, how to maintain it, and when and how you can dispose of it.
- Recognize your obligations and the best practices for responding to FOI requests
- Be privacy aware and know what steps to take in the event of an information incident.

Information on how to access the contacts and resources referred to in this material is provided in the Resources section of the course.

2. What is Information Management?

2.1 The Benefits of Good Information Management



The Benefits of Good Information Management

- **Transparency** - Making information proactively available to citizens and responding to Freedom of Information (FOI) requests openly, accurately and completely.
- **Efficiency** - When we don't manage our information effectively, it impairs our productivity and increases costs to government.
- **Trust** - We have an important obligation to protect the personal information of citizens and sensitive government information, while at the same time balancing that obligation with an equally important commitment to make information available.
- **Value** - Government information is a valuable strategic asset that informs public policy and drives economic and social development in the province.

Notes:

Everyone has a part to play in good information management.

As public servants, the information we create and receive belongs to the citizens of this province, and the records we create support public transparency.

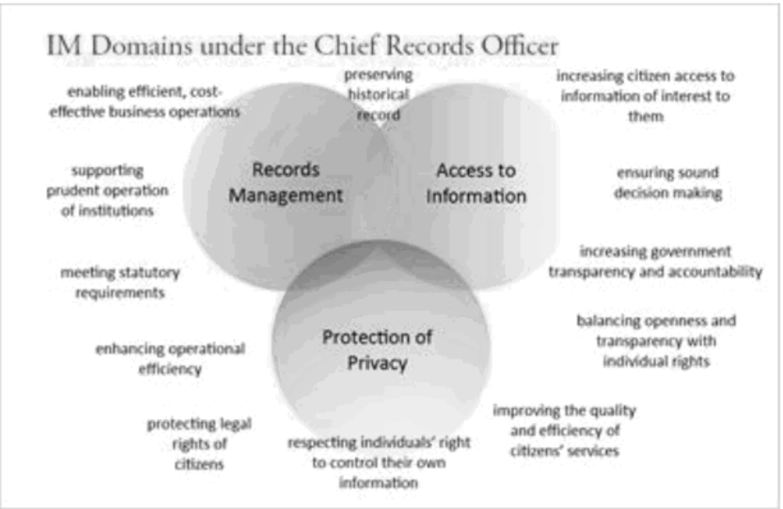
As importantly, without reliable information management practices, we can't do our jobs effectively.

Information management is also about carefully protecting personal information and other sensitive information. The public entrusts us with their most personal data, and relies on us to keep that data safe.

It has been said that we should manage our information assets more like we manage our financial assets. We need to give the same care and attention to how we handle government information as we would if it was money.

We have a rich store of information which - if properly managed and analyzed - has the power to transform service delivery, increase citizen engagement, reduce inefficiencies, unlock solutions to a range of challenges, and generate economic development in the province.

2.2 IM Domains under the Chief Records Officer


IM Domains under the Chief Records Officer
preserving historical record
enabling efficient, cost-effective business operations
increasing citizen access to information of interest to them
Records Management
Access to Information
supporting prudent operation of institutions
ensuring sound decision making
increasing government transparency and accountability
meeting statutory requirements
balancing openness and transparency with individual rights
Protection of Privacy
enhancing operational efficiency
improving the quality and efficiency of citizens' services
protecting legal rights of citizens
respecting individuals' right to control their own information

Notes:

Information Management is an emerging and dynamic field.

All BC Government employees have responsibilities for information management as a part of their everyday work.

There are three domains within the Information Management sphere: Records Management, Access to Information (including FOI), and Protection of Privacy.

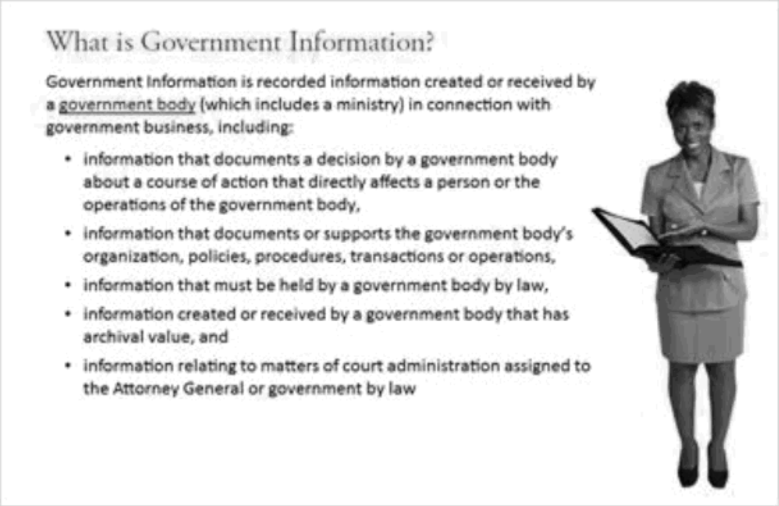
Following good practice in these three areas supports an increase in accountability, operational efficiency and the quality of citizen services.

To manage information effectively, we need to ensure integration of our practices across and between all three of these areas. Implementing effective records management practices supports a comprehensive access to information program, and supports the protection of personal and sensitive information. Ultimately the release of information must be done in a privacy protective manner, too.

Some of the outcomes of a highly functioning information management system are public accountability and improved service - which are fundamentally important in your work as a public servant. Furthermore, effective information management contributes significantly to efficient public administration, which reduces government costs borne by taxpayers.

3. Records Management

3.1 What is Government Information?



What is Government Information?

Government Information is recorded information created or received by a government body (which includes a ministry) in connection with government business, including:

- information that documents a decision by a government body about a course of action that directly affects a person or the operations of the government body,
- information that documents or supports the government body's organization, policies, procedures, transactions or operations,
- information that must be held by a government body by law,
- information created or received by a government body that has archival value, and
- information relating to matters of court administration assigned to the Attorney General or government by law

Notes:

Government Information is recorded information created or received by a government body in connection with government business.

Briefing notes are government information. Usually, Outlook calendar entries, entries in your notebook or in OneNote, emails, instant messages, and texts are government information, too.

Because policy permits the personal use of government IT resources, some of these kinds of records may not be government information at all. A good example of this would be when you send an email to your child's school from your government email address.

You don't have to manage your non-work-related information according to records management policy. But you should be aware that information you may have stored on a government system for a non-work related reason may be included within regular government business activities including audits, investigations, or Freedom of Information requests. For example, an

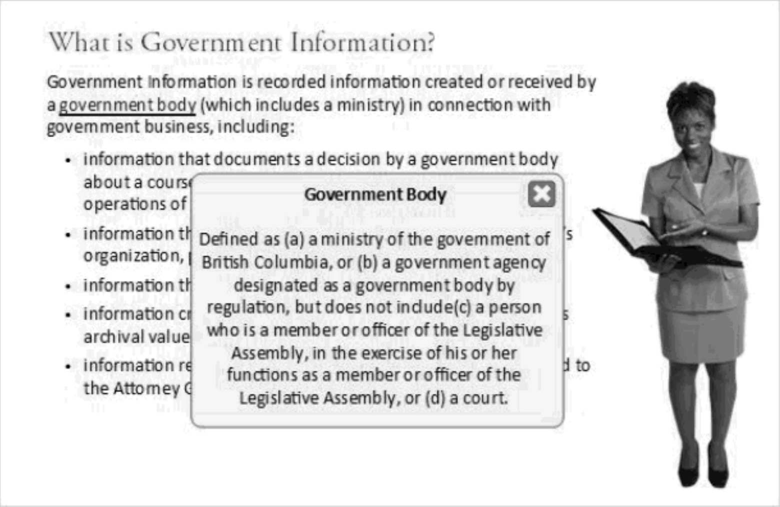
FOI request for all of an employee's emails would capture both non-work related and government records.

While non-work related records are very unlikely to be released to a third party, the information would be processed by those responsible for the FOI process. This happens rarely - for example, when you've written a non-work related note on the same page in your notebook as your meeting notes. Later, we'll cover email best practices that will help you avoid this situation.

Ministries are subject to the Information Management Act, sometimes referred to as the "IMA", the Freedom of Information and Protection of Privacy Act referred to as "FOIPPA", and other acts that require government information to be created, maintained or disclosed.

All employees are required to manage government information throughout its lifecycle according to information schedules and other policies that flow from these Acts. We'll get into this in detail later.

Government Body (Slide Layer)



What is Government Information?

Government Information is recorded information created or received by a government body (which includes a ministry) in connection with government business, including:

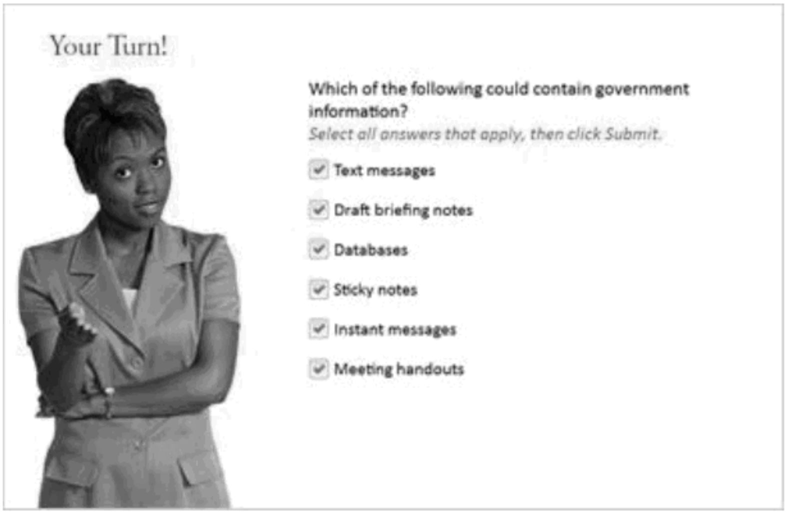
- information that documents a decision by a government body about a cours operations of
- information th 's organization,
- information th
- information cr s archival value
- information re d to the Attorney G

Government Body

Defined as (a) a ministry of the government of British Columbia, or (b) a government agency designated as a government body by regulation, but does not include(c) a person who is a member or officer of the Legislative Assembly, in the exercise of his or her functions as a member or officer of the Legislative Assembly, or (d) a court.

3.2 Your Turn!

(Multiple Response, 10 points, 2 attempts permitted)



Your Turn!

Which of the following could contain government information?

Select all answers that apply, then click Submit.

☑ Text messages

☑ Draft briefing notes

☑ Databases

☑ Sticky notes

☑ Instant messages

☑ Meeting handouts

Correct	Choice
X	Text messages
X	Draft briefing notes
X	Databases
X	Sticky notes
X	Instant messages
X	Meeting handouts

Feedback when correct:

That's right! All of these records could contain government information.

It doesn't matter what medium is used to produce a record. What makes it government information is the context and, perhaps most importantly, the content - and that the information in the record relates to government business.

Feedback when incorrect:

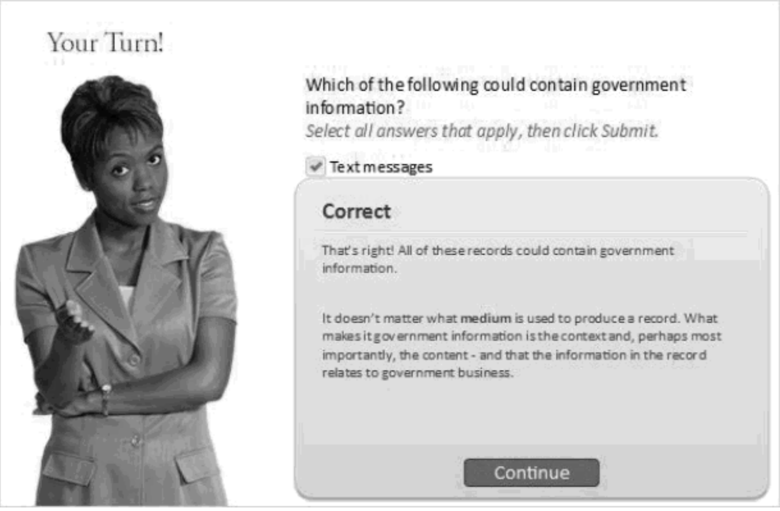
Not quite. All of these records could contain government information.

It doesn't matter what medium is used to produce a record. What makes it government information is the context and, perhaps most importantly, the content - and that the information in the record relates to government business.

Notes:

You're up! Which of the following types of recorded information could contain government information?

Correct (Slide Layer)



Which of the following could contain government information?

Select all answers that apply, then click Submit.

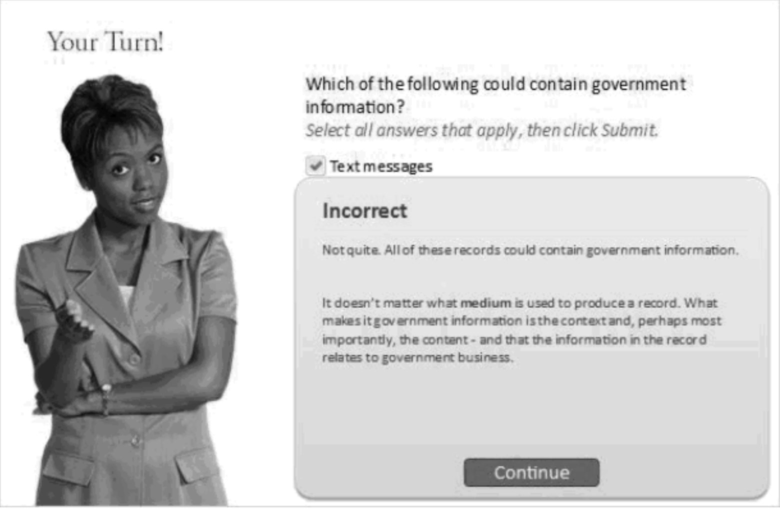
☑ Text messages

Correct

That's right! All of these records could contain government information.

It doesn't matter what **medium** is used to produce a record. What makes it government information is the context and, perhaps most importantly, the content - and that the information in the record relates to government business.

Incorrect (Slide Layer)



Your Turn!

Which of the following could contain government information?

Select all answers that apply, then click Submit.

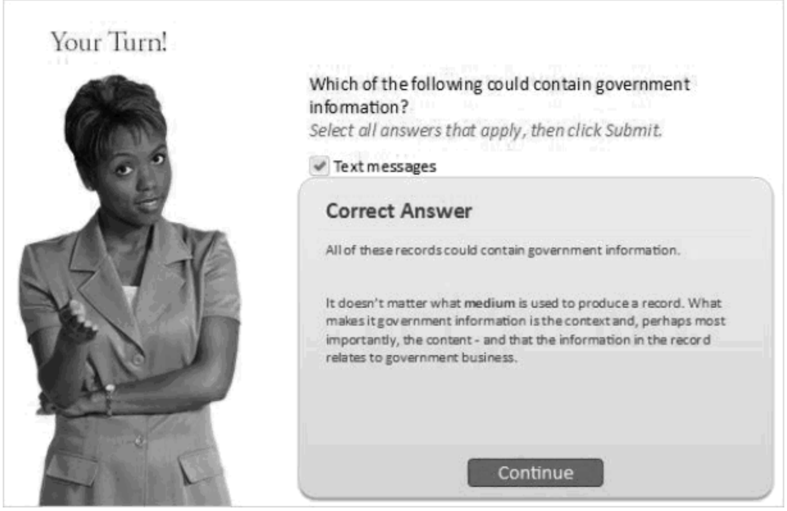
☑ Text messages

Incorrect

Not quite. All of these records could contain government information.

It doesn't matter what **medium** is used to produce a record. What makes it government information is the context and, perhaps most importantly, the content - and that the information in the record relates to government business.

Answer (Slide Layer)



Your Turn!

Which of the following could contain government information?

Select all answers that apply, then click Submit.

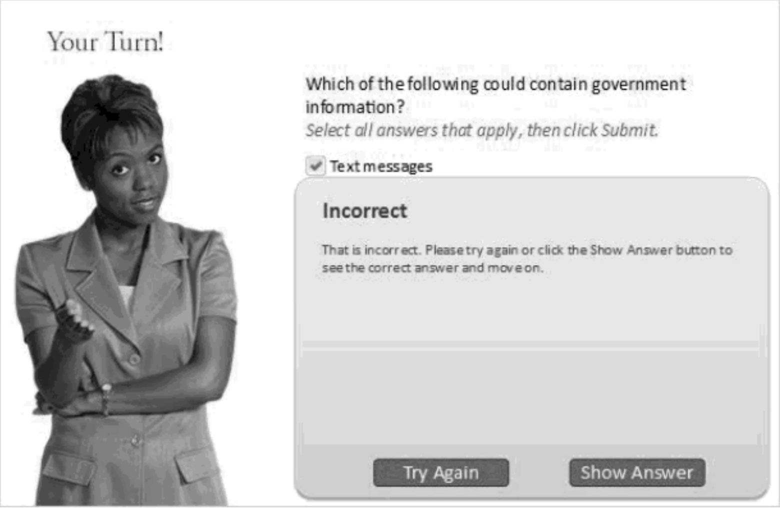
☑ Text messages

Correct Answer

All of these records could contain government information.

It doesn't matter what **medium** is used to produce a record. What makes it government information is the context and, perhaps most importantly, the content - and that the information in the record relates to government business.

Try Again (Slide Layer)



Your Turn!

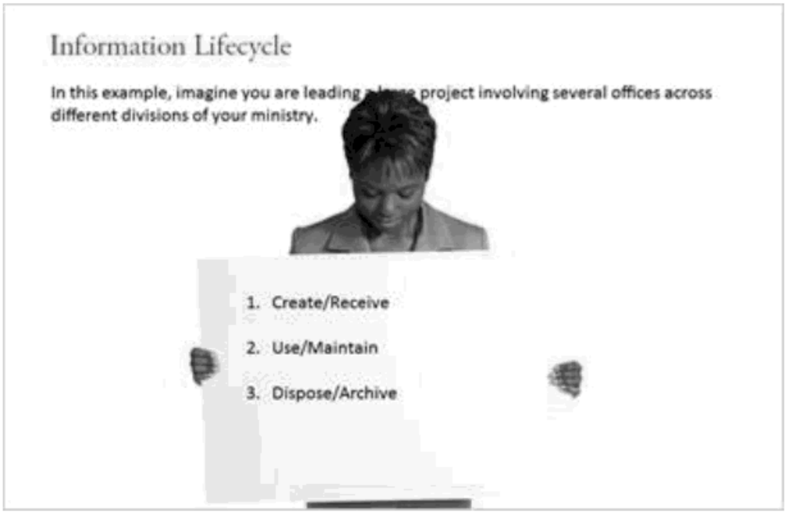
Which of the following could contain government information?
Select all answers that apply, then click Submit.

☑ Text messages

Incorrect

That is incorrect. Please try again or click the Show Answer button to see the correct answer and move on.

3.3 Information Lifecycle



Information Lifecycle

In this example, imagine you are leading a large project involving several offices across different divisions of your ministry.

1. Create/Receive
2. Use/Maintain
3. Dispose/Archive

Notes:

Now it’s time to talk about what to do with government information, from the beginning to the end of its lifecycle. The lifecycle of government information is simple - information is created or received, you use and maintain it, and then the information is either disposed of or sent to the government archives. Some information only lives for a few minutes or hours, and some is never disposed of, but rather is permanently preserved in the government archives.

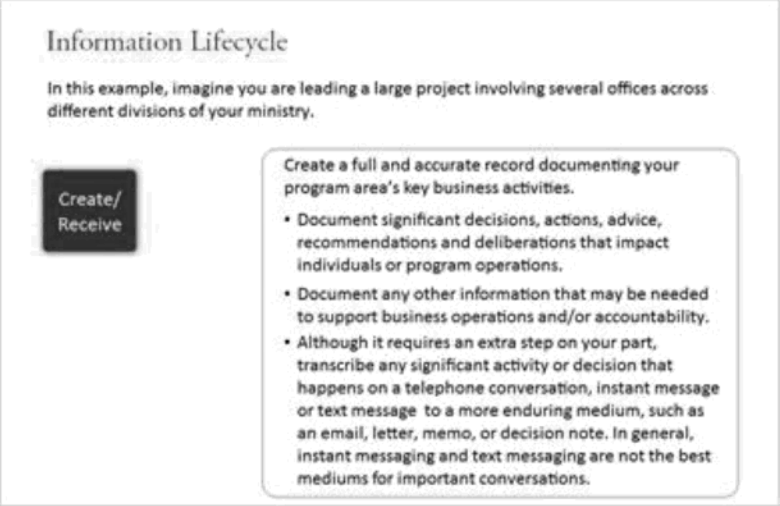
Always ensure that you are creating a full and accurate account of decisions and actions that support business operations.

We will now walk through each stage of the lifecycle of government information in order to learn more about it. We'll use an example to make these stages easier to understand. Think about a project where your office is leading a large project involving several offices across different divisions of your ministry.

Create/Receive
As you work on the project, you naturally create and receive government information, such as a project charter, meeting agendas and minutes, email correspondence, and project plans and reports.

To have a full and accurate record of the project, you need to have documentation of significant project activities, decisions and results.

3.4 Information Lifecycle



Information Lifecycle

In this example, imagine you are leading a large project involving several offices across different divisions of your ministry.

Create a full and accurate record documenting your program area's key business activities.

- Document significant decisions, actions, advice, recommendations and deliberations that impact individuals or program operations.
- Document any other information that may be needed to support business operations and/or accountability.
- Although it requires an extra step on your part, transcribe any significant activity or decision that happens on a telephone conversation, instant message or text message to a more enduring medium, such as an email, letter, memo, or decision note. In general, instant messaging and text messaging are not the best mediums for important conversations.

Notes:

Now it's time to talk about what to do with government information, from the beginning to the end of its lifecycle. The lifecycle of government information is simple - information is created or received, you use and maintain it, and then the information is either disposed of or sent to the government archives. Some information only lives for a few minutes or hours, and some is never disposed of, but rather is permanently preserved in the government archives.

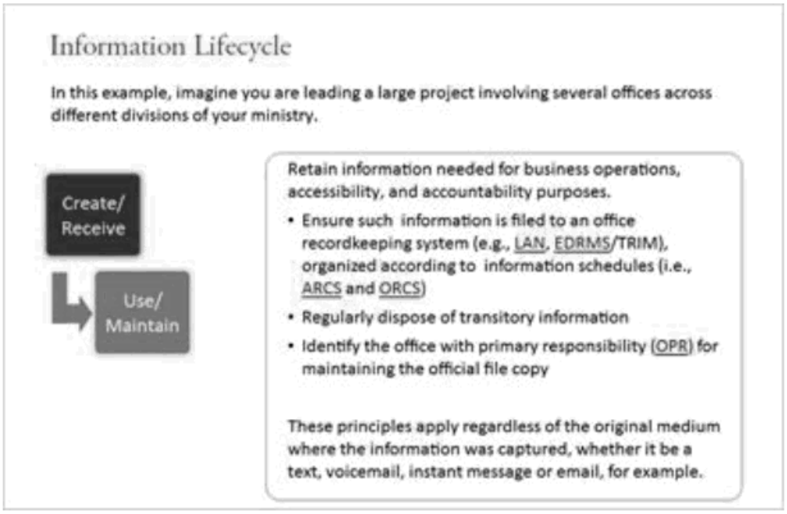
Always ensure that you are creating a full and accurate account of decisions and actions that support business operations.

We will now walk through each stage of the lifecycle of government information in order to learn more about it. We'll use an example to make these stages easier to understand. Think about a project where your office is leading a large project involving several offices across different divisions of your ministry.

Create/Receive
As you work on the project, you naturally create and receive government information, such as a project charter, meeting agendas and minutes, email correspondence, and project plans and reports.

To have a full and accurate record of the project, you need to have documentation of significant project activities, decisions and results.

3.5 Information Lifecycle



Information Lifecycle

In this example, imagine you are leading a large project involving several offices across different divisions of your ministry.

Retain information needed for business operations, accessibility, and accountability purposes.

- Ensure such information is filed to an office recordkeeping system (e.g., LAN, EDRMS/TRIM), organized according to information schedules (i.e., ARCS and ORCS)
- Regularly dispose of transitory information
- Identify the office with primary responsibility (OPR) for maintaining the official file copy

These principles apply regardless of the original medium where the information was captured, whether it be a text, voicemail, instant message or email, for example.

Notes:

Use/Maintain

As you create and receive government information, it is important to ensure that you maintain the information so that it is available to those who need it and is kept for the required length of time. You should always retain information that details significant activities of your unit, as well as changes to existing programs or the establishment of new ones.

Going back to our example, any information that is needed by your office to perform or document project activities must be filed in your office recordkeeping system. You can file these temporarily, in a collaboration system such as SharePoint, but be sure to transfer them to the recordkeeping system when you have wrapped up the project.

A recordkeeping system is a shared system organized according to government information schedules. Two examples of office recordkeeping systems are an appropriately organized office network drive, sometimes called your “LAN”, or the government Enterprise Document and Records Management System (EDRMS), known as TRIM. This office recordkeeping system does not include locations that are only available to you, such as your desktop, home drive or the hard drive of your computer.

Your office may also use other information systems for recordkeeping, such as SharePoint. This is fine, as long as they have appropriate information management controls, including use of information schedules.

These schedules specify how long each category of information must be kept. Within the office recordkeeping system for government we use ARCS, which stands for the Administrative Records Classification System, and ORCS, which stands for Operational Records Classification System.

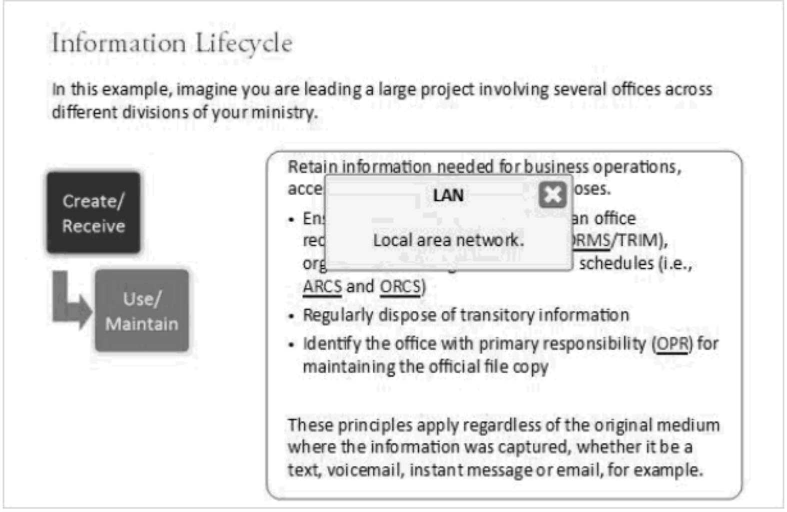
In our example, project information would be categorized according to the ARCS classification for large administrative projects.

Of course, not all government information has to be kept - and this will be discussed later.

Since your project involves multiple offices of your ministry, you will need to be clear about which office is the office of primary responsibility (or "OPR") for the project. The OPR maintains the official file copy of government information.

In our example, you are the project lead and your office is the OPR. If other offices in your ministry need to keep copies of project information for their own business purposes, they can keep them as "non-OPR" copies and dispose of them when they no longer need them.

LAN (Slide Layer)



Information Lifecycle

In this example, imagine you are leading a large project involving several offices across different divisions of your ministry.

Retain information needed for business operations,
acce oses.

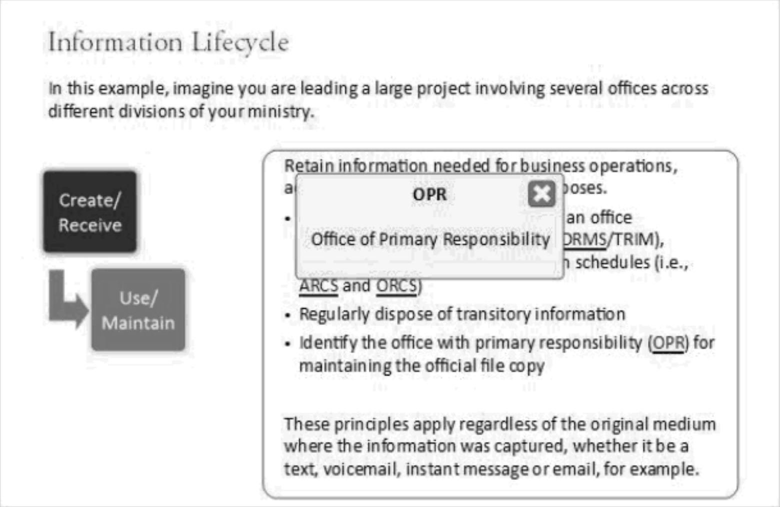
- En an office
  rec RMS/TRIM),
  org schedules (i.e.,
  ARCS and ORCS)
- Regularly dispose of transitory information
- Identify the office with primary responsibility (OPR) for maintaining the official file copy

These principles apply regardless of the original medium where the information was captured, whether it be a text, voicemail, instant message or email, for example.

LAN

Local area network.

OPR (Slide Layer)



Information Lifecycle

In this example, imagine you are leading a large project involving several offices across different divisions of your ministry.

Create/ Receive

Use/ Maintain

Retain information needed for business operations, a oses.

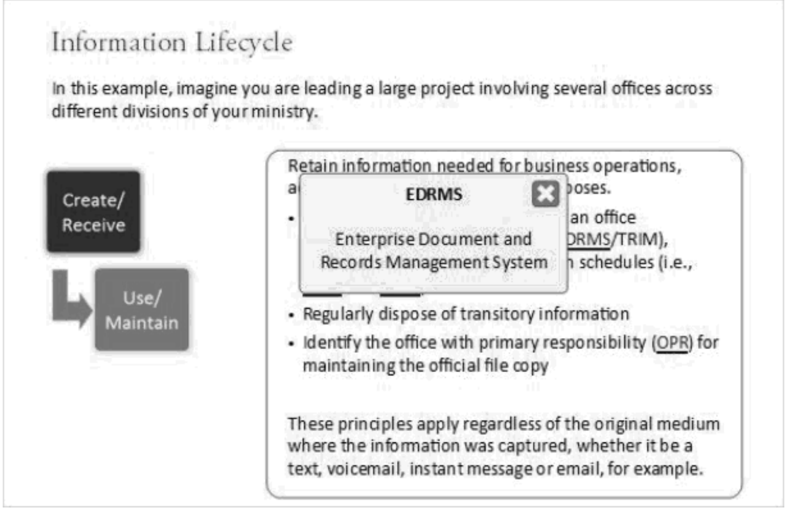
- an office DRMS/TRIM), schedules (i.e., ARCS and ORCS)
- Regularly dispose of transitory information
- Identify the office with primary responsibility (OPR) for maintaining the official file copy

These principles apply regardless of the original medium where the information was captured, whether it be a text, voicemail, instant message or email, for example.

OPR

Office of Primary Responsibility

EDRMS (Slide Layer)



Information Lifecycle

In this example, imagine you are leading a large project involving several offices across different divisions of your ministry.

Create/ Receive

Use/ Maintain

Retain information needed for business operations, a oses.

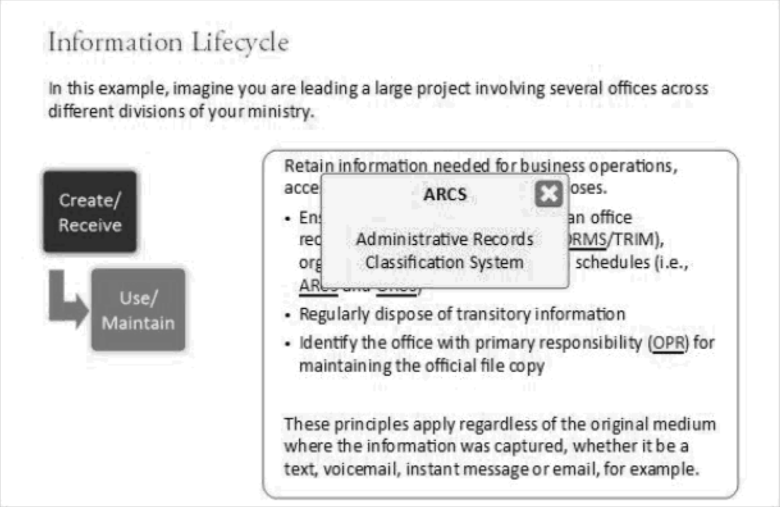
- an office DRMS/TRIM), schedules (i.e.,
- Regularly dispose of transitory information
- Identify the office with primary responsibility (OPR) for maintaining the official file copy

These principles apply regardless of the original medium where the information was captured, whether it be a text, voicemail, instant message or email, for example.

EDRMS

Enterprise Document and Records Management System

ARCS (Slide Layer)



Information Lifecycle

In this example, imagine you are leading a large project involving several offices across different divisions of your ministry.

Retain information needed for business operations, acce oses.

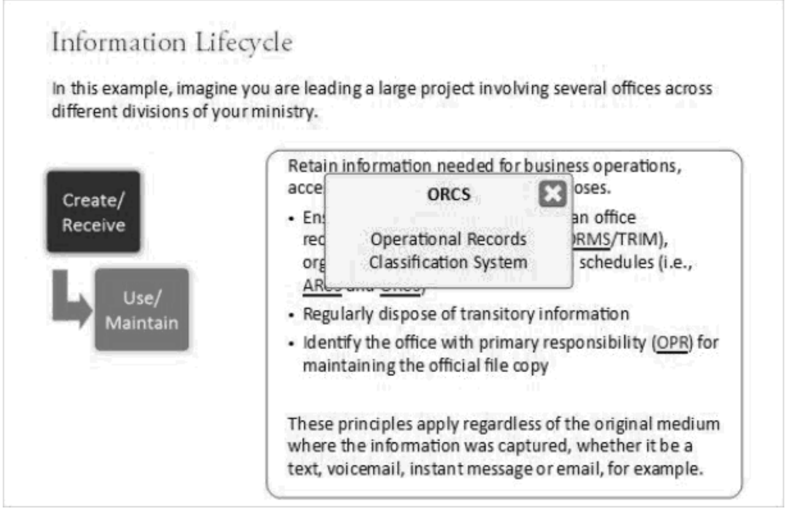
- En an office rec RMS/TRIM), org schedules (i.e., ARCS and ORCS)
- Regularly dispose of transitory information
- Identify the office with primary responsibility (OPR) for maintaining the official file copy

These principles apply regardless of the original medium where the information was captured, whether it be a text, voicemail, instant message or email, for example.

ARCS

Administrative Records Classification System

ORCS (Slide Layer)



Information Lifecycle

In this example, imagine you are leading a large project involving several offices across different divisions of your ministry.

Retain information needed for business operations, acce oses.

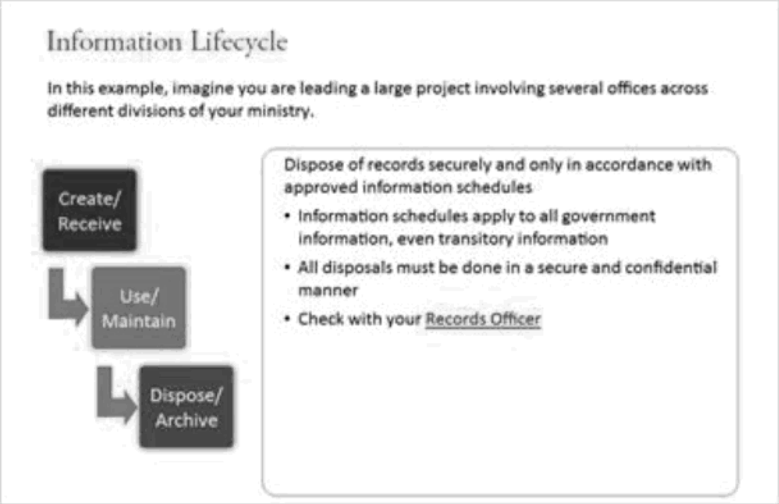
- En an office rec RMS/TRIM), org schedules (i.e., ARCS and ORCS)
- Regularly dispose of transitory information
- Identify the office with primary responsibility (OPR) for maintaining the official file copy

These principles apply regardless of the original medium where the information was captured, whether it be a text, voicemail, instant message or email, for example.

ORCS

Operational Records Classification System

3.6 Information Lifecycle



Information Lifecycle

In this example, imagine you are leading a large project involving several offices across different divisions of your ministry.

Create/ Receive

Use/ Maintain

Dispose/ Archive

Dispose of records securely and only in accordance with approved information schedules

- Information schedules apply to all government information, even transitory information
- All disposals must be done in a secure and confidential manner
- Check with your Records Officer

Notes:

Dispose/Archive

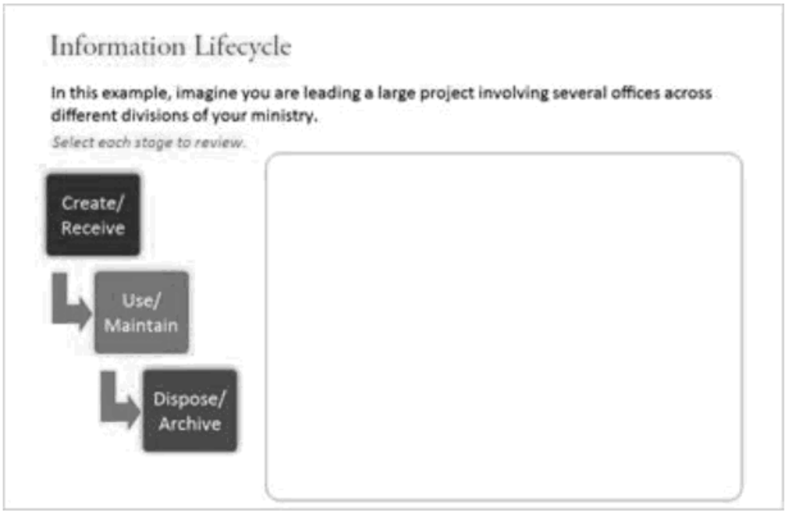
Information schedules provide timetables which tell us how long different types of information is needed and when the information may be disposed of or sent to the government archives.

This is important because you cannot dispose of information unless there is an information schedule to authorize it. Some information schedules identify information that must never be disposed of, but rather must be maintained until it is ready to be transferred to the government archives. Transitory information has its own information schedule that allows you to dispose of the information when it is no longer useful. You will learn more about transitory information shortly.

All disposals must be carried out in a secure and confidential manner. The more sensitive information is, the more measures we have to take to ensure it is securely and appropriately disposed of. Your Records Officer in the Government Records Service (GRS) can help with this.

Returning to our example, once the project is completed or cancelled and a further two years have elapsed, your project file can be disposed of. This meets the requirements established in ARCS for large-scale projects.

3.7 Information Lifecycle



Information Lifecycle

In this example, imagine you are leading a large project involving several offices across different divisions of your ministry.

Select each stage to review.

Notes:

Dispose/Archive

Information schedules provide timetables which tell us how long different types of information is needed and when the information may be disposed of or sent to the government archives.

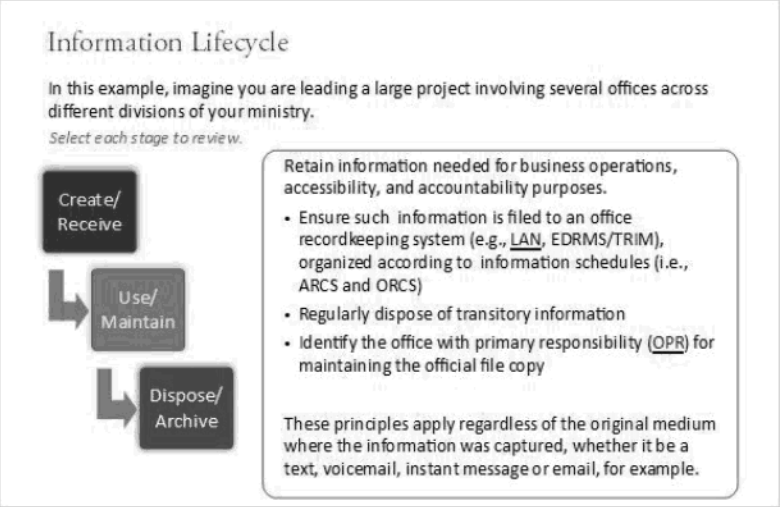
This is important because you cannot dispose of information unless there is an information schedule to authorize it. Some information schedules identify information that must never be disposed of, but rather must be maintained until it is ready to be transferred to the government archives. Transitory information has its own information schedule that allows you to dispose of the information when it is no longer useful. You will learn more about transitory information shortly.

All disposals must be carried out in a secure and confidential manner. The more sensitive information is, the more measures we have to take to ensure it is securely and appropriately disposed of. Your Records Officer in the

Government Records Service (GRS) can help with this.

Returning to our example, once the project is completed or cancelled and a further two years have elapsed, your project file can be disposed of. This meets the requirements established in ARCS for large-scale projects.

Maintain (Slide Layer)



Information Lifecycle

In this example, imagine you are leading a large project involving several offices across different divisions of your ministry.

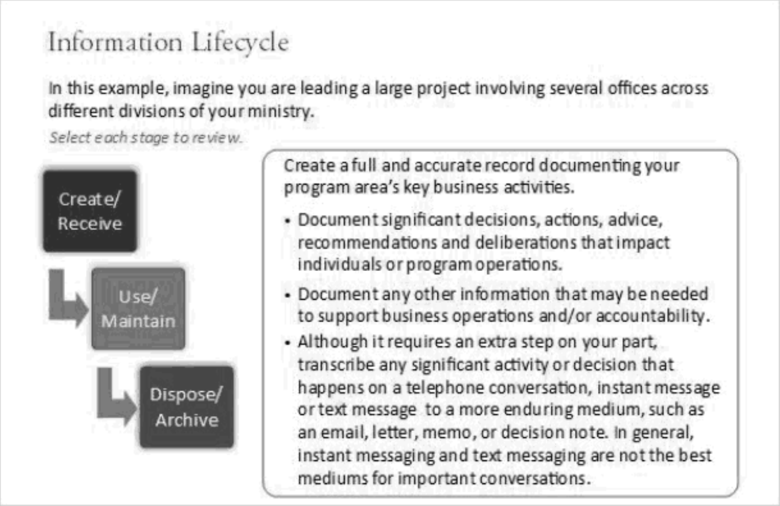
Select each stage to review.

Retain information needed for business operations, accessibility, and accountability purposes.

- Ensure such information is filed to an office recordkeeping system (e.g., LAN, EDRMS/TRIM), organized according to information schedules (i.e., ARCS and ORCS)
- Regularly dispose of transitory information
- Identify the office with primary responsibility (OPR) for maintaining the official file copy

These principles apply regardless of the original medium where the information was captured, whether it be a text, voicemail, instant message or email, for example.

Create (Slide Layer)



Information Lifecycle

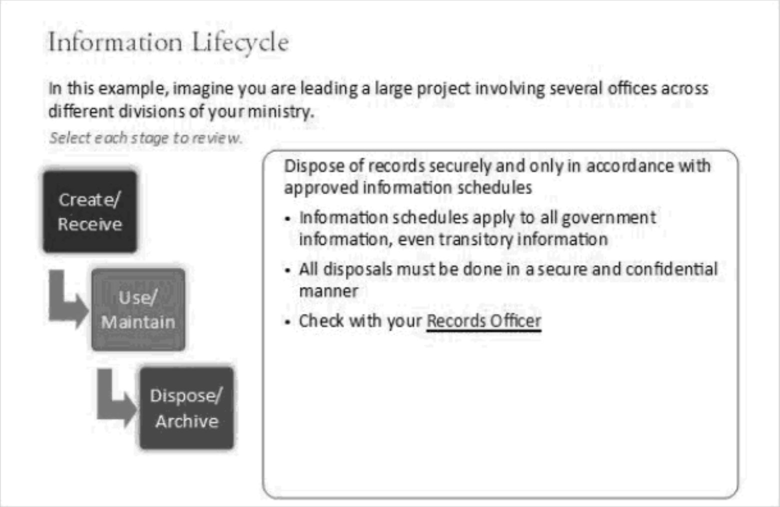
In this example, imagine you are leading a large project involving several offices across different divisions of your ministry.

Select each stage to review.

Create a full and accurate record documenting your program area's key business activities.

- Document significant decisions, actions, advice, recommendations and deliberations that impact individuals or program operations.
- Document any other information that may be needed to support business operations and/or accountability.
- Although it requires an extra step on your part, transcribe any significant activity or decision that happens on a telephone conversation, instant message or text message to a more enduring medium, such as an email, letter, memo, or decision note. In general, instant messaging and text messaging are not the best mediums for important conversations.

Dispose (Slide Layer)



Information Lifecycle

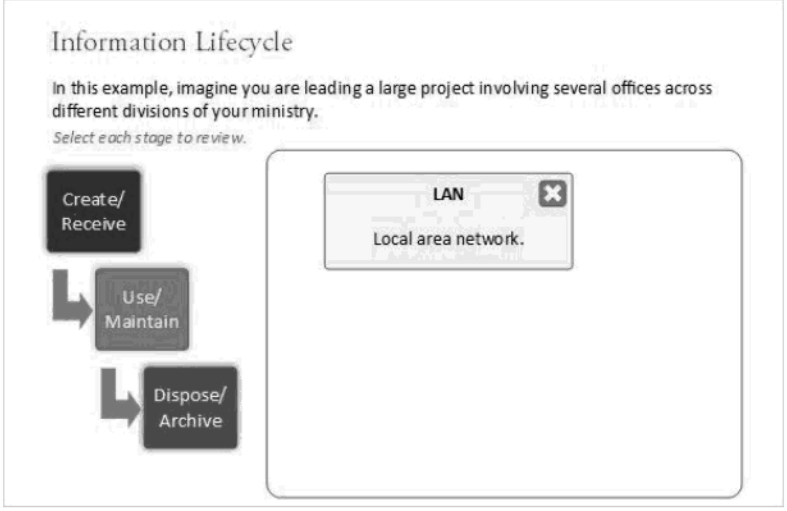
In this example, imagine you are leading a large project involving several offices across different divisions of your ministry.

Select each stage to review.

Dispose of records securely and only in accordance with approved information schedules

- Information schedules apply to all government information, even transitory information
- All disposals must be done in a secure and confidential manner
- Check with your Records Officer

LAN (Slide Layer)



Information Lifecycle

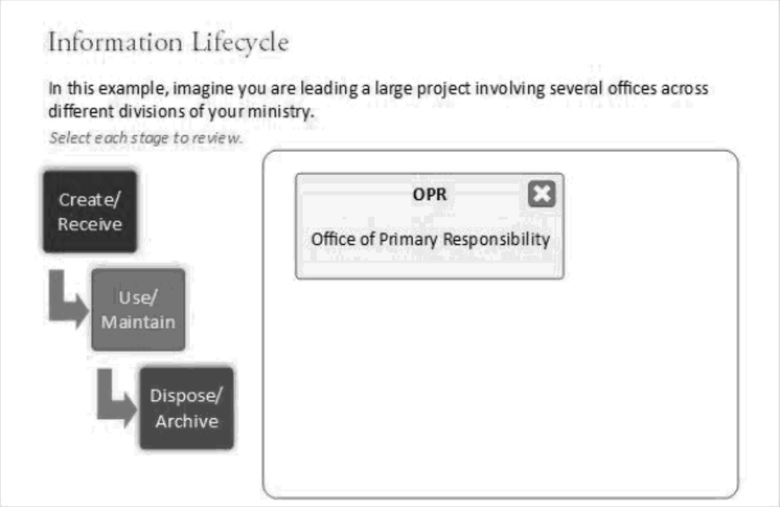
In this example, imagine you are leading a large project involving several offices across different divisions of your ministry.

Select each stage to review.

LAN

Local area network.

OPR (Slide Layer)



Information Lifecycle

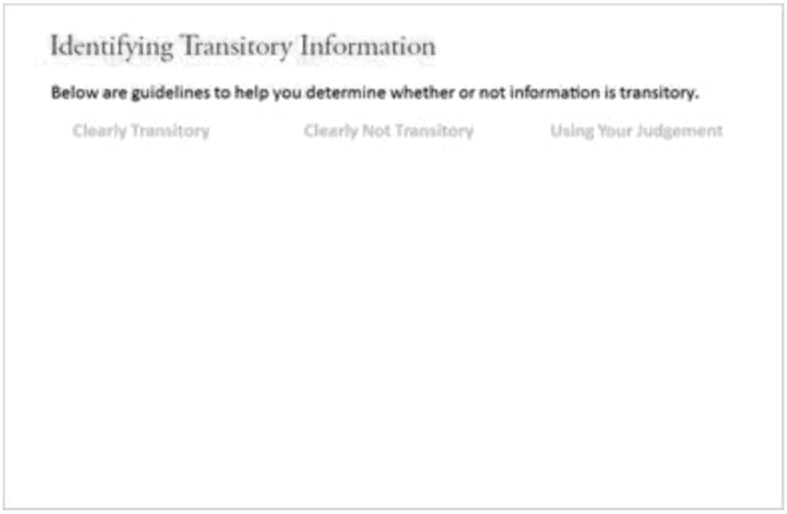
In this example, imagine you are leading a large project involving several offices across different divisions of your ministry.

Select each stage to review.

OPR

Office of Primary Responsibility

3.8 Identifying Transitory Information



Identifying Transitory Information

Below are guidelines to help you determine whether or not information is transitory.

Notes:

It can be a challenge to determine whether information is transitory, but there are some general guidelines you can follow to help make the determination easier.

Clearly Transitory
Duplicated information is a good example of what can be transitory. Imagine a typical email conversation that goes something like this:

Email from another office: “Have you considered the proposal that we talked about?”
You respond: “Yes, I like the idea, could you please send it in writing?”
Other office: “Here it is. Tell me if you need any changes.”
You: “Your proposal (attached) is approved.”

In this simple example, you will end up with four emails, two sent and two received. Each of which contains the previous emails. In this example, you can feel confident deleting the first three emails if you are retaining the fourth, as the fourth contains the entire chain, as well as the decision.

As another example, if you make a handwritten note while you are listening to a voicemail, and then copy your note into an email, you can delete the voicemail, and dispose of your handwritten note as transitory.

Non-substantive prior drafts, which can include those that contain changes to elements like the formatting and margins, or corrections to grammatical errors are also transitory. Drafts that were never circulated or reviewed are also considered non-substantive.

Even though transitory information may be disposed of when it is no longer required, it is unlawful to delete or destroy any transitory record that is the subject of a current FOI request.

Transitory records also must not be deleted where they may be relevant to an expected future legal action.

Clearly Not Transitory
Information that is clearly not transitory would include incoming public correspondence, meeting minutes, and case files. You may, however, have copies of information such as meeting minutes that are transitory, provided that:

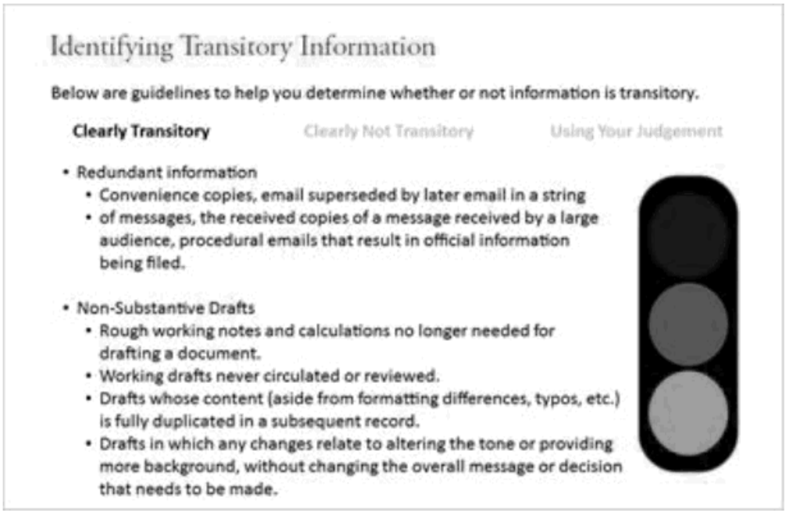
- You know that you are not the Office of Primary Responsibility or OPR, and
- Your office has no need to file your copies for its own business use.

Using Your Judgement
When faced with information that is neither clearly transitory or official, you will need to ask yourself these questions:

- Does the information document an important activity, or decision?
- To what extent is this already documented somewhere else?
- Is the information important in relation to the activity for which it was created or which it was used to support?
- In relation to other information, does this information best document the function or activity for which it was created or which it was used to support?

If you are unsure as to whether something is transitory or not, you can contact your Records Officer in the Government Records Service (GRS) for assistance.

3.9 Identifying Transitory Information



Identifying Transitory Information

Below are guidelines to help you determine whether or not information is transitory.

- Redundant information
  - Convenience copies, email superseded by later email in a string
  - of messages, the received copies of a message received by a large audience, procedural emails that result in official information being filed.
- Non-Substantive Drafts
  - Rough working notes and calculations no longer needed for drafting a document.
  - Working drafts never circulated or reviewed.
  - Drafts whose content (aside from formatting differences, typos, etc.) is fully duplicated in a subsequent record.
  - Drafts in which any changes relate to altering the tone or providing more background, without changing the overall message or decision that needs to be made.

Notes:

It can be a challenge to determine whether information is transitory, but there are some general guidelines you can follow to help make the determination easier.

Clearly Transitory

Duplicated information is a good example of what can be transitory. Imagine a typical email conversation that goes something like this:

Email from another office: “Have you considered the proposal that we talked about?”
You respond: “Yes, I like the idea, could you please send it in writing?”
Other office: “Here it is. Tell me if you need any changes.”
You: “Your proposal (attached) is approved.”

In this simple example, you will end up with four emails, two sent and two received. Each of which contains the previous emails. In this example, you can feel confident deleting the first three emails if you are retaining the fourth, as the fourth contains the entire chain, as well as the decision.

As another example, if you make a handwritten note while you are listening to a voicemail, and then copy your note into an email, you can delete the voicemail, and dispose of your handwritten note as transitory.

Non-substantive prior drafts, which can include those that contain changes to elements like the formatting and margins, or corrections to grammatical errors are also transitory. Drafts that were never circulated or reviewed are also considered non-substantive.

Even though transitory information may be disposed of when it is no longer required, it is unlawful to delete or destroy any transitory record that is the subject of a current FOI request.

Transitory records also must not be deleted where they may be relevant to an expected future legal action.

Clearly Not Transitory
Information that is clearly not transitory would include incoming public correspondence, meeting minutes, and case files. You may, however, have copies of information such as meeting minutes that are transitory, provided that:

- You know that you are not the Office of Primary Responsibility or OPR, and

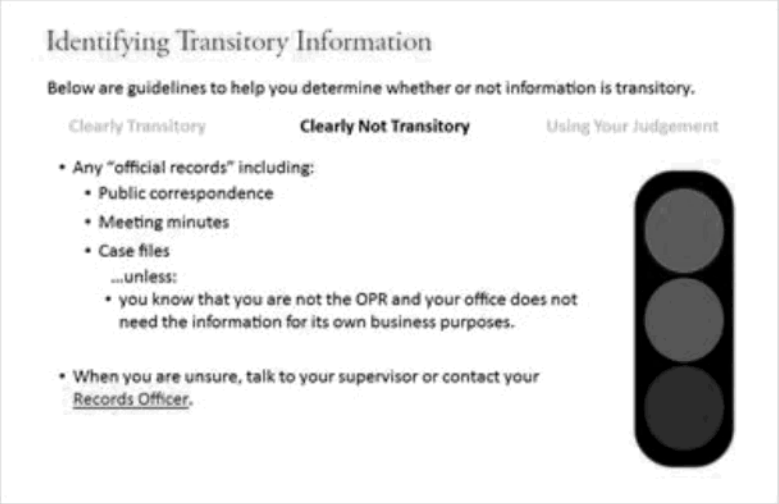
- Your office has no need to file your copies for its own business use.

Using Your Judgement
When faced with information that is neither clearly transitory or official, you will need to ask yourself these questions:

- Does the information document an important activity, or decision?
- To what extent is this already documented somewhere else?
- Is the information important in relation to the activity for which it was created or which it was used to support?
- In relation to other information, does this information best document the function or activity for which it was created or which it was used to support?

If you are unsure as to whether something is transitory or not, you can contact your Records Officer in the Government Records Service (GRS) for assistance.

3.10 Identifying Transitory Information



Identifying Transitory Information

Below are guidelines to help you determine whether or not information is transitory.

Clearly Transitory | **Clearly Not Transitory** | Using Your Judgement

- Any "official records" including:
  - Public correspondence
  - Meeting minutes
  - Case files

    ...unless:
    - you know that you are not the OPR and your office does not need the information for its own business purposes.
- When you are unsure, talk to your supervisor or contact your Records Officer.

Notes:

It can be a challenge to determine whether information is transitory, but there are some general guidelines you can follow to help make the determination easier.

Clearly Transitory

Duplicated information is a good example of what can be transitory. Imagine a typical email conversation that goes something like this:

Email from another office: “Have you considered the proposal that we talked about?”
You respond: “Yes, I like the idea, could you please send it in writing?”
Other office: “Here it is. Tell me if you need any changes.”
You: “Your proposal (attached) is approved.”

In this simple example, you will end up with four emails, two sent and two received. Each of which contains the previous emails. In this example, you can feel confident deleting the first three emails if you are retaining the fourth, as the fourth contains the entire chain, as well as the decision.

As another example, if you make a handwritten note while you are listening to a voicemail, and then copy your note into an email, you can delete the voicemail, and dispose of your handwritten note as transitory.

Non-substantive prior drafts, which can include those that contain changes to elements like the formatting and margins, or corrections to grammatical errors are also transitory. Drafts that were never circulated or reviewed are also considered non-substantive.

Even though transitory information may be disposed of when it is no longer required, it is unlawful to delete or destroy any transitory record that is the subject of a current FOI request.

Transitory records also must not be deleted where they may be relevant to an expected future legal action.

Clearly Not Transitory

Information that is clearly not transitory would include incoming public correspondence, meeting minutes, and case files. You may, however, have copies of information such as meeting minutes that are transitory, provided that:

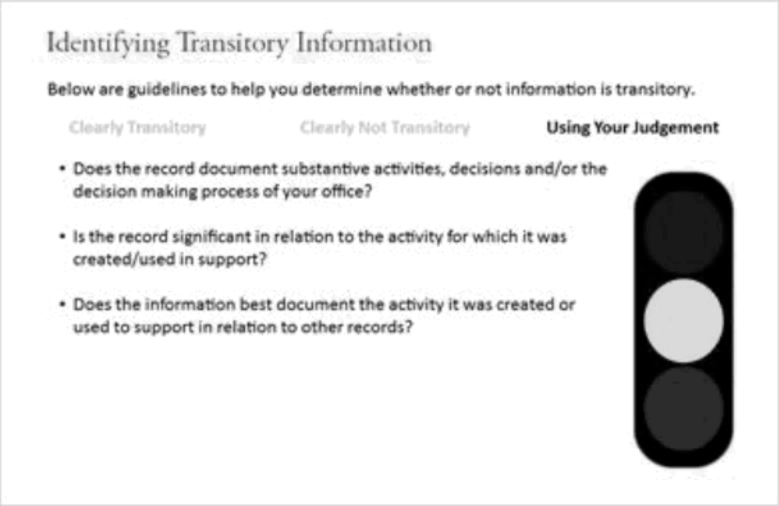
- You know that you are not the Office of Primary Responsibility or OPR, and
- Your office has no need to file your copies for its own business use.

Using Your Judgement
When faced with information that is neither clearly transitory or official, you will need to ask yourself these questions:

- Does the information document an important activity, or decision?
- To what extent is this already documented somewhere else?
- Is the information important in relation to the activity for which it was created or which it was used to support?
- In relation to other information, does this information best document the function or activity for which it was created or which it was used to support?

If you are unsure as to whether something is transitory or not, you can contact your Records Officer in the Government Records Service (GRS) for assistance.

3.11 Identifying Transitory Information



Identifying Transitory Information

Below are guidelines to help you determine whether or not information is transitory.

Clearly Transitory   Clearly Not Transitory   **Using Your Judgement**

- Does the record document substantive activities, decisions and/or the decision making process of your office?
- Is the record significant in relation to the activity for which it was created/used in support?
- Does the information best document the activity it was created or used to support in relation to other records?

Notes:

It can be a challenge to determine whether information is transitory, but there are some general guidelines you can follow to help make the determination easier.

Clearly Transitory

Duplicated information is a good example of what can be transitory. Imagine a typical email conversation that goes something like this:

Email from another office: “Have you considered the proposal that we talked about?”
You respond: “Yes, I like the idea, could you please send it in writing?”
Other office: “Here it is. Tell me if you need any changes.”
You: “Your proposal (attached) is approved.”

In this simple example, you will end up with four emails, two sent and two received. Each of which contains the previous emails. In this example, you can feel confident deleting the first three emails if you are retaining the fourth, as the fourth contains the entire chain, as well as the decision.

As another example, if you make a handwritten note while you are listening to a voicemail, and then copy your note into an email, you can delete the voicemail, and dispose of your handwritten note as transitory.

Non-substantive prior drafts, which can include those that contain changes to elements like the formatting and margins, or corrections to grammatical errors are also transitory. Drafts that were never circulated or reviewed are also considered non-substantive.

Even though transitory information may be disposed of when it is no longer required, it is unlawful to delete or destroy any transitory record that is the subject of a current FOI request.

Transitory records also must not be deleted where they may be relevant to an expected future legal action.

Clearly Not Transitory

Information that is clearly not transitory would include incoming public correspondence, meeting minutes, and case files. You may, however, have copies of information such as meeting minutes that are transitory, provided that:

- You know that you are not the Office of Primary Responsibility or OPR, and
- Your office has no need to file your copies for its own business use.

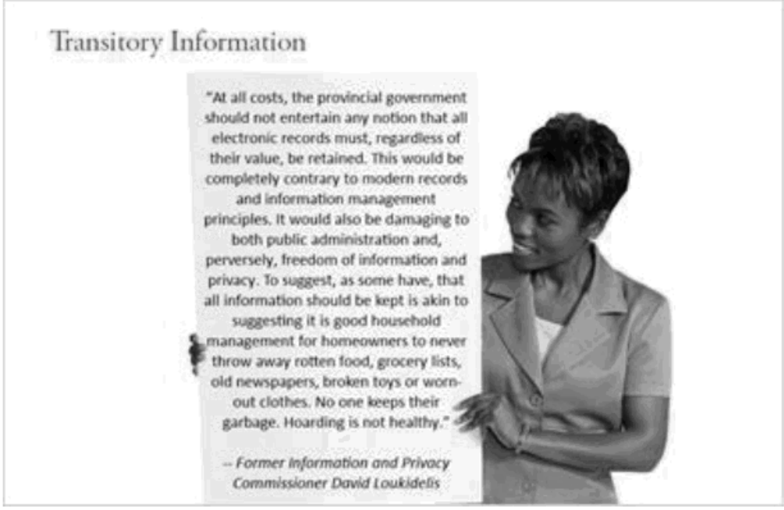
Using Your Judgement

When faced with information that is neither clearly transitory or official, you will need to ask yourself these questions:

- Does the information document an important activity, or decision?
- To what extent is this already documented somewhere else?
- Is the information important in relation to the activity for which it was created or which it was used to support?
- In relation to other information, does this information best document the function or activity for which it was created or which it was used to support?

If you are unsure as to whether something is transitory or not, you can contact your Records Officer in the Government Records Service (GRS) for assistance.

3.12 Transitory Information



Transitory Information

"At all costs, the provincial government should not entertain any notion that all electronic records must, regardless of their value, be retained. This would be completely contrary to modern records and information management principles. It would also be damaging to both public administration and, perversely, freedom of information and privacy. To suggest, as some have, that all information should be kept is akin to suggesting it is good household management for homeowners to never throw away rotten food, grocery lists, old newspapers, broken toys or worn-out clothes. No one keeps their garbage. Hoarding is not healthy."

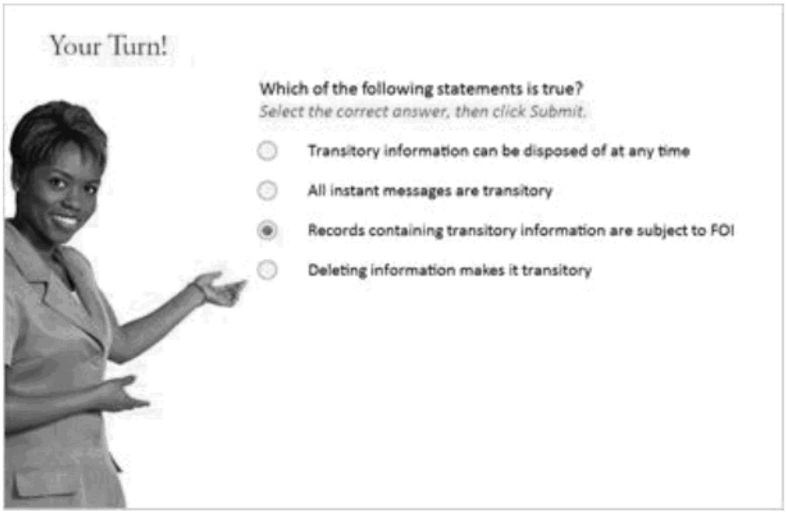
-- Former Information and Privacy Commissioner David Loukidelis

Notes:

It is also important to remember that not all electronic records must be retained. Take a moment to reflect on these words.

3.13 Your Turn!

(Multiple Choice, 10 points, 1 attempt permitted)



Your Turn!

Which of the following statements is true?

Select the correct answer, then click Submit.

○ Transitory information can be disposed of at any time

○ All instant messages are transitory

● Records containing transitory information are subject to FOI

○ Deleting information makes it transitory

Correct	Choice
	Transitory information can be disposed of at any time
	All instant messages are transitory
X	Records containing transitory information are subject to FOI
	Deleting information makes it transitory

Feedback when correct:

That's right! Records containing transitory information are subject to FOI. Transitory information can be disposed of at any time after it is no longer needed.

Deleting information does not make it transitory. The transitory information schedule determines which information can be deleted and when – not the other way around.

Transitory information that is subject to an FOI request or litigation hold, even if it is transitory, cannot be deleted while the request is being processed or the legal issue is still unresolved.

Work-related instant messages that document key decisions are not considered transitory. In general, instant messaging is not the best medium for important conversations.

Feedback when incorrect:

You did not select the correct response. Records containing transitory information are subject to FOI. Transitory information can be disposed of at any time after it is no longer needed.

Deleting information does not make it transitory. The transitory information schedule determines which information can be deleted and when – not the other way around.

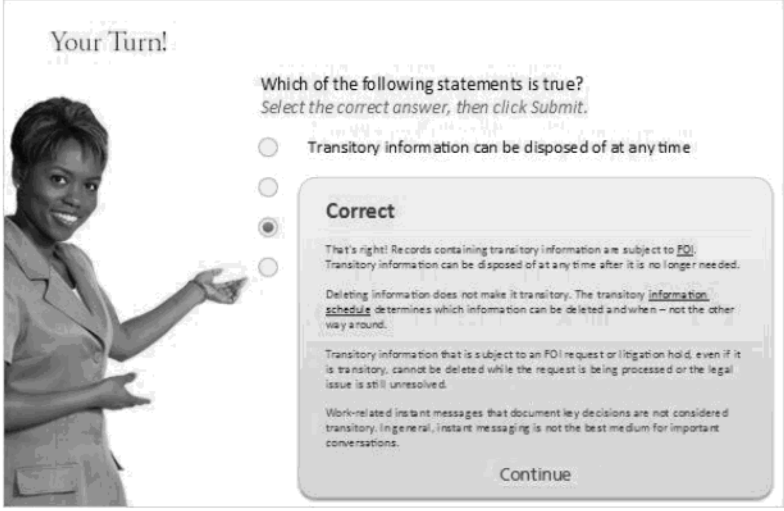
Transitory information that is subject to an FOI request or litigation hold, even if it is transitory, cannot be deleted while the request is being processed or the legal issue is still unresolved.

Work-related instant messages that document key decisions are not considered transitory. In general, instant messaging is not the best medium for important conversations.

Notes:

Now that we've spent some time talking about transitory information, try this knowledge check.

Correct (Slide Layer)



Your Turn!

Which of the following statements is true?
Select the correct answer, then click Submit.

○ Transitory information can be disposed of at any time

○

●

○

Correct

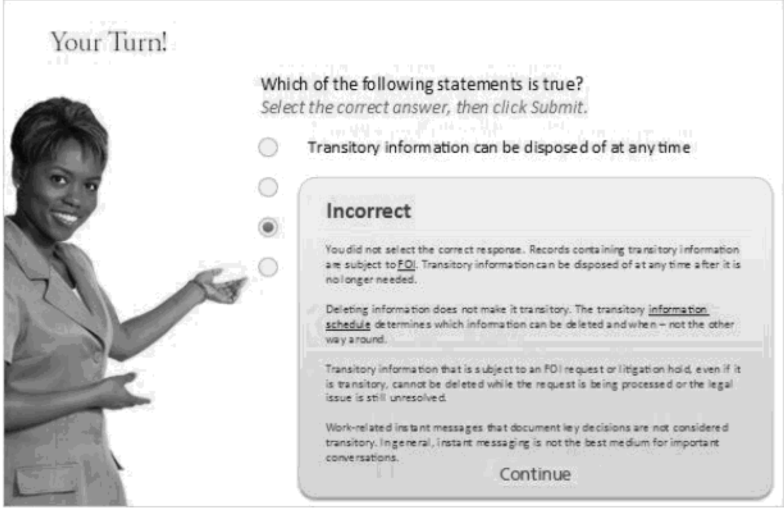
That's right! Records containing transitory information are subject to FOI. Transitory information can be disposed of at any time after it is no longer needed.

Deleting information does not make it transitory. The transitory information schedule determines which infomation can be deleted and when – not the other way around.

Transitory information that is subject to an FOI request or litigation hold, even if it is transitory, cannot be deleted while the request is being processed or the legal issue is still unresolved.

Work-related instant messages that document key decisions are not considered transitory. In general, instant messaging is not the best medium for important conversations.

Incorrect (Slide Layer)



Your Turn!

Which of the following statements is true?
Select the correct answer, then click Submit.

○ Transitory information can be disposed of at any time

○

●

○

Incorrect

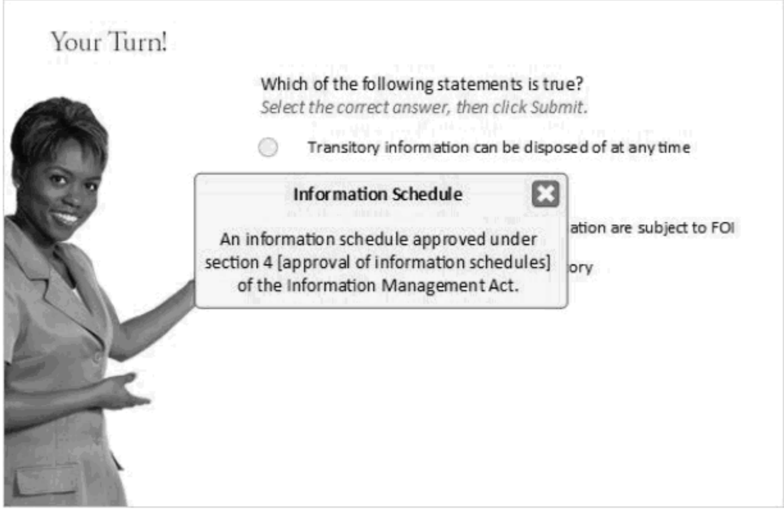
You did not select the correct response. Records containing transitory information are subject to FOI. Transitory information can be disposed of at any time after it is no longer needed.

Deleting information does not make it transitory. The transitory information schedule determines which infomation can be deleted and when – not the other way around.

Transitory information that is subject to an FOI request or litigation hold, even if it is transitory, cannot be deleted while the request is being processed or the legal issue is still unresolved.

Work-related instant messages that document key decisions are not considered transitory. In general, instant messaging is not the best medium for important conversations.

Information Schedule (Slide Layer)



Your Turn!

Which of the following statements is true?

Select the correct answer, then click Submit.

○ Transitory information can be disposed of at any time

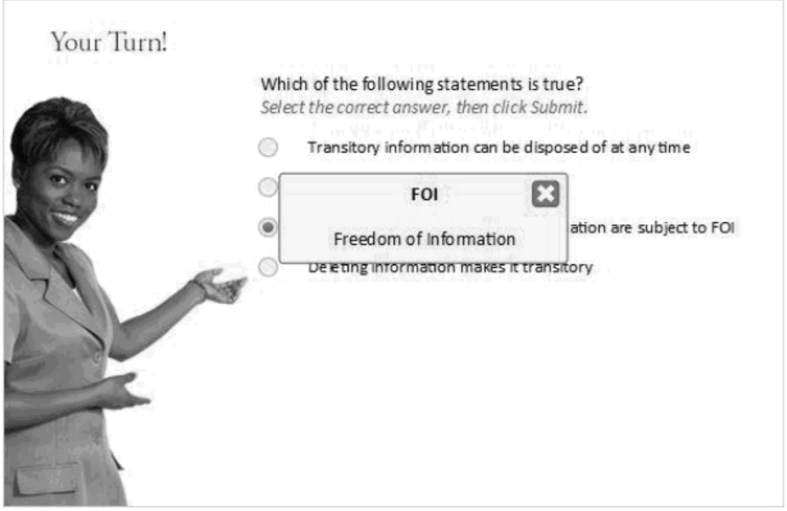
ation are subject to FOI

ory

Information Schedule

An information schedule approved under section 4 [approval of information schedules] of the Information Management Act.

FOI (Slide Layer)



Your Turn!

Which of the following statements is true?

Select the correct answer, then click Submit.

○ Transitory information can be disposed of at any time

○

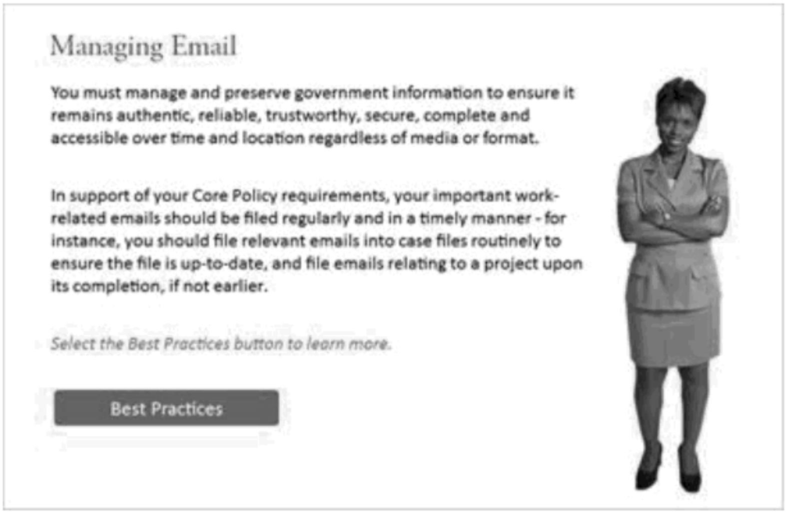
● ation are subject to FOI

○ Deleting information makes it transitory

FOI

Freedom of Information

3.14 Managing Email



Managing Email

You must manage and preserve government information to ensure it remains authentic, reliable, trustworthy, secure, complete and accessible over time and location regardless of media or format.

In support of your Core Policy requirements, your important work-related emails should be filed regularly and in a timely manner - for instance, you should file relevant emails into case files routinely to ensure the file is up-to-date, and file emails relating to a project upon its completion, if not earlier.

Select the Best Practices button to learn more.

Notes:

It is important to remember that work emails contain government information. How you manage email depends on its content.

You know your work and therefore you are able to determine which emails are important to that work. If you have emails with information that will either be useful to document the work of your office or for others in doing their work, then you should file those emails in your office recordkeeping system. Likely, for most of you, this won't be a significant number of your emails. Most of the information we share by email is repeated in other documents and is already stored elsewhere. But if you think the email contains the only copy of an important piece of information, you should save a copy, or use the email to prepare a formal document and then dispose of it.

It can be challenging to manage emails when they contain a lot of different topics or move into overlapping and lengthy threads. If you can, try to be specific, to limit the content of your email to one subject area, and to clean up email chains and lengthy threads.

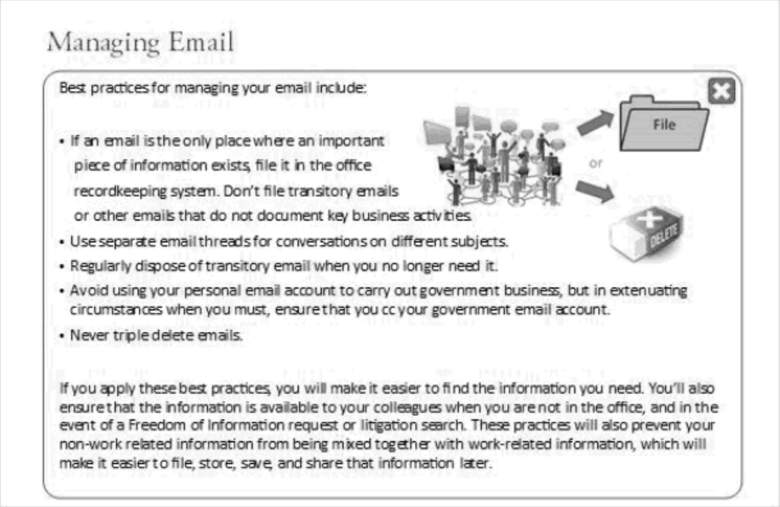
You should also try to stay on top of tasks like regularly deleting transitory email. Many emails are only of temporary use and are therefore considered transitory.

For example, a ministry-wide notice to all employees can usually be disposed of as transitory. It is the responsibility of the initiating office to file and maintain an official copy, in their office recordkeeping system.

You should also avoid using your personal email account to do your work. In the extenuating circumstance when you absolutely must do so, there are rules you have to follow, which include “cc-ing” your government email account, deleting the emails from your personal email account as soon as possible, and ensuring you share the least amount of sensitive information that is necessary in the circumstance. Where that sensitive information is someone’s personal information, use additional caution to ensure that it is adequately protected. In general, personal information cannot be shared outside of Canada. We will review data residency requirements later in this material.

Lastly, you should be aware that triple deleting email, which involves purging emails from the “Recover Deleted Items” folder, is never permitted. This should not be confused with double deletion, which happens when deleted emails are cleared out of the “Deleted Items” folder. The double deletion process is important for clearing space in your Outlook folders, but must only be done if the items in question are permitted to be disposed of.

Best Practices (Slide Layer)



Managing Email

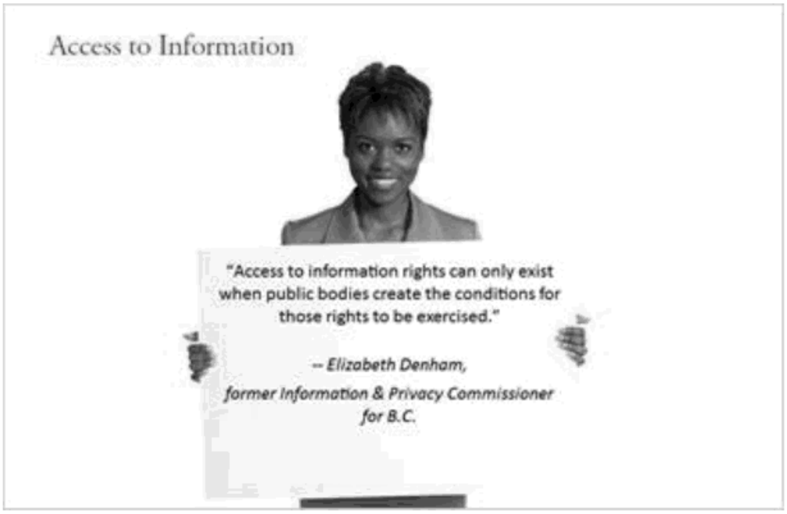
Best practices for managing your email include:

- If an email is the only place where an important piece of information exists, file it in the office recordkeeping system. Don't file transitory emails or other emails that do not document key business activities.
- Use separate email threads for conversations on different subjects.
- Regularly dispose of transitory email when you no longer need it.
- Avoid using your personal email account to carry out government business, but in extenuating circumstances when you must, ensure that you cc your government email account.
- Never triple delete emails.

If you apply these best practices, you will make it easier to find the information you need. You'll also ensure that the information is available to your colleagues when you are not in the office, and in the event of a Freedom of Information request or litigation search. These practices will also prevent your non-work related information from being mixed together with work-related information, which will make it easier to file, store, save, and share that information later.

4. Access to Information

4.1 Access to Information



Access to Information

"Access to information rights can only exist when public bodies create the conditions for those rights to be exercised."

-- Elizabeth Denham,
former Information & Privacy Commissioner for B.C.

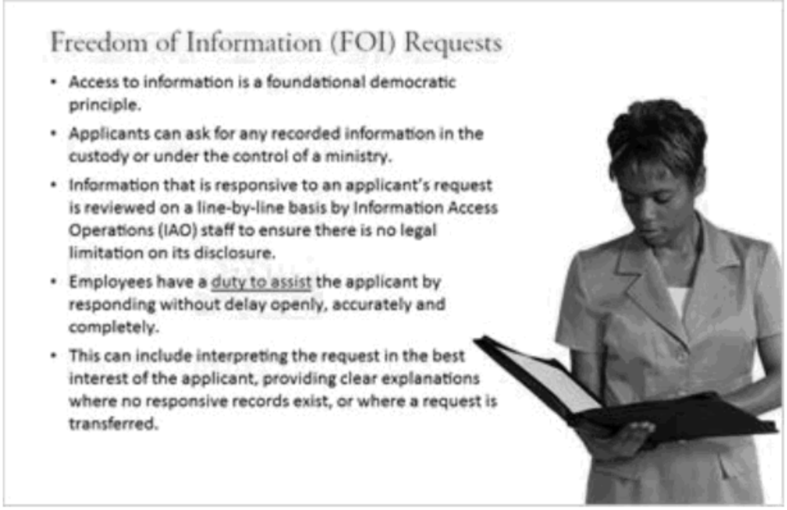
Notes:

Government is committed to expanding the public availability of government information and data through the disclosure of information without a formal Freedom of Information (FOI) request. Whenever possible, information is released to the public as permitted under the legislation and policies that apply to government or public sector organizations.

In this next section, we'll discuss access to information, and talk about both Freedom of Information, or "FOI", and proactive disclosures of information outside of the FOI process.

Remember that creating and keeping the right records is key to enabling access to information.

4.2 Freedom of Information (FOI) Requests



Freedom of Information (FOI) Requests

- Access to information is a foundational democratic principle.
- Applicants can ask for any recorded information in the custody or under the control of a ministry.
- Information that is responsive to an applicant's request is reviewed on a line-by-line basis by Information Access Operations (IAO) staff to ensure there is no legal limitation on its disclosure.
- Employees have a duty to assist the applicant by responding without delay openly, accurately and completely.
- This can include interpreting the request in the best interest of the applicant, providing clear explanations where no responsive records exist, or where a request is transferred.

Notes:

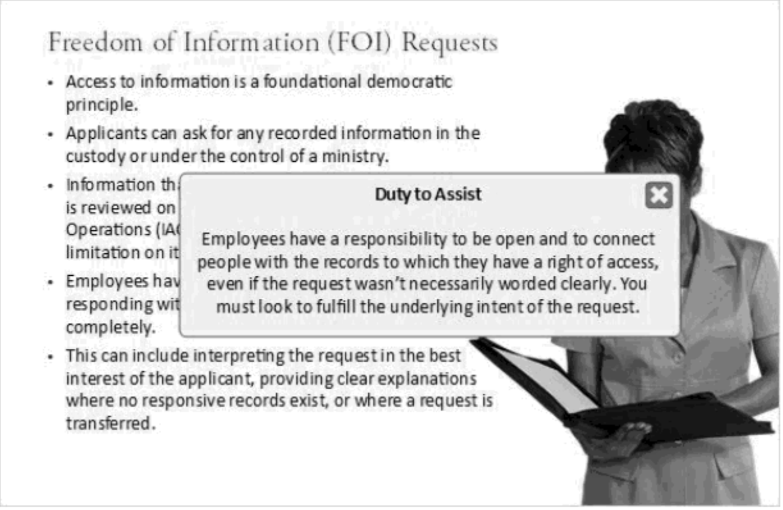
Anyone can make a Freedom of Information request. Typically, the bulk of these requests come from individuals, political parties and law firms, but requests also come in from the media, businesses, researchers, interest groups, and the public sector.

An FOI applicant can ask for any record, but it must be a specific record or records. A record includes anything on which information is recorded or stored.

Access to information in a record is granted based on a line-by-line review to ensure that the information is legally appropriate for release.

Keep in mind that we have a responsibility to be open and to connect people with the records to which they have a right of access, even if the request wasn't necessarily worded clearly. You must look to fulfill the underlying intent of the request. This is called the "duty to assist" an applicant, and we'll talk more about this concept later.

Duty to Assist (Slide Layer)



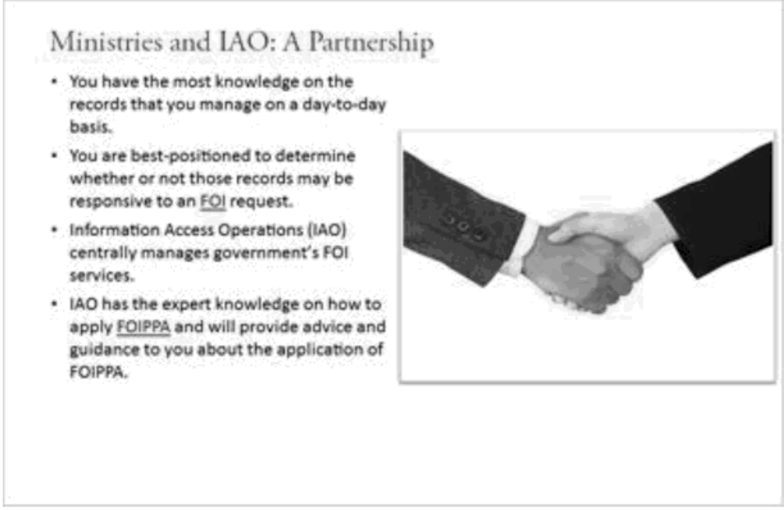
Freedom of Information (FOI) Requests

- Access to information is a foundational democratic principle.
- Applicants can ask for any recorded information in the custody or under the control of a ministry.
- Information th is reviewed on Operations (IA limitation on it
- Employees hav responding wit completely.
- This can include interpreting the request in the best interest of the applicant, providing clear explanations where no responsive records exist, or where a request is transferred.

Duty to Assist

Employees have a responsibility to be open and to connect people with the records to which they have a right of access, even if the request wasn't necessarily worded clearly. You must look to fulfill the underlying intent of the request.

4.3 Ministries and IAO: A Partnership



Ministries and IAO: A Partnership

- You have the most knowledge on the records that you manage on a day-to-day basis.
- You are best-positioned to determine whether or not those records may be responsive to an FOI request.
- Information Access Operations (IAO) centrally manages government's FOI services.
- IAO has the expert knowledge on how to apply FOIPPA and will provide advice and guidance to you about the application of FOIPPA.

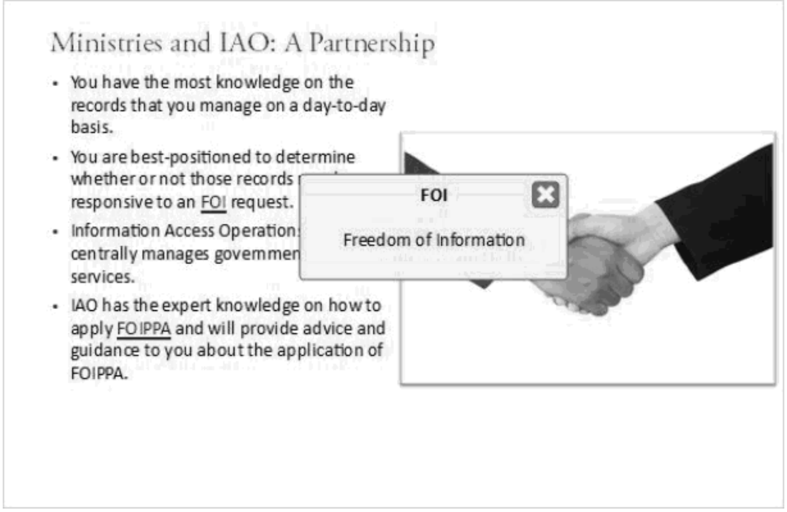
Notes:

Ministries and Information Access Operations work in concert to respond to FOI requests. As a member of the public service, you are the subject matter expert on your records. You know what information you have and whether or not the information you have is responsive to an FOI request.

You are not expected to know what section of FOIPPA may apply in terms of removing that information, but you are in the best position to identify whether something may be harmful if it were released.

You are responsible for ensuring that this information is communicated back to IAO via the Call for Records Form. IAO is the expert when it comes to processing FOI requests. They have the expertise required to apply FOIPPA, to manage the legislated timelines and to communicate with the applicant with a customer focus. IAO also possesses the technology required to effectively sever information from records as required or permitted by FOIPPA.

FOI (Slide Layer)



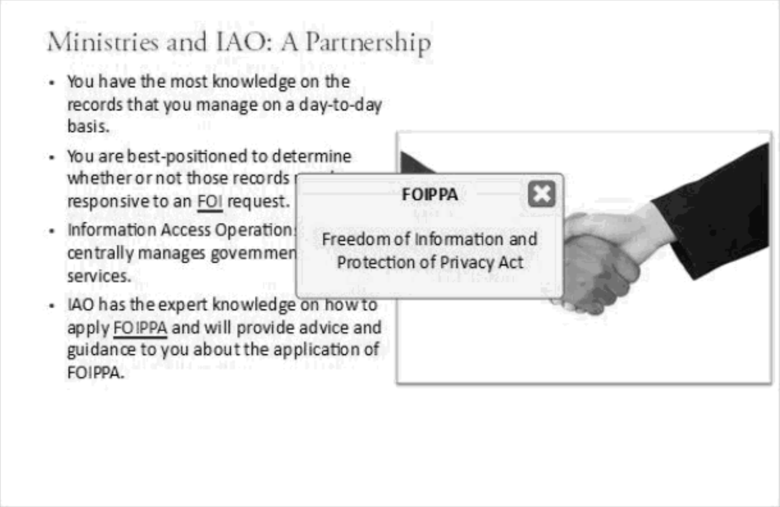
Ministries and IAO: A Partnership

- You have the most knowledge on the records that you manage on a day-to-day basis.
- You are best-positioned to determine whether or not those records
responsive to an FOI request.
- Information Access Operation
centrally manages governmen
services.
- IAO has the expert knowledge on how to apply FOIPPA and will provide advice and guidance to you about the application of FOIPPA.

FOI

Freedom of Information

FOIPPA (Slide Layer)



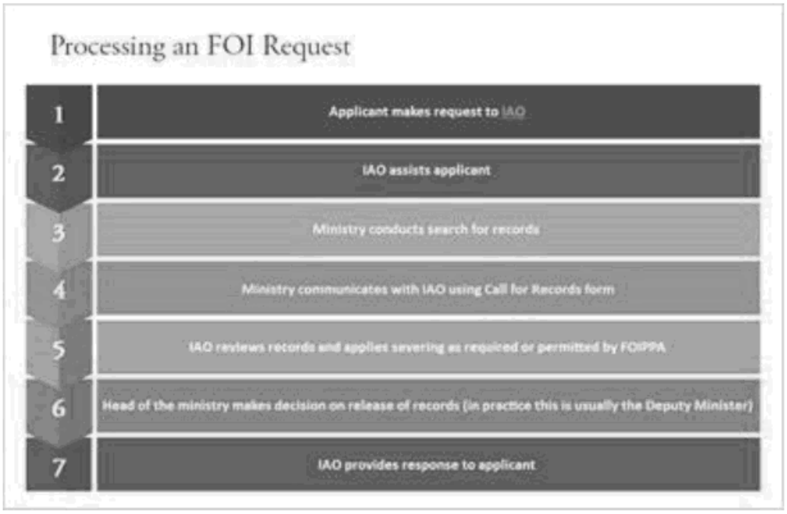
Ministries and IAO: A Partnership

- You have the most knowledge on the records that you manage on a day-to-day basis.
- You are best-positioned to determine whether or not those records
responsive to an FOI request.
- Information Access Operation
centrally manages governmen
services.
- IAO has the expert knowledge on how to apply FOIPPA and will provide advice and guidance to you about the application of FOIPPA.

FOIPPA

Freedom of Information and Protection of Privacy Act

4.4 Processing an FOI Request



Processing an FOI Request

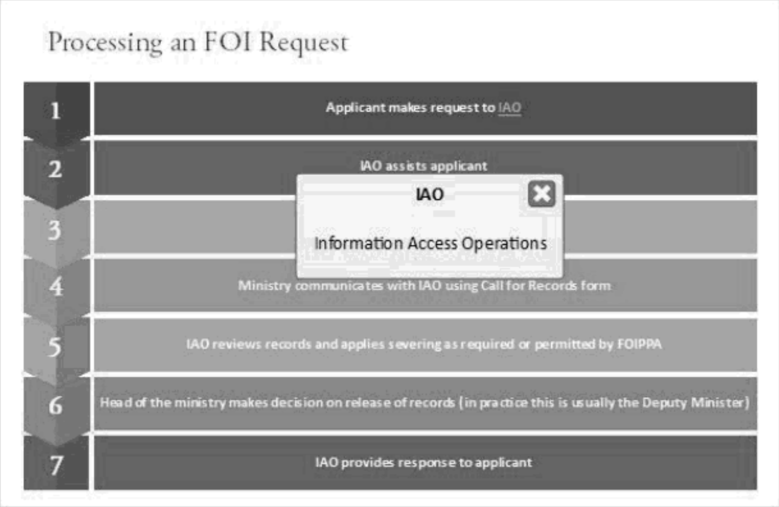
1. Applicant makes request to IAO
2. IAO assists applicant
3. Ministry conducts search for records
4. Ministry communicates with IAO using Call for Records form
5. IAO reviews records and applies severing as required or permitted by FOIPPA
6. Head of the ministry makes decision on release of records (in practice this is usually the Deputy Minister)
7. IAO provides response to applicant

Notes:

Take a moment to review this high-level overview of the FOI process for government. Remember that the purpose of this process is to create a system that will ensure an effective, customer focused information access experience.

It is also important to note that FOIPPA includes timelines for responding to FOI requests. Your FOI coordinator is an excellent resource for coordinating the FOI requests and tracking upcoming due dates. Your FOI coordinator is the person within your office from whom you receive the FOI request. For example, this can be a dedicated FOI coordinator for your ministry, or your office manager.

IAO (Slide Layer)



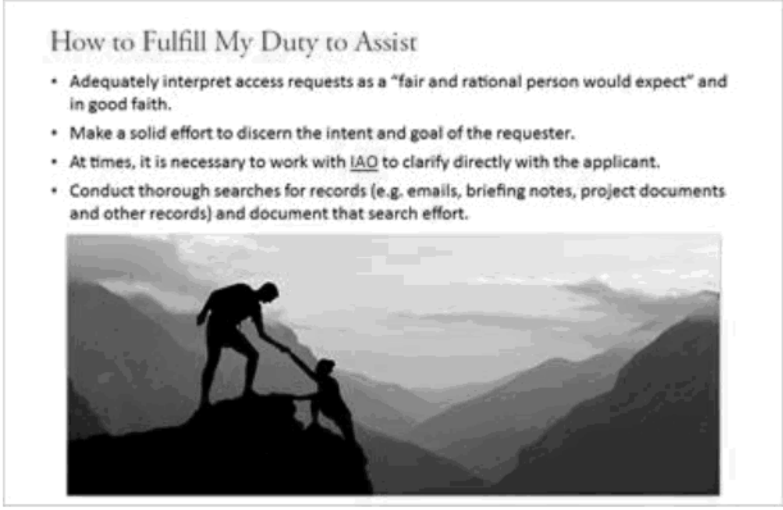
Processing an FOI Request

1. Applicant makes request to IAO
2. IAO assists applicant
3.
4. Ministry communicates with IAO using Call for Records form
5. IAO reviews records and applies severing as required or permitted by FOIPPA
6. Head of the ministry makes decision on release of records (in practice this is usually the Deputy Minister)
7. IAO provides response to applicant

IAO

Information Access Operations

4.5 How to Fulfill My Duty to Assist



How to Fulfill My Duty to Assist

- Adequately interpret access requests as a "fair and rational person would expect" and in good faith.
- Make a solid effort to discern the intent and goal of the requester.
- At times, it is necessary to work with IAO to clarify directly with the applicant.
- Conduct thorough searches for records (e.g. emails, briefing notes, project documents and other records) and document that search effort.

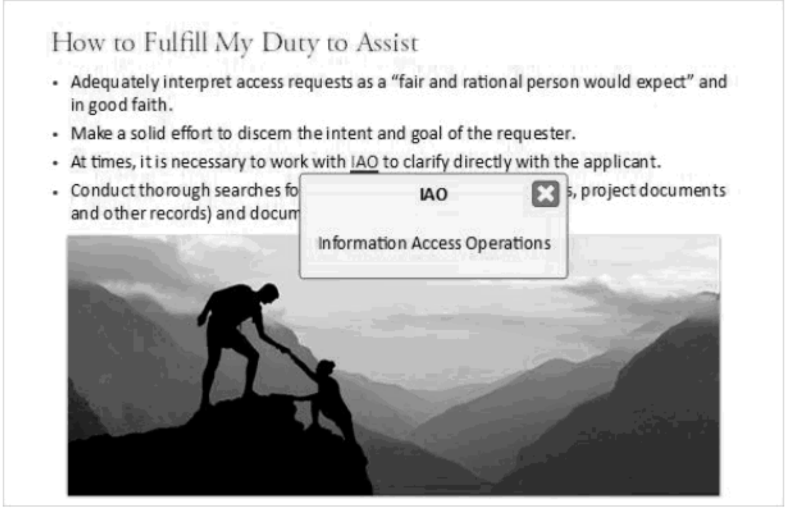
Notes:

Government employees must make every reasonable effort to assist FOI applicants and to respond to each applicant openly, accurately and completely in a timely way. After all, access to information is a foundational democratic principle.

The “duty to assist” goes beyond just meeting the letter of the law; it involves providing an excellent service experience to each applicant.

To meet your duty to assist an FOI applicant, you need to interpret FOI requests in the best interest of the applicant. This means steering clear of narrow interpretations, and following these best practices to ensure you’re being diligent in your search for responsive records.

IAO (Slide Layer)



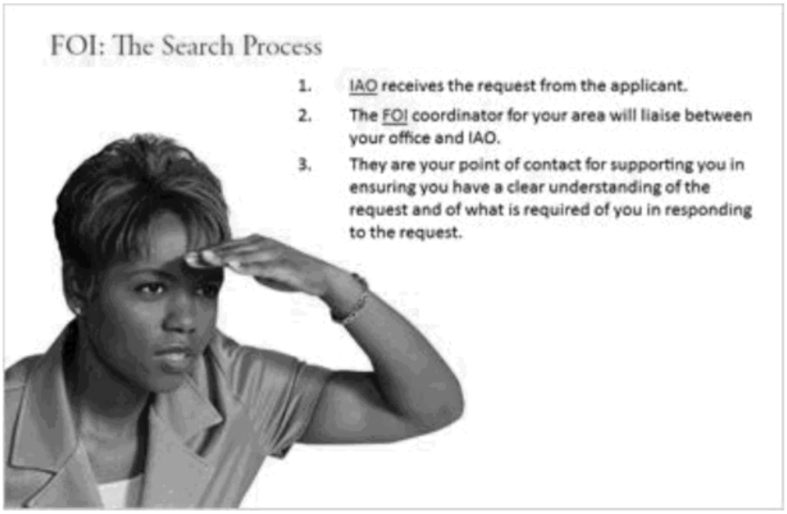
How to Fulfill My Duty to Assist

- Adequately interpret access requests as a “fair and rational person would expect” and in good faith.
- Make a solid effort to discern the intent and goal of the requester.
- At times, it is necessary to work with IAO to clarify directly with the applicant.
- Conduct thorough searches fo s, project documents and other records) and docum

IAO

Information Access Operations

4.6 FOI: The Search Process



FOI: The Search Process

1. IAO receives the request from the applicant.
2. The FOI coordinator for your area will liaise between your office and IAO.
3. They are your point of contact for supporting you in ensuring you have a clear understanding of the request and of what is required of you in responding to the request.

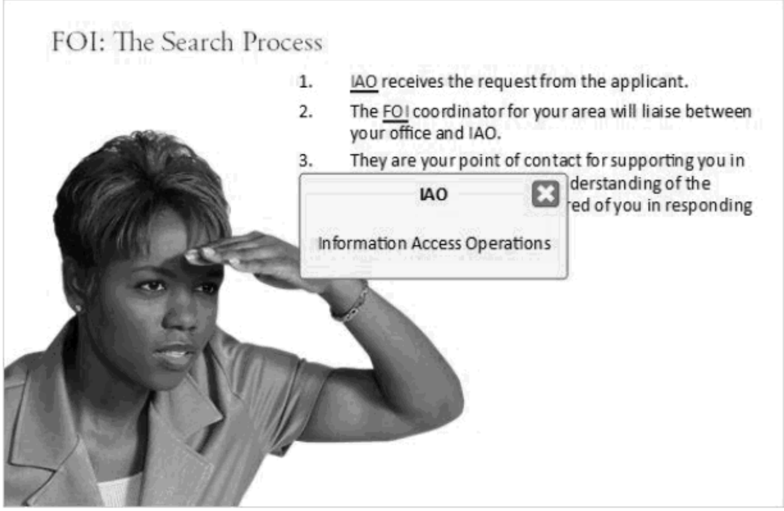
Notes:

A diligent search for records is one of the most important things you can do to assist citizens in accessing the information that interests them. You are responsible for searching anywhere you or your office has stored recorded information.

IAO receives the request from the applicant. An FOI coordinator for your area will liaise between your office and IAO. They are your point of contact for supporting you in ensuring you have a clear understanding of the request and of what is required of you in responding to the request.

It is an expectation across government that IAO be able to provide evidence that a thorough and comprehensive search has been conducted. That's why it's very important that you document the details of your efforts, as well as an explanation in the event of a no-records response.

IAO (Slide Layer)



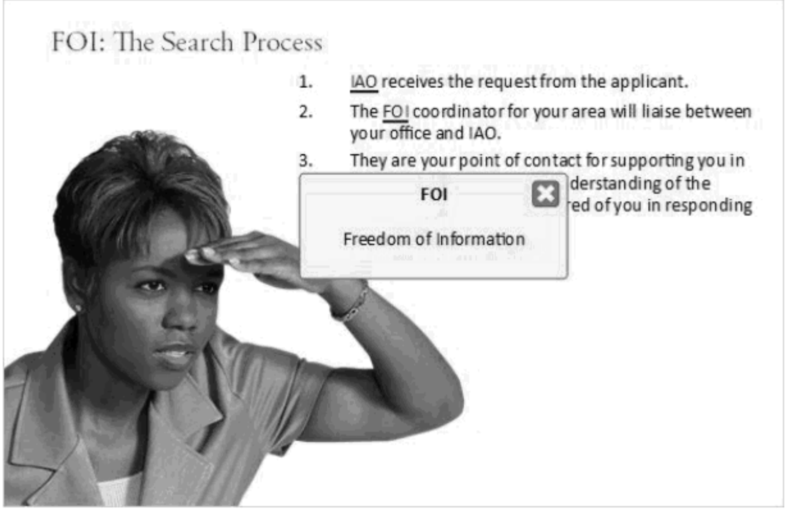
FOI: The Search Process

1. IAO receives the request from the applicant.
2. The FOI coordinator for your area will liaise between your office and IAO.
3. They are your point of contact for supporting you in … derstanding of the … red of you in responding

IAO

Information Access Operations

FOI (Slide Layer)



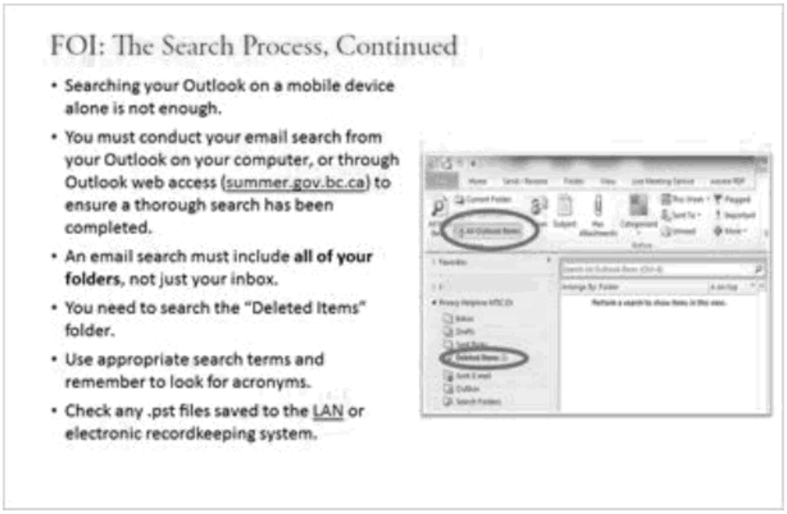
FOI: The Search Process

1. IAO receives the request from the applicant.
2. The FOI coordinator for your area will liaise between your office and IAO.
3. They are your point of contact for supporting you in … derstanding of the … red of you in responding

FOI

Freedom of Information

4.7 FOI: The Search Process, Continued



FOI: The Search Process, Continued

- Searching your Outlook on a mobile device alone is not enough.
- You must conduct your email search from your Outlook on your computer, or through Outlook web access (summer.gov.bc.ca) to ensure a thorough search has been completed.
- An email search must include **all of your folders**, not just your inbox.
- You need to search the "Deleted Items" folder.
- Use appropriate search terms and remember to look for acronyms.
- Check any .pst files saved to the LAN or electronic recordkeeping system.

Notes:

As we've already learned, emails are only one example of government records, and an adequate search for records following an FOI request requires more than just searching emails. When conducting a search, you need to look in your electronic recordkeeping system, your home drive or LAN, and your notebook, as well as in your paper files.

However, because email is so commonly used to communicate with our colleagues, it is worthwhile to spend some time now to talk about useful email search tips.
To conduct a thorough email search, you must ensure that you are searching all of Outlook - or all of your mailboxes, and not *just* your inbox. This includes your deleted and sent mail folders as well as any subfolders.

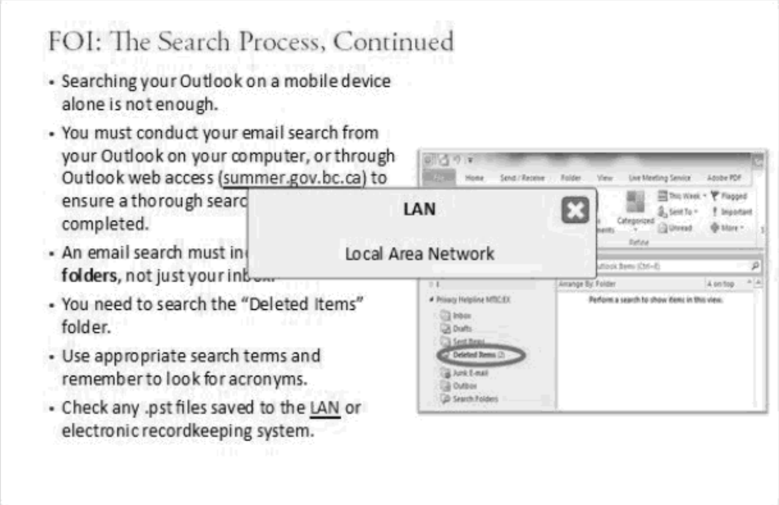
Remember to use a set of broad search terms. Don't just search using the precise wording of the applicant's request. You need to use your expertise and knowledge of your own records to find everything that may respond to a given FOI request. Don't forget to search common acronyms too!

If you have .pst files saved to your LAN or electronic recordkeeping system containing old emails, you may need to search these files as well. This is important to remember, as a search through All Mail Items will not capture these files, which could contain records responsive to a request. This also applies to individual emails you may have saved elsewhere, outside of outlook.

These tips will also help you when conducting searches in other locations - like your office recordkeeping system.

It is also important to remember when searching for records responsive to an FOI request, that even your transitory records should be included if they had not been disposed of when the FOI request was received. As mentioned previously, you are not permitted to dispose of transitory records if they are responsive to an ongoing FOI request.

LAN (Slide Layer)



FOI: The Search Process, Continued

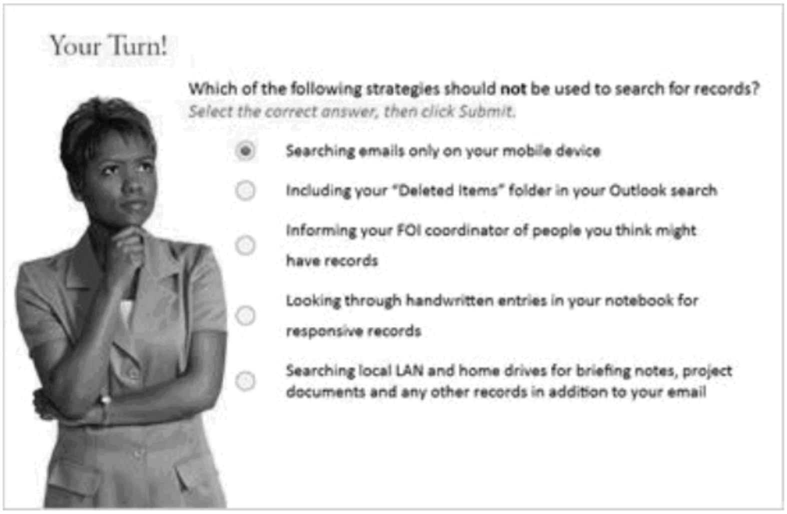
- Searching your Outlook on a mobile device alone is not enough.
- You must conduct your email search from your Outlook on your computer, or through Outlook web access (summer.gov.bc.ca) to ensure a thorough searc completed.
- An email search must in **folders**, not just your inb
- You need to search the "Deleted Items" folder.
- Use appropriate search terms and remember to look for acronyms.
- Check any .pst files saved to the LAN or electronic recordkeeping system.

LAN

Local Area Network

4.8 Your Turn!

(Multiple Choice, 10 points, 1 attempt permitted)



Your Turn!

Which of the following strategies should **not** be used to search for records?

Select the correct answer, then click Submit.

● Searching emails only on your mobile device

○ Including your "Deleted Items" folder in your Outlook search

○ Informing your FOI coordinator of people you think might have records

○ Looking through handwritten entries in your notebook for responsive records

○ Searching local LAN and home drives for briefing notes, project documents and any other records in addition to your email

Correct	Choice
X	Searching emails only on your mobile device
	Including your “Deleted Items” folder in your Outlook search
	Informing your FOI coordinator of people you think might have records
	Looking through handwritten entries in your notebook for responsive records
	Searching local LAN and home drives for briefing notes, project documents and any other records in addition to your email

Feedback when correct:

Correct! You have not carried out a complete search if it was only conducted on your mobile device as it will not return a full and complete list of entries to your query.

Including your “Deleted Items” folder in your Outlook search, searching local LAN and home drives in addition to your email, informing your FOI coordinator of people you think might have records, and looking through handwritten entries in your notebook for responsive records are all examples of strategies you should be following when searching for records.

Feedback when incorrect:

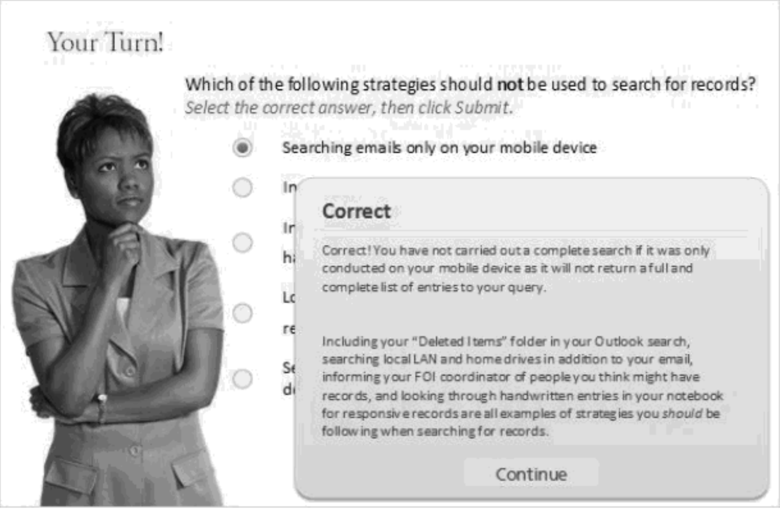
Incorrect. You have not carried out a complete search if it was only conducted on your mobile device as it will not return a full and complete list of entries to your query.

Including your “Deleted Items” folder in your Outlook search, searching local LAN and home drives in addition to your email, informing your FOI coordinator of people you think might have records, and looking through handwritten entries in your notebook for responsive records are all examples of strategies you should be following when searching for records.

Notes:

You’re up! Complete this knowledge check before we move on to the next section.

Correct (Slide Layer)



Your Turn!

Which of the following strategies should **not** be used to search for records?
Select the correct answer, then click Submit.

● Searching emails only on your mobile device

○ In

○ In
ha

○ Lo
re

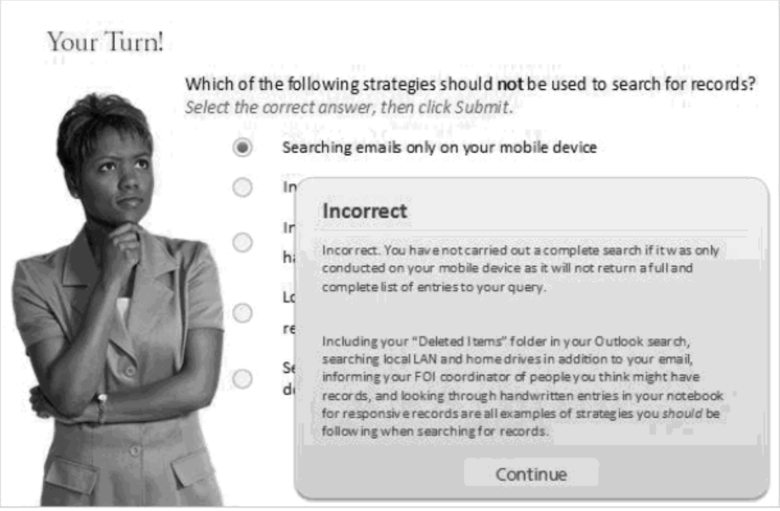
○ Se
de

Correct

Correct! You have not carried out a complete search if it was only conducted on your mobile device as it will not return a full and complete list of entries to your query.

Including your “Deleted Items” folder in your Outlook search, searching local LAN and home drives in addition to your email, informing your FOI coordinator of people you think might have records, and looking through handwritten entries in your notebook for responsive records are all examples of strategies you *should* be following when searching for records.

Incorrect (Slide Layer)



Your Turn!

Which of the following strategies should **not** be used to search for records?
Select the correct answer, then click Submit.

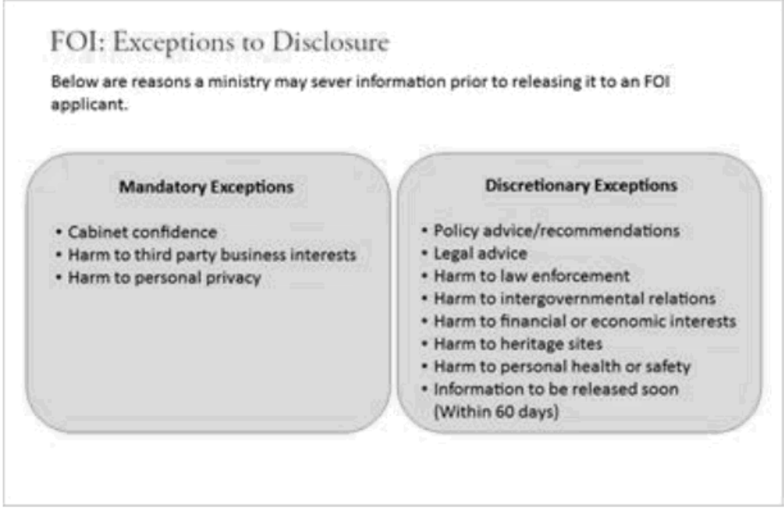
- ● Searching emails only on your mobile device
- ○ In
- ○ In
ha
- ○ Lo
re
- ○ Se
de

Incorrect

Incorrect. You have not carried out a complete search if it was only conducted on your mobile device as it will not return a full and complete list of entries to your query.

Including your "Deleted Items" folder in your Outlook search, searching local LAN and home drives in addition to your email, informing your FOI coordinator of people you think might have records, and looking through handwritten entries in your notebook for responsive records are all examples of strategies you *should* be following when searching for records.

4.9 FOI: Exceptions to Disclosure



FOI: Exceptions to Disclosure

Below are reasons a ministry may sever information prior to releasing it to an FOI applicant.

Mandatory Exceptions

- Cabinet confidence
- Harm to third party business interests
- Harm to personal privacy

Discretionary Exceptions

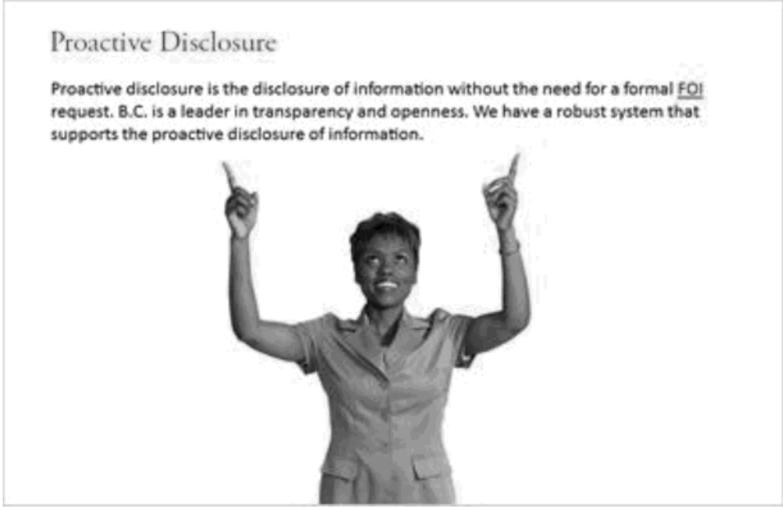
- Policy advice/recommendations
- Legal advice
- Harm to law enforcement
- Harm to intergovernmental relations
- Harm to financial or economic interests
- Harm to heritage sites
- Harm to personal health or safety
- Information to be released soon (Within 60 days)

Notes:

There are reasons that a ministry can take out - or in other words, "sever" - information from a record prior to releasing it to an applicant. You do not need to be an expert on what can be severed, though; Information Access Operations' FOI Analysts do that work for you.

Our default position is always to release information to an applicant. In other words, the question shouldn't be "*Can* we withhold this information?" but instead, “*Should* we?” or “Do we really need to?” Ultimately, this is a recommendation that will come from working with the experts at IAO, and it is a decision that will be made by the Deputy Minister. The Deputy Minister will rely on your advice and expertise about what can be shared without risking harm to government or another individual.

4.10 Proactive Disclosure



Proactive Disclosure

Proactive disclosure is the disclosure of information without the need for a formal FOI request. B.C. is a leader in transparency and openness. We have a robust system that supports the proactive disclosure of information.

Notes:

Proactive disclosure is the disclosure of information without the need for a formal FOI request. You may have also heard this referred to as “routine release”.

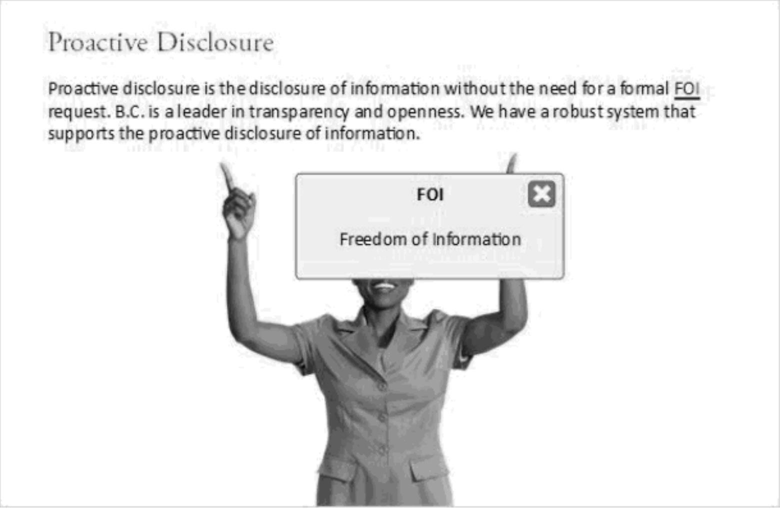
There are lots of examples of proactively disclosed information. The BC Data catalogue, for instance, contains thousands of high-quality datasets.

One way that we make information available without an FOI request is through a Minister establishing, for their ministry, a whole category of recorded information that can be disclosed.

In addition, the Minister responsible for FOIPPA may issue corporate directives that require the regular release of various types of cross-government information. For example, directives are in place requiring the disclosure of ministerial travel expenses, calendars and summaries of directly awarded contracts.

Other disclosures are more casual - you might give the general public non-personal and non-sensitive information over the phone, or via your website. Not all disclosures are repeatable -- and that's okay. Sometimes a disclosure is a one-off.

FOI (Slide Layer)



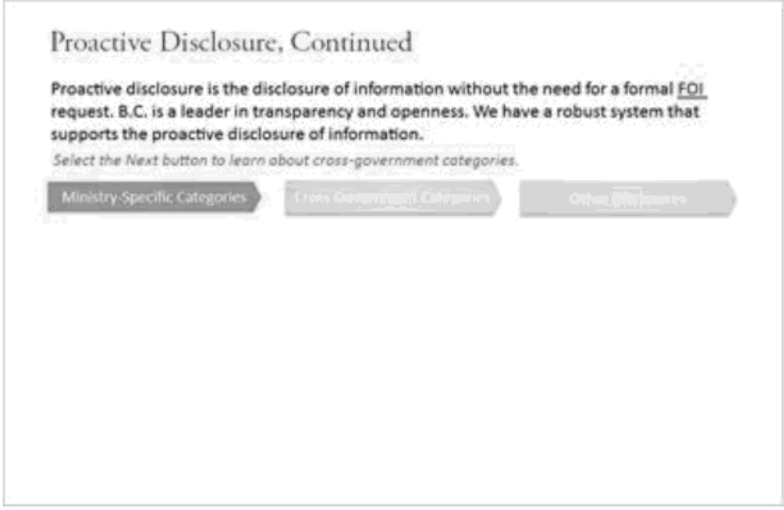
Proactive Disclosure

Proactive disclosure is the disclosure of information without the need for a formal FOI request. B.C. is a leader in transparency and openness. We have a robust system that supports the proactive disclosure of information.

FOI

Freedom of Information

4.11 Proactive Disclosure, Continued



Proactive Disclosure, Continued

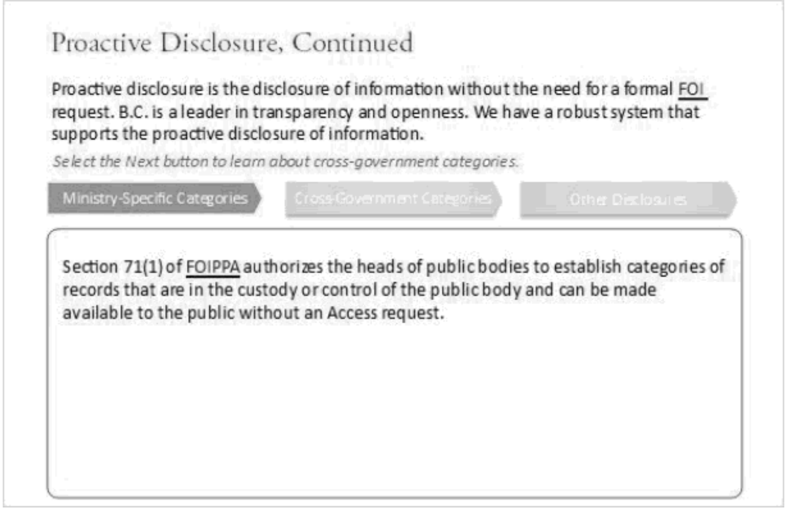
Proactive disclosure is the disclosure of information without the need for a formal FOI request. B.C. is a leader in transparency and openness. We have a robust system that supports the proactive disclosure of information.

Select the Next button to learn about cross-government categories.

Notes:

As a government, we disclose many different kinds of information outside of FOI. If it makes sense to consistently replicate a disclosure, your area should consider formalizing the disclosure by establishing it under FOIPPA as a category of information available without a request. If you see a potential opportunity, bring it to your manager and ask to work with your Ministry Privacy Officer to ensure the appropriate risk assessments are carried out.

Ministry (Slide Layer)



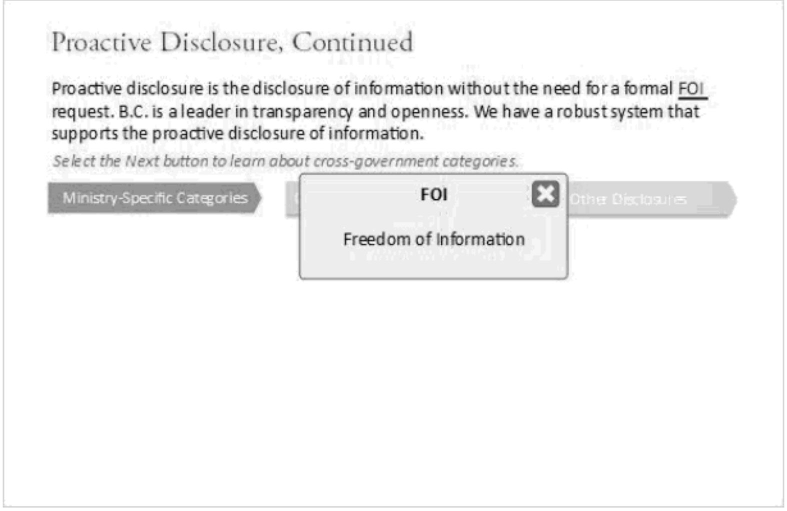
Proactive Disclosure, Continued

Proactive disclosure is the disclosure of information without the need for a formal FOI request. B.C. is a leader in transparency and openness. We have a robust system that supports the proactive disclosure of information.

Select the Next button to learn about cross-government categories.

Section 71(1) of FOIPPA authorizes the heads of public bodies to establish categories of records that are in the custody or control of the public body and can be made available to the public without an Access request.

FOI (Slide Layer)



Proactive Disclosure, Continued

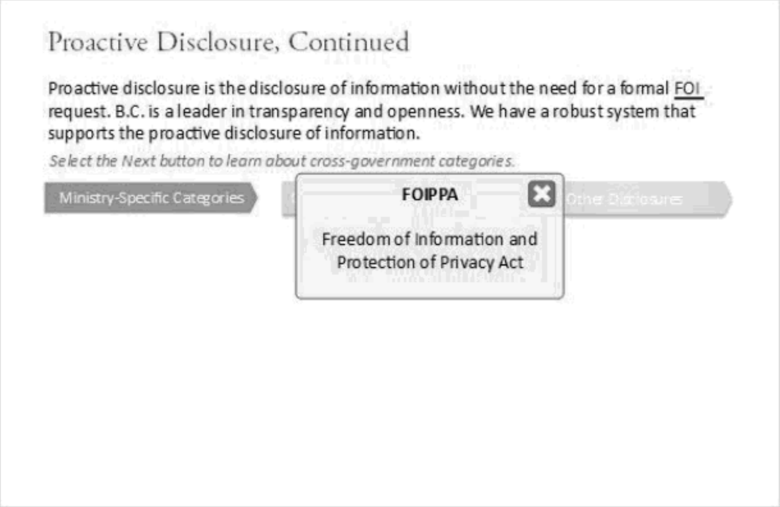
Proactive disclosure is the disclosure of information without the need for a formal FOI request. B.C. is a leader in transparency and openness. We have a robust system that supports the proactive disclosure of information.

Select the Next button to learn about cross-government categories.

FOI

Freedom of Information

FOIPPA (Slide Layer)



Proactive Disclosure, Continued

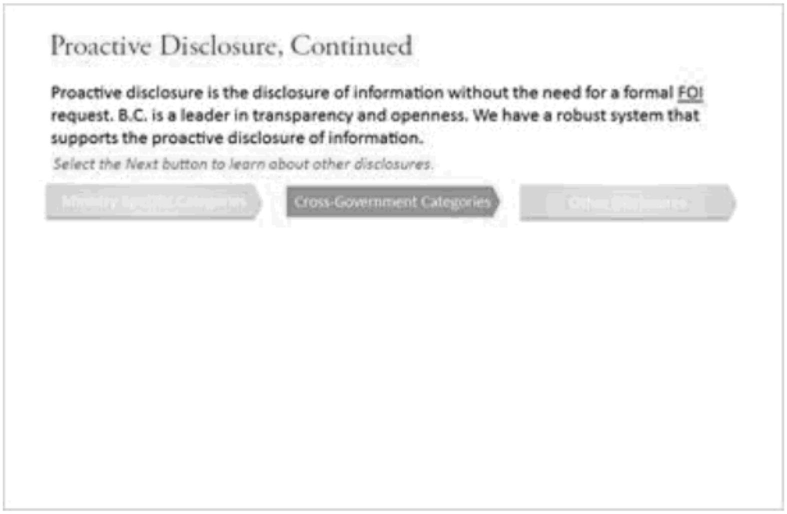
Proactive disclosure is the disclosure of information without the need for a formal FOI request. B.C. is a leader in transparency and openness. We have a robust system that supports the proactive disclosure of information.

Select the Next button to learn about cross-government categories.

FOIPPA

Freedom of Information and Protection of Privacy Act

4.12 Proactive Disclosure, Continued



Proactive Disclosure, Continued

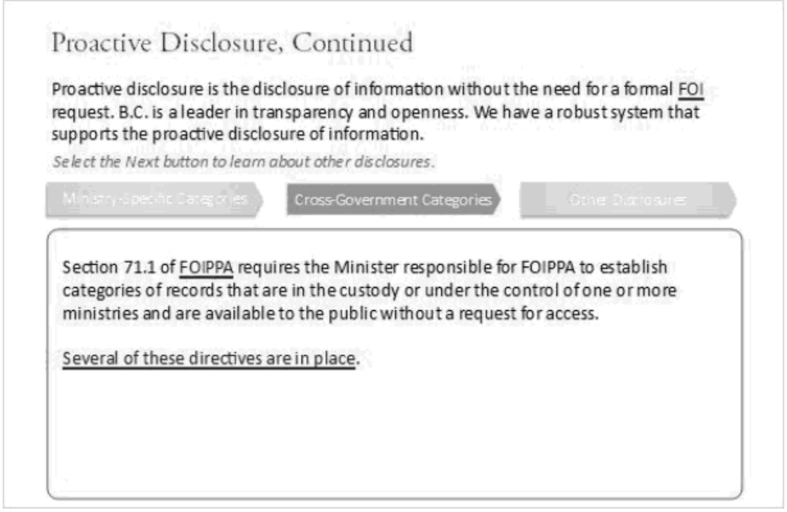
Proactive disclosure is the disclosure of information without the need for a formal FOI request. B.C. is a leader in transparency and openness. We have a robust system that supports the proactive disclosure of information.

Select the Next button to learn about other disclosures.

Notes:

If the category of information you have in mind crosses multiple ministries, it might be a good opportunity for the Minister responsible for FOIPPA to issue a corporate directive. These can be proposed to staff in the Corporate Information and Records Management Office’s Strategic Policy and Projects Branch. They will work with you and other stakeholders to design a balanced approach. A good first step is to contact your supervisor who can engage your Ministry Privacy Officer to start this process.

Cross-Government (Slide Layer)



Proactive Disclosure, Continued

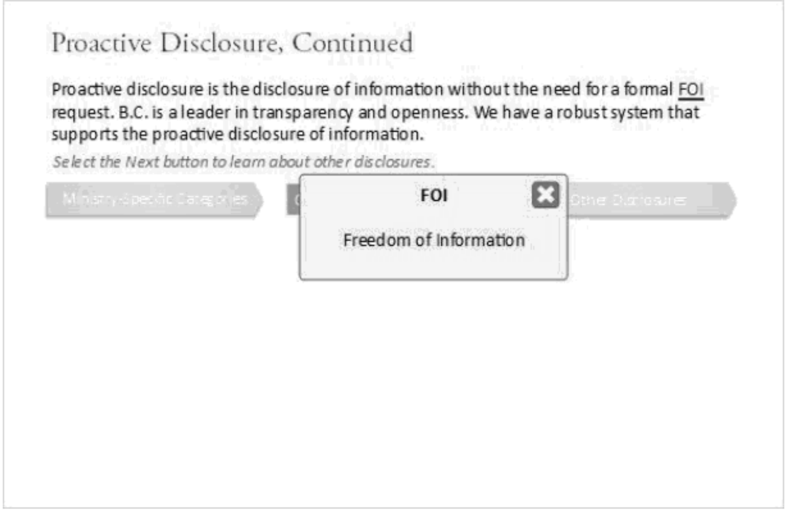
Proactive disclosure is the disclosure of information without the need for a formal FOI request. B.C. is a leader in transparency and openness. We have a robust system that supports the proactive disclosure of information.

Select the Next button to learn about other disclosures.

Section 71.1 of FOIPPA requires the Minister responsible for FOIPPA to establish categories of records that are in the custody or under the control of one or more ministries and are available to the public without a request for access.

Several of these directives are in place.

FOI (Slide Layer)



Proactive Disclosure, Continued

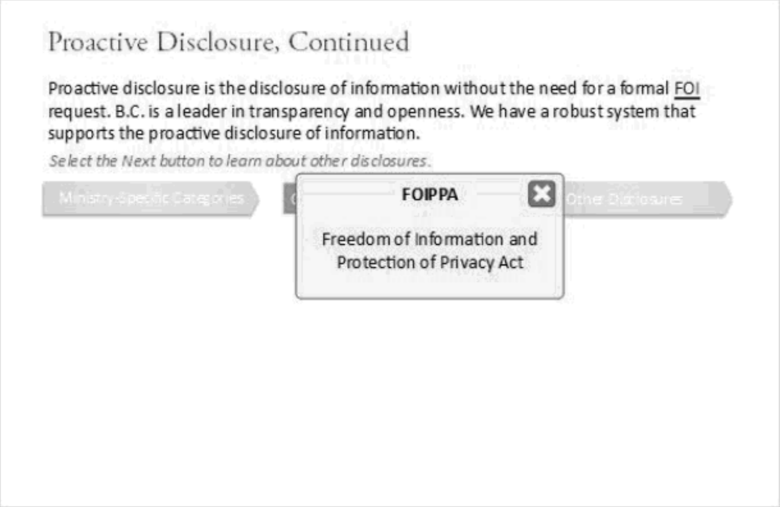
Proactive disclosure is the disclosure of information without the need for a formal FOI request. B.C. is a leader in transparency and openness. We have a robust system that supports the proactive disclosure of information.

Select the Next button to learn about other disclosures.

FOI

Freedom of Information

FOIPPA (Slide Layer)



Proactive Disclosure, Continued

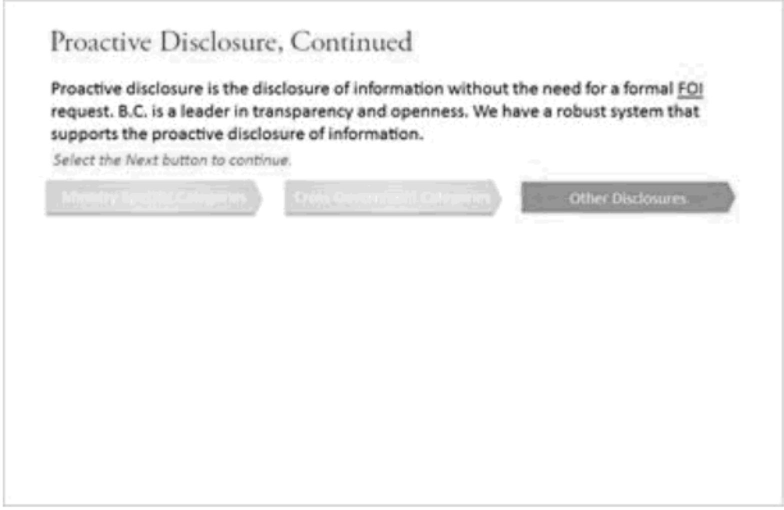
Proactive disclosure is the disclosure of information without the need for a formal FOI request. B.C. is a leader in transparency and openness. We have a robust system that supports the proactive disclosure of information.

Select the Next button to learn about other disclosures.

FOIPPA

Freedom of Information and Protection of Privacy Act

4.13 Proactive Disclosure, Continued



Proactive Disclosure, Continued

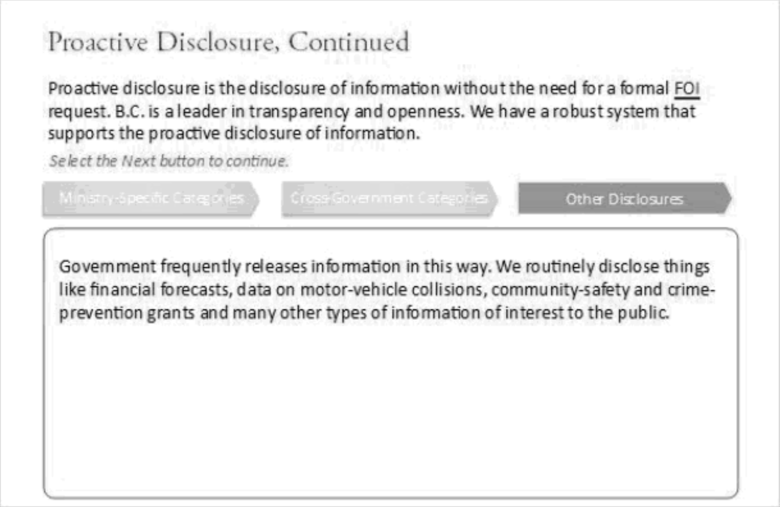
Proactive disclosure is the disclosure of information without the need for a formal FOI request. B.C. is a leader in transparency and openness. We have a robust system that supports the proactive disclosure of information.

Select the Next button to continue.

Notes:

Any information a ministry makes available on its website, or when citizens call a hotline or come to a service counter is a proactive disclosure. Each time we do this, we contribute to citizens receiving the information they're interested in, more efficiently.

Other (Slide Layer)



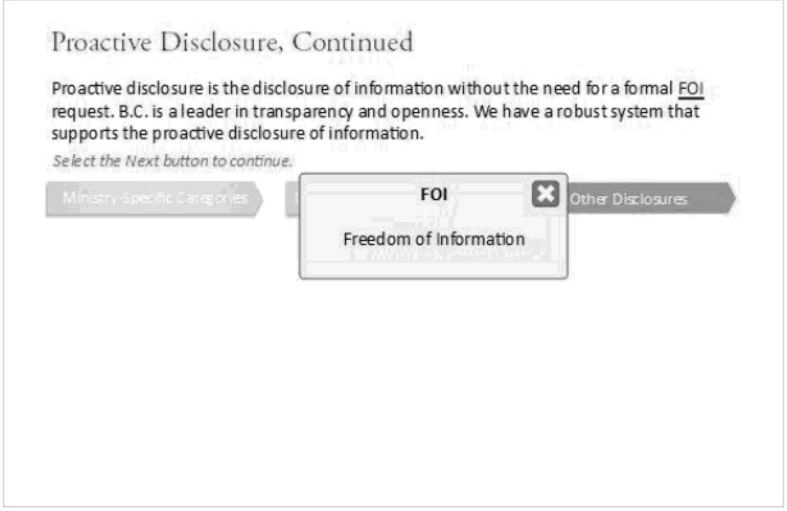
Proactive Disclosure, Continued

Proactive disclosure is the disclosure of information without the need for a formal FOI request. B.C. is a leader in transparency and openness. We have a robust system that supports the proactive disclosure of information.

Select the Next button to continue.

Government frequently releases information in this way. We routinely disclose things like financial forecasts, data on motor-vehicle collisions, community-safety and crime-prevention grants and many other types of information of interest to the public.

FOI (Slide Layer)



Proactive Disclosure, Continued

Proactive disclosure is the disclosure of information without the need for a formal FOI request. B.C. is a leader in transparency and openness. We have a robust system that supports the proactive disclosure of information.

Select the Next button to continue.

FOI

Freedom of Information

5. Managing Sensitive and Personal Information

5.1 Personal Information

Personal Information

Information about an identifiable individual other than their business contact information.

Notes:

Personal information is recorded information about an identifiable individual other than their business contact information. Personal information therefore includes things like someone's home address, voting habits, and DNA. It also includes their educational history, employment history, health history, and even their personal opinions.

Two common considerations in identifying personal information are the mosaic effect and context:

The mosaic effect occurs when non-personal pieces of information, which are normally harmless, are grouped in a way that can reveal the identity of an individual.

For example, information about what an individual's vehicle and hometown may not identify anyone if they drive a Honda Civic and are from Vancouver. However, if they drive a Rolls Royce and are from Sicamous, then it is more likely to identify them.

It is also important to realize that some information can be either personal information or business contact information, depending on the context. For instance, if someone runs a professional daycare out of their home, then their address could be both personal and business related. If that individual uses their address to order a shipment of baby supplies for the daycare, then it is business contact information, but if that same address is used to register for a home owner grant, it's personal information and should be handled accordingly.

5.2 Sensitive Information

Sensitive Information

Information that if compromised could result in serious consequences for individuals, organizations or government.

Notes:

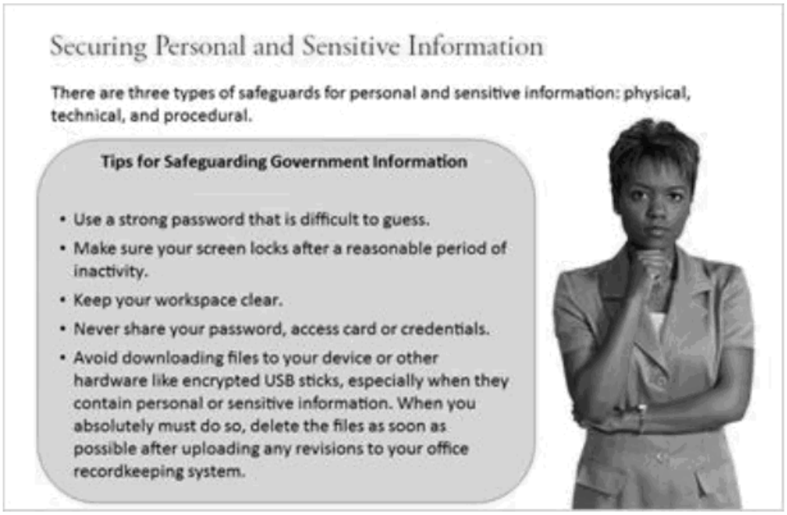
Sensitive information, though not always personal information must be treated with care and secured properly. Sensitive information is information that if compromised could result in serious consequences for individuals, organizations or government.

The significance of designating information as sensitive depends on factors such as the value of the information and the probability and impacts of unauthorized use, alteration, loss or destruction.

Examples of sensitive information can include:

- Architectural drawings of a correctional facility
- Draft legislation or policy that has not yet been passed or made public

5.3 Securing Personal and Sensitive Information



Securing Personal and Sensitive Information

There are three types of safeguards for personal and sensitive information: physical, technical, and procedural.

Tips for Safeguarding Government Information

- Use a strong password that is difficult to guess.
- Make sure your screen locks after a reasonable period of inactivity.
- Keep your workspace clear.
- Never share your password, access card or credentials.
- Avoid downloading files to your device or other hardware like encrypted USB sticks, especially when they contain personal or sensitive information. When you absolutely must do so, delete the files as soon as possible after uploading any revisions to your office recordkeeping system.

Notes:

Now let's consider best practices for securing personal or other sensitive information.

Whether you're in the office, travelling, or working from home or elsewhere, there are steps you need to take to ensure that the valuable government information you handle is protected.

You have to ensure reasonable security arrangements; this means that the steps you take are appropriate and proportional to the sensitivity of the information.

When you're handling personal information, you also need to know that, for the most part, storage and access must be within Canada. While there are limited exceptions to this rule, you must keep personal information in Canada unless you are specifically authorized by law to share the information outside of Canada.

There is a robust policy framework to support you in this, and, when you're working on a government device, or in the office, there are lots of protections built in. Your building may have a security guard, and access cards or keys are often used to restrict access to various locations - especially those locations where more sensitive information is stored. Your government-issued device, such as your smart phone, portable drive or other information technology tools, are encrypted and have their protective settings turned on.

There’s an active role for you to play, too.

Think about three aspects of security:

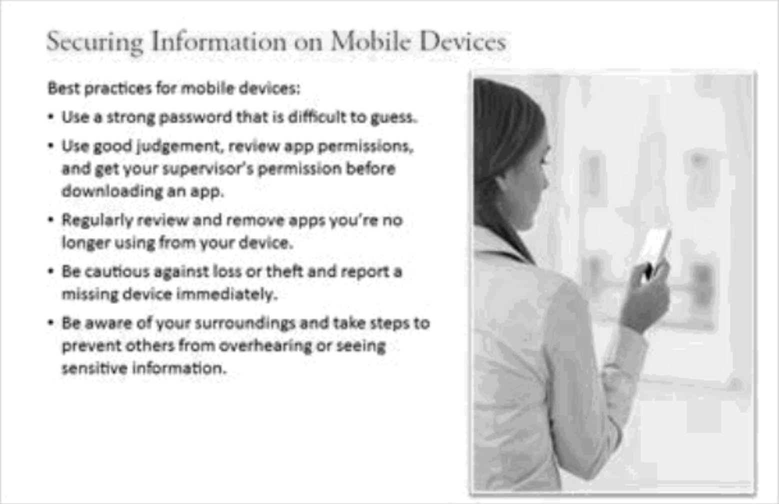
What physical security measures have you taken, what technical measures have you taken and what procedural measures have you taken?

In terms of physical security, consider locking cabinet and office doors, using privacy screens, locking your computer screen when you walk away from it, and taking measures to prevent others from overhearing or viewing sensitive information.

With respect to technical security, think about using strong passwords, not re-using passwords, downloading device updates as appropriate, and using only government-issued devices. Or, when you have to use your personal device, use VPN or DTS and access your email through Outlook Web Access.

In terms of procedural security, there are a number of things you can do: don’t leave your keys taped to the file cabinet, share your password, or let someone else use your access card. Keep your workspace clear, especially when you are away from it. When you travel with physical documents, only take what you need to do the job, and make sure you have appropriate approval to transport the material.

5.4 Securing Information on Mobile Devices



Securing Information on Mobile Devices

Best practices for mobile devices:

- Use a strong password that is difficult to guess.
- Use good judgement, review app permissions, and get your supervisor's permission before downloading an app.
- Regularly review and remove apps you're no longer using from your device.
- Be cautious against loss or theft and report a missing device immediately.
- Be aware of your surroundings and take steps to prevent others from overhearing or seeing sensitive information.

Notes:

Now let's focus on the additional measures you need to take when you're working on a mobile device.

When you're working on a mobile device like a smart phone, tablet, or laptop, there are specific things you need to do to ensure that information remains appropriately managed and secured.

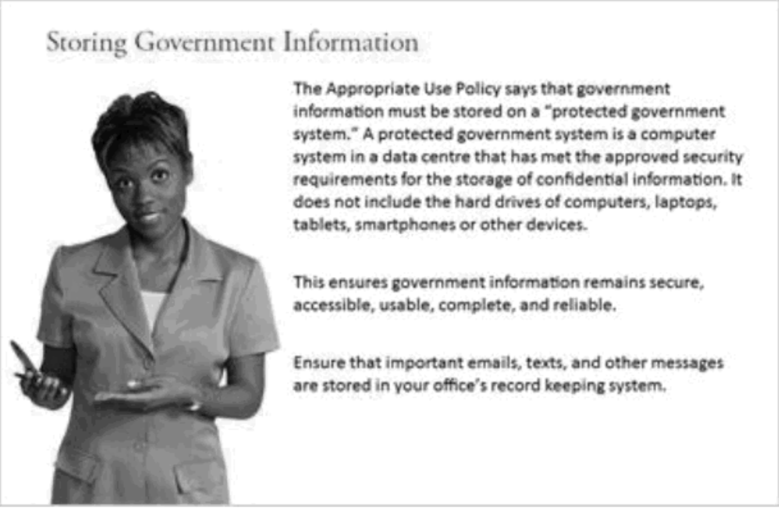
Passwords:
It's always important to choose a strong password. On smartphones and tablets in particular, you might be tempted to choose a simpler access password because there is no physical keyboard. It's important that your mobile device password be strong and difficult for someone else to guess.

Apps:
You need to be mindful of what apps you download to your government-issued mobile device. Many applications access information on your device such as your contacts and your calendar. This can be a problem if that information is personal information, which typically must be stored inside Canada. You must get your supervisor's permission before downloading an application. There's a checklist supervisors can use to assess the potential privacy or security risks of downloading a particular application. It's also a good practice to remove apps you're no longer using.

Loss:
Mobile devices are particularly vulnerable to being lost or stolen. If you must leave your device unattended outside the office, take reasonable steps to secure it, like locking it in a hotel safe. If you lose your device, you must report it right away.

Awareness:
When you are traveling or working from home, a hotel or another location outside your regular workplace, it's particularly important to take appropriate measures to prevent others from overhearing or viewing sensitive information. This can include using a privacy screen, preventing others from looking over your shoulder, or finding a private place to take a phone call.

5.5 Storing Government Information



Storing Government Information

The Appropriate Use Policy says that government information must be stored on a "protected government system." A protected government system is a computer system in a data centre that has met the approved security requirements for the storage of confidential information. It does not include the hard drives of computers, laptops, tablets, smartphones or other devices.

This ensures government information remains secure, accessible, usable, complete, and reliable.

Ensure that important emails, texts, and other messages are stored in your office's record keeping system.

Notes:

You likely use lots of different tools and technologies to do your work. Whether you have a smart phone, a tablet, a laptop or a desktop computer, you may use social media, text messaging, applications, and other platforms throughout the course of your day.

So, how do you manage all the government information you're creating or receiving across these platforms?

Government information must be stored on a “protected government system”. In general, this means information must be stored in your office’s record keeping system.

Your computer’s hard drive and mobile media such as USB sticks and portable hard drives are not appropriate places to permanently store government information.

In fact, in order to ensure that government information remains available and is complete, these kinds of media should only be used when it’s absolutely necessary. If you’re using mobile media, ensure it’s encrypted.

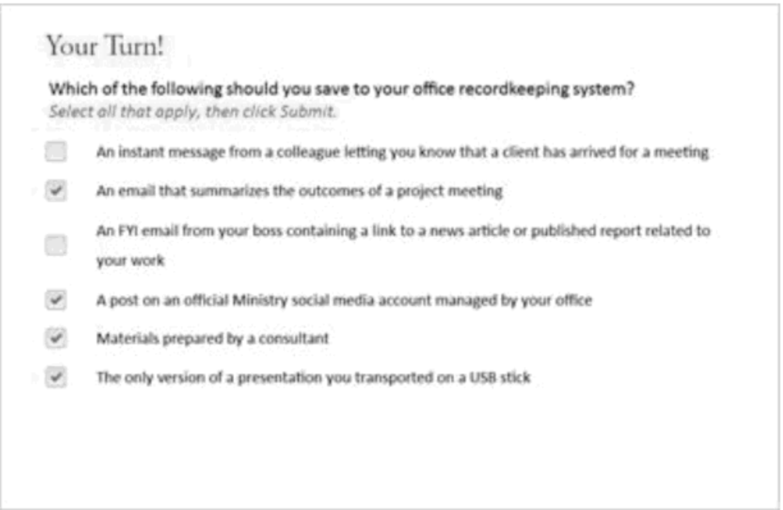
Outlook also shouldn’t be used as a permanent file storage location. Important emails should be saved in your office’s records keeping system. The same is true of texts, messages on social media, and instant messages. Whether you copy these to the LAN or TRIM, or you summarize their contents in another document, you must ensure you’re storing all important government information appropriately, regardless of its original source.

Personal email accounts should never be used to carry out government business, except in extenuating circumstances. When it is used, there are rules you need to follow. This includes copying emails to your government email address, deleting the information from your personal account as soon as you can, and ensuring you have shared the least amount of sensitive information that is necessary in the circumstance.

You must not email personal information in these circumstances unless you are specifically authorized by law to share the information outside of Canada.

5.6 Your Turn!

(Multiple Response, 10 points, 1 attempt permitted)



Your Turn!

Which of the following should you save to your office recordkeeping system?

Select all that apply, then click Submit.

- ☐ An instant message from a colleague letting you know that a client has arrived for a meeting
- ☑ An email that summarizes the outcomes of a project meeting
- ☐ An FYI email from your boss containing a link to a news article or published report related to your work
- ☑ A post on an official Ministry social media account managed by your office
- ☑ Materials prepared by a consultant
- ☑ The only version of a presentation you transported on a USB stick

Correct	Choice
	An instant message from a colleague letting you know that a client has arrived for a meeting
X	An email that summarizes the outcomes of a project meeting
	An FYI email from your boss containing a link to a news article or published report related to your work
X	A post on an official Ministry social media account managed by your office
X	Materials prepared by a consultant
X	The only version of a presentation you transported on a USB stick

Feedback when correct:

That's right!

The instant message is transitory and, because it has no ongoing value once you've seen it and responded, you can safely delete it.

Likewise, the FYI email doesn't need to be kept since the information is available elsewhere. Although you might want to save a convenience copy of the report itself, this email isn't likely to be needed to support any future decision or action.

Feedback when incorrect:

Incorrect. You did not select the correct response. Two of the examples contain transitory information:

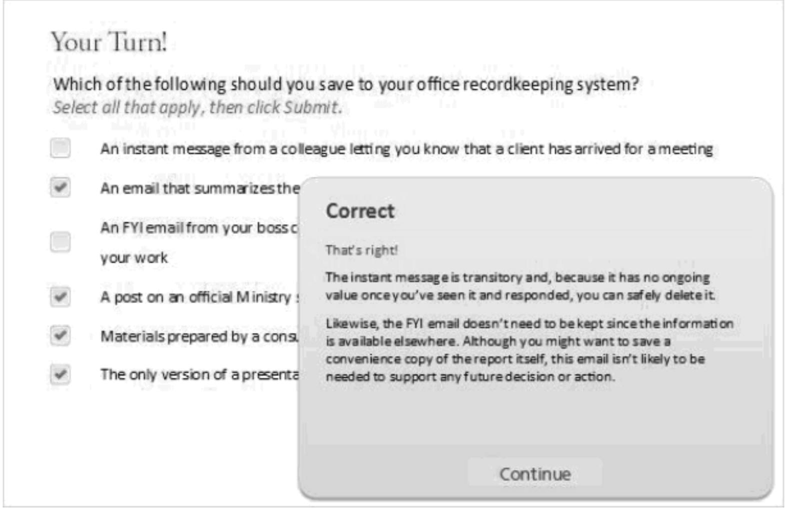
The instant message is transitory and, because it has no ongoing value once you've seen it and responded, you can safely delete it.

Likewise, the FYI email doesn't need to be kept since the information is available elsewhere. Although you might want to save a convenience copy of the report itself, this email isn't likely to be needed to support any future decision or action.

Notes:

You're up! Which of these things need to be saved to your office recordkeeping system?

Correct (Slide Layer)



Your Turn!

Which of the following should you save to your office recordkeeping system?

Select all that apply, then click Submit.

☐ An instant message from a colleague letting you know that a client has arrived for a meeting

☑ An email that summarizes the

☐ An FYI email from your boss c your work

☑ A post on an official Ministry

☑ Materials prepared by a consu

☑ The only version of a presenta

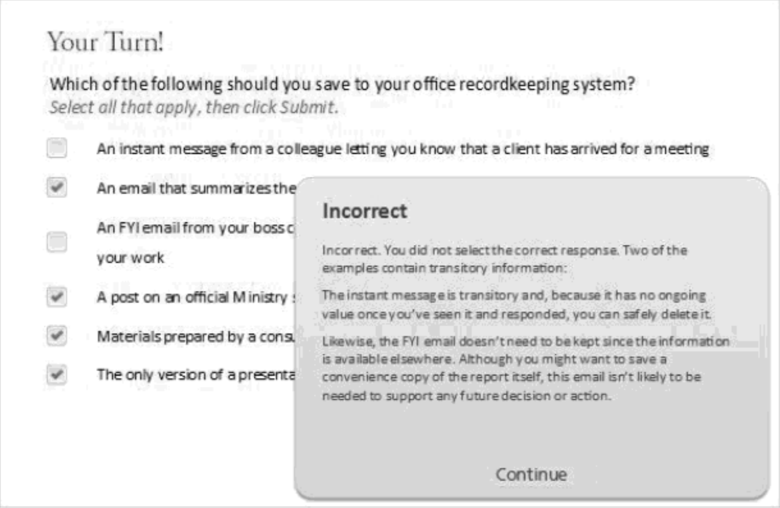
Correct

That's right!

The instant message is transitory and, because it has no ongoing value once you've seen it and responded, you can safely delete it.

Likewise, the FYI email doesn't need to be kept since the information is available elsewhere. Although you might want to save a convenience copy of the report itself, this email isn't likely to be needed to support any future decision or action.

Incorrect (Slide Layer)



Your Turn!

Which of the following should you save to your office recordkeeping system?
Select all that apply, then click Submit.

- □ An instant message from a colleague letting you know that a client has arrived for a meeting
- ☑ An email that summarizes the
- □ An FYI email from your boss c
  your work
- ☑ A post on an official Ministry :
- ☑ Materials prepared by a consu
- ☑ The only version of a presenta

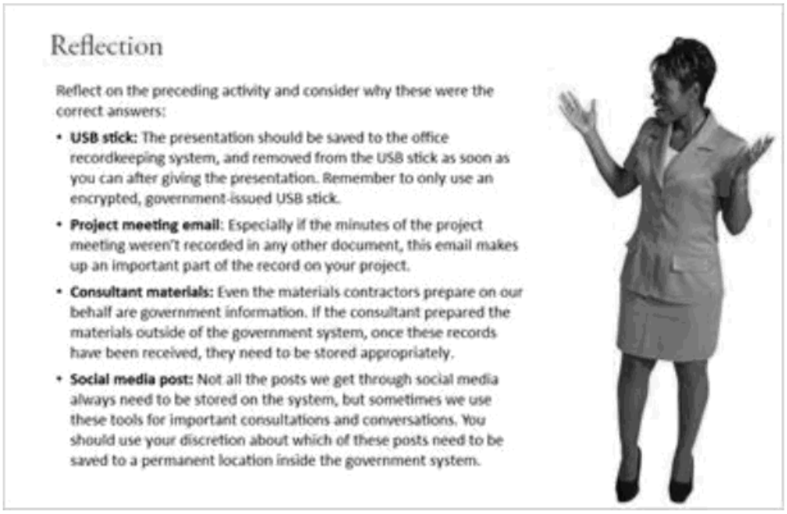
Incorrect

Incorrect. You did not select the correct response. Two of the examples contain transitory information:

The instant message is transitory and, because it has no ongoing value once you've seen it and responded, you can safely delete it.

Likewise, the FYI email doesn't need to be kept since the information is available elsewhere. Although you might want to save a convenience copy of the report itself, this email isn't likely to be needed to support any future decision or action.

5.7 Reflection



Reflection

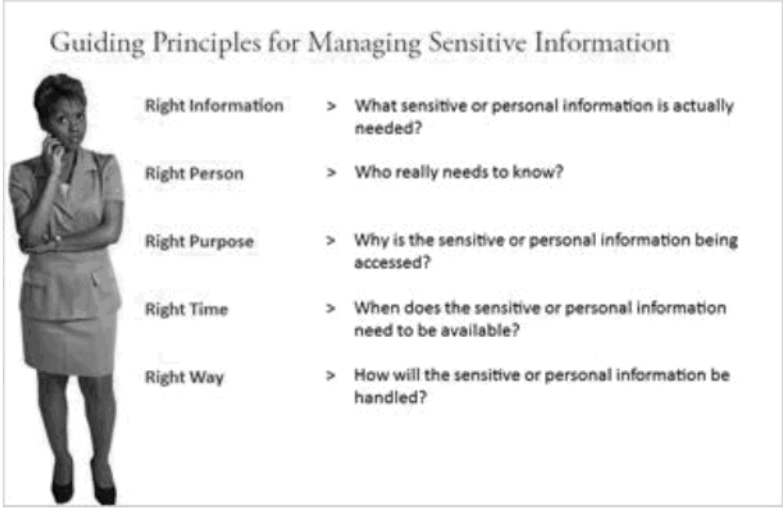
Reflect on the preceding activity and consider why these were the correct answers:

- **USB stick:** The presentation should be saved to the office recordkeeping system, and removed from the USB stick as soon as you can after giving the presentation. Remember to only use an encrypted, government-issued USB stick.
- **Project meeting email**: Especially if the minutes of the project meeting weren't recorded in any other document, this email makes up an important part of the record on your project.
- **Consultant materials:** Even the materials contractors prepare on our behalf are government information. If the consultant prepared the materials outside of the government system, once these records have been received, they need to be stored appropriately.
- **Social media post:** Not all the posts we get through social media always need to be stored on the system, but sometimes we use these tools for important consultations and conversations. You should use your discretion about which of these posts need to be saved to a permanent location inside the government system.

Notes:

Before we continue, let's take a moment to review the rationale behind the correct choices in the preceding activity.

5.8 Guiding Principles for Managing Sensitive Information



Guiding Principles for Managing Sensitive Information

Right Information	>	What sensitive or personal information is actually needed?
Right Person	>	Who really needs to know?
Right Purpose	>	Why is the sensitive or personal information being accessed?
Right Time	>	When does the sensitive or personal information need to be available?
Right Way	>	How will the sensitive or personal information be handled?

Notes:

Let's spend some time now talking about managing sensitive information, including personal information, starting with these guiding principles. Adhering to these will help you ensure you're on the right track with respect to the FOIPPA provisions and your other obligations for protecting sensitive information. These principles are not meant to discourage the appropriate sharing of information but are meant to provide guidance on the appropriate way to handle sensitive information.

Right Information:

You must always ensure that you are accessing only the personal or sensitive information you need to perform your jobs. While employees can have access to a wide range of personal and sensitive information, it is important that only that information that is required for work purposes is accessed and used.

Right Person:

It's very important to know who has access to sensitive information in your workplace. When individuals have access to sensitive information, it is important that they know how this information should be handled and who else should have access. Ask yourself "who needs to know?" It is quite possible that not everyone in your office requires access to the sensitive information you work with, so make sure it is properly secured, whether this be in a locked cabinet, or in a restricted access local area network drive.

Right Purpose:

Sensitive and personal information should only be accessed for work related purposes and certainly not for out of personal interest. The use of this personal or sensitive information should be consistent with the purpose for collecting it in the first place.

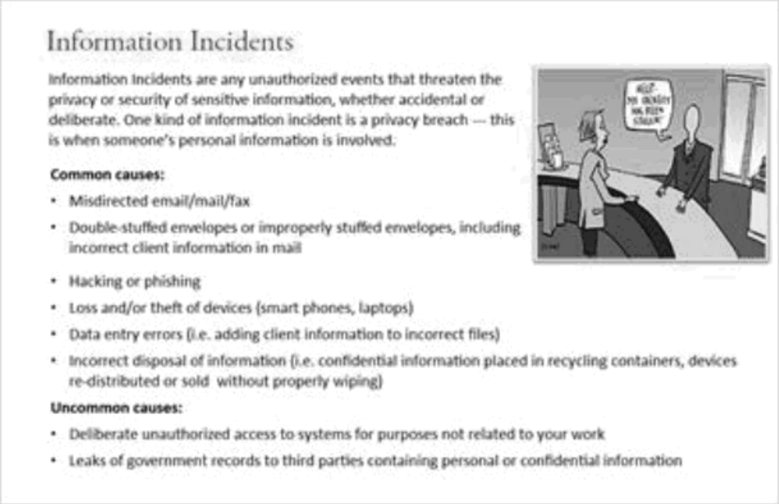
Right Time:

The sensitive information we need to do our work should only be made available when we need it to perform our duties. Access permissions should be assigned to personal and sensitive information to ensure it cannot be accessed when it is not required for work purposes. This may mean restricting access outside of working hours for example.

Right Way:

The sensitive and personal information we use in our daily work should always be handled in a way that respects and protects personal information held by government. and the confidentiality of sensitive government program information.

5.9 Information Incidents



HELP— MY IDENTITY HAS BEEN STOLEN!

Information Incidents

Information Incidents are any unauthorized events that threaten the privacy or security of sensitive information, whether accidental or deliberate. One kind of information incident is a privacy breach — this is when someone's personal information is involved.

Common causes:

- Misdirected email/mail/fax
- Double-stuffed envelopes or improperly stuffed envelopes, including incorrect client information in mail
- Hacking or phishing
- Loss and/or theft of devices (smart phones, laptops)
- Data entry errors (i.e. adding client information to incorrect files)
- Incorrect disposal of information (i.e. confidential information placed in recycling containers, devices re-distributed or sold without properly wiping)

Uncommon causes:

- Deliberate unauthorized access to systems for purposes not related to your work
- Leaks of government records to third parties containing personal or confidential information

Notes:

Information Incidents are any unauthorized events that threaten the privacy or security of sensitive information, whether accidental or deliberate.

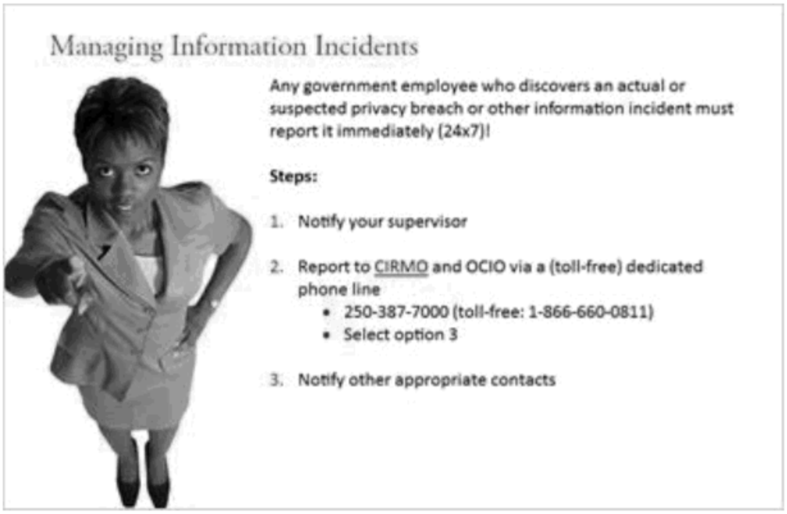
These incidents can cause financial harm to government, lead to the invasion of someone's personal privacy, or threaten the safety of an individual.

Disclosure of sensitive or personal information to unauthorized parties is just one type of incident. Others incident types include the inappropriate collection or use of sensitive or personal information. You must also be careful about how you store sensitive and personal information. At all times, you must handle the sensitive or personal information in your care appropriately.

Privacy breaches occur when there is inappropriate collection, use, disclosure, disposal or storage of, or access to personal information. Privacy breaches are one type of Information Incident. To prevent information incidents from occurring in the first place, you must think about the potential for something to go wrong and put proper safeguards in place up front.

This is what it means to be privacy and security aware.

5.10 Managing Information Incidents



Managing Information Incidents

Any government employee who discovers an actual or suspected privacy breach or other information incident must report it immediately (24x7)!

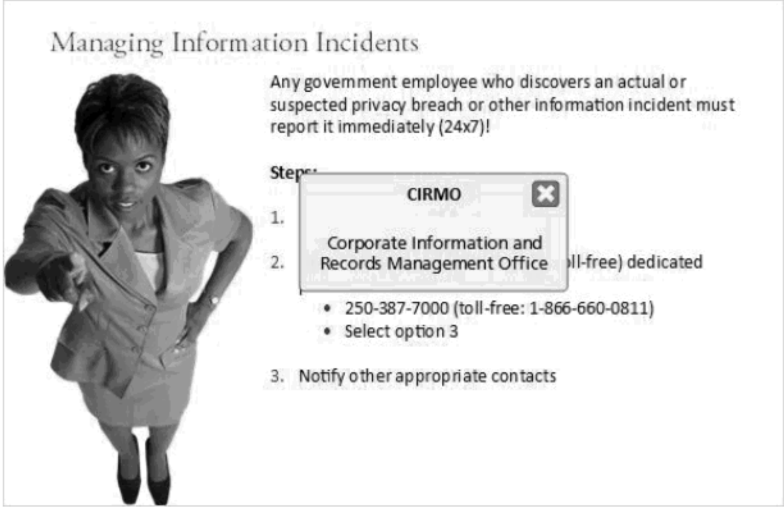
Steps:

1. Notify your supervisor
2. Report to CIRMO and OCIO via a (toll-free) dedicated phone line
   - 250-387-7000 (toll-free: 1-866-660-0811)
   - Select option 3
3. Notify other appropriate contacts

Notes:

If you discover or suspect an information incident, report it immediately. Here are the steps that must be followed in such a case. Please review them carefully.

CIRMO (Slide Layer)



Managing Information Incidents

Any government employee who discovers an actual or suspected privacy breach or other information incident must report it immediately (24x7)!

Step

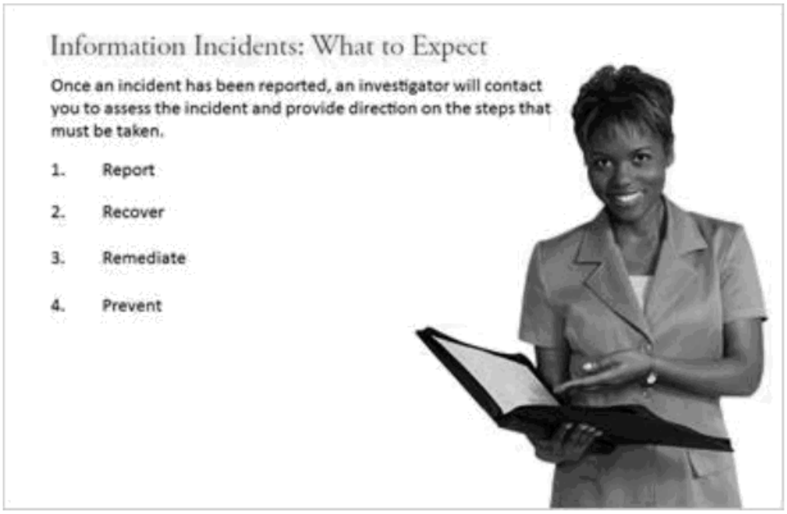
CIRMO

Corporate Information and Records Management Office

1.

2. ll-free) dedicated
   - 250-387-7000 (toll-free: 1-866-660-0811)
   - Select option 3
3. Notify other appropriate contacts

5.11 Information Incidents: What to Expect



Information Incidents: What to Expect

Once an incident has been reported, an investigator will contact you to assess the incident and provide direction on the steps that must be taken.

1. Report
2. Recover
3. Remediate
4. Prevent

Notes:

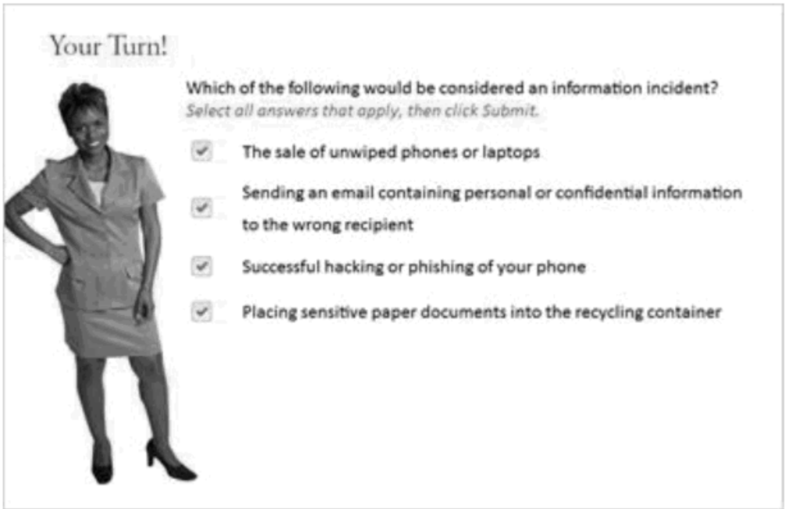
Once an information incident has been reported, an investigator will contact you to assess the incident and provide direction on the steps that must be taken.

These steps focus on:

- ensuring that the proper stakeholders are notified;
- containment of the incident, including the recovery of any information that was inappropriately disclosed;
- remediation, including determining whether notifying impacted parties is necessary; and
- strategies for preventing a future incident

5.12 Your Turn!

(Multiple Response, 10 points, 2 attempts permitted)



Your Turn!

Which of the following would be considered an information incident?

Select all answers that apply, then click Submit.

☑ The sale of unwiped phones or laptops

☑ Sending an email containing personal or confidential information to the wrong recipient

☑ Successful hacking or phishing of your phone

☑ Placing sensitive paper documents into the recycling container

Correct	Choice
X	The sale of unwiped phones or laptops
X	Sending an email containing personal or confidential information to the wrong recipient
X	Successful hacking or phishing of your phone
X	Placing sensitive paper documents into the recycling container

Feedback when correct:

Correct! All of these would be considered information incidents.

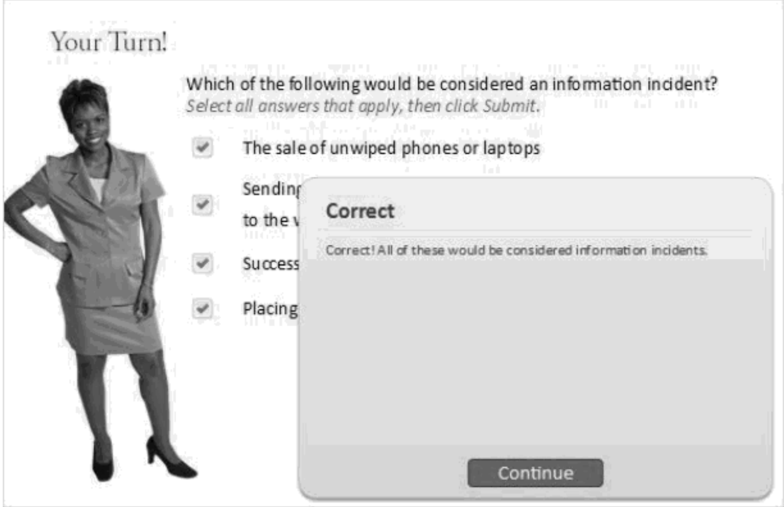
Feedback when incorrect:

Not quite. All of these would be considered information incidents.

Notes:

You're up! Which of the following would be considered an information incident?

Correct (Slide Layer)



Your Turn!

Which of the following would be considered an information incident?
Select all answers that apply, then click Submit.

☑ The sale of unwiped phones or laptops

☑ Sendin
to the v

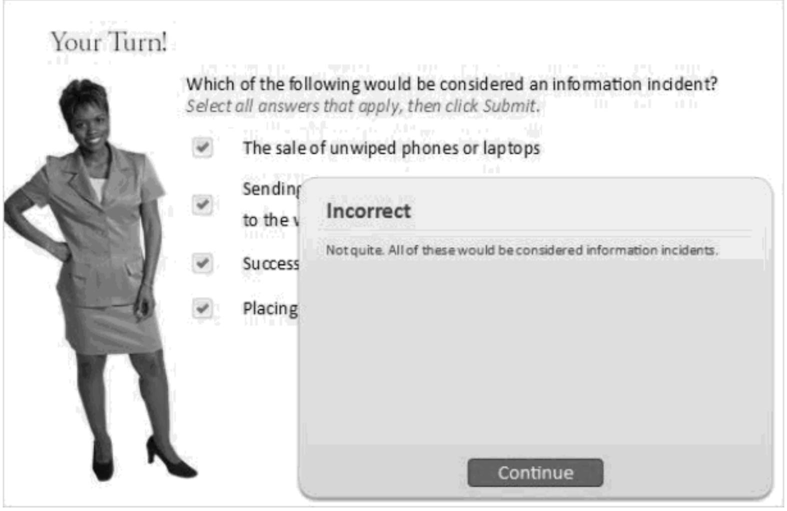
☑ Success

☑ Placing

Correct

Correct! All of these would be considered information incidents.

Incorrect (Slide Layer)



Your Turn!

Which of the following would be considered an information incident?
Select all answers that apply, then click Submit.

☑ The sale of unwiped phones or laptops

☑ Sendin
to the v

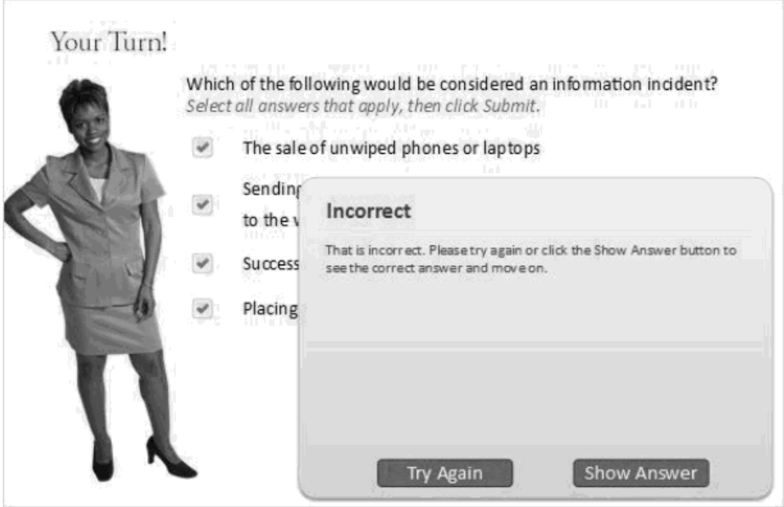
☑ Success

☑ Placing

Incorrect

Not quite. All of these would be considered information incidents.

Try Again (Slide Layer)



Your Turn!

Which of the following would be considered an information incident?
Select all answers that apply, then click Submit.

☑ The sale of unwiped phones or laptops

☑ Sendin
to the v

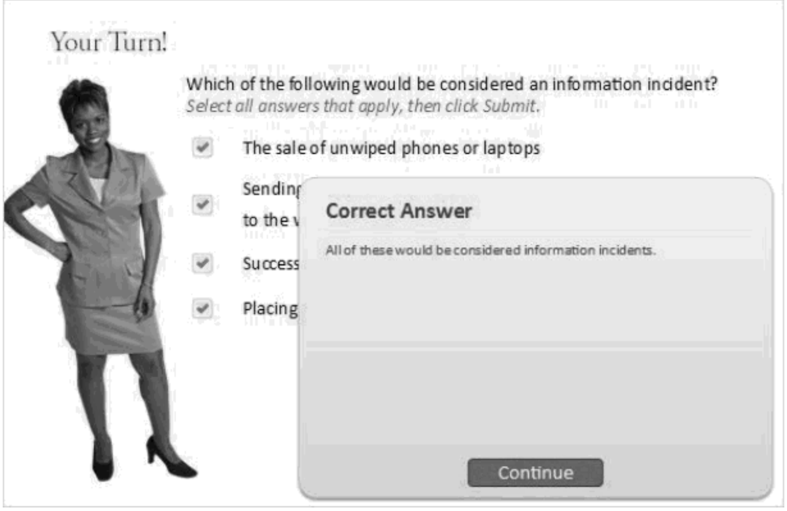
☑ Success

☑ Placing

Incorrect

That is incorrect. Please try again or click the Show Answer button to see the correct answer and move on.

Answer (Slide Layer)



Your Turn!

Which of the following would be considered an information incident?
Select all answers that apply, then click Submit.

☑ The sale of unwiped phones or laptops

☑ Sendin
to the v

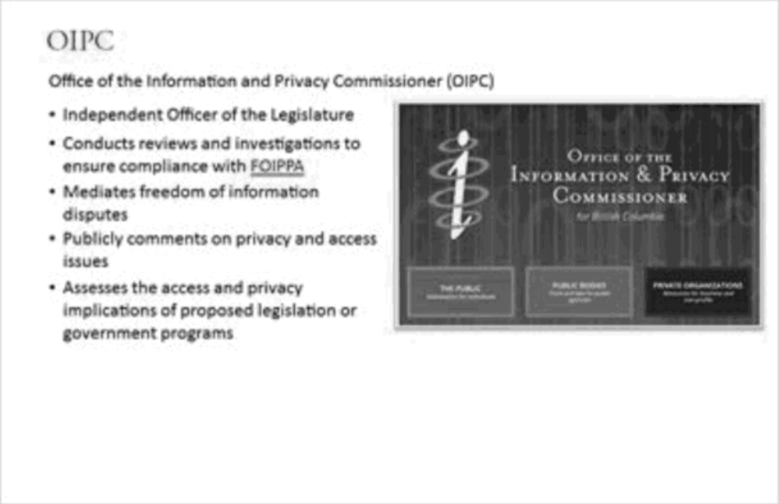
☑ Success

☑ Placing

Correct Answer

All of these would be considered information incidents.

5.13 OIPC



OIPC

Office of the Information and Privacy Commissioner (OIPC)

- Independent Officer of the Legislature
- Conducts reviews and investigations to ensure compliance with FOIPPA
- Mediates freedom of information disputes
- Publicly comments on privacy and access issues
- Assesses the access and privacy implications of proposed legislation or government programs

Notes:

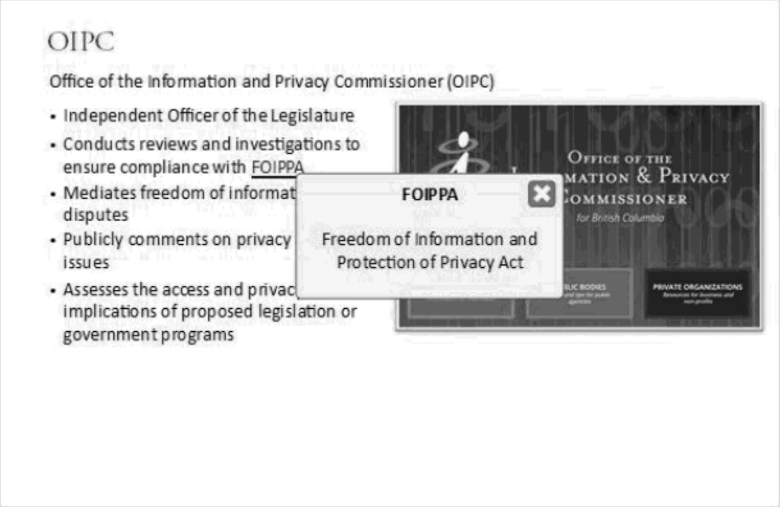
A key stakeholder in the realms privacy and FOI that you should be aware of is the Office of the Information and Privacy Commissioner.

Established in 1993, the Office of the Information and Privacy Commissioner (OIPC) provides independent oversight and enforcement of B.C.'s access and privacy laws.

Among their many responsibilities, the Office of the Information and Privacy Commissioner (OIPC): conducts reviews and investigations to ensure compliance with FOIPPA; mediates freedom of information disputes; and comments on FOI and privacy implications of proposed legislative initiatives or public body programs.

CIRMO is government's liaison with the OIPC. Whether you're dealing with a Privacy Impact Assessment or a Freedom of Information request that requires OIPC involvement, you should always contact CIRMO to initiate and manage communication with the OIPC on your behalf.

FOIPPA (Slide Layer)



OIPC

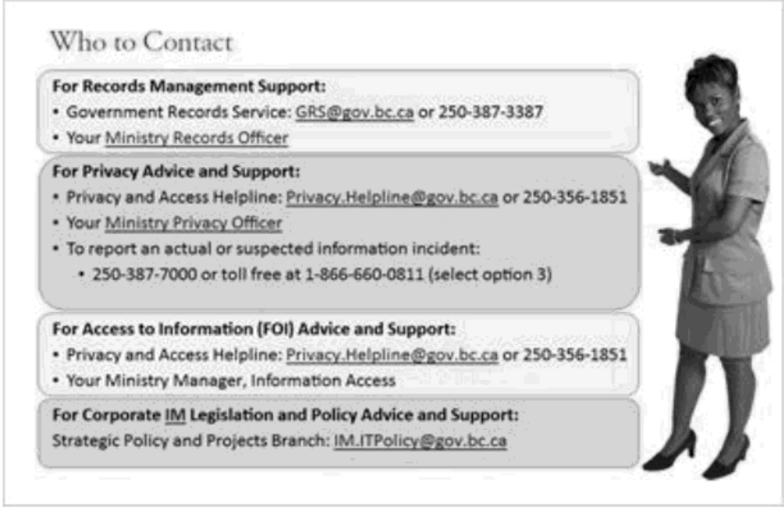
Office of the Information and Privacy Commissioner (OIPC)

- Independent Officer of the Legislature
- Conducts reviews and investigations to ensure compliance with FOIPPA
- Mediates freedom of informat
disputes
- Publicly comments on privacy
issues
- Assesses the access and privac
implications of proposed legislation or government programs

FOIPPA

Freedom of Information and Protection of Privacy Act

5.14 Who to Contact



Who to Contact

For Records Management Support:

- Government Records Service: GRS@gov.bc.ca or 250-387-3387
- Your Ministry Records Officer

For Privacy Advice and Support:

- Privacy and Access Helpline: Privacy.Helpline@gov.bc.ca or 250-356-1851
- Your Ministry Privacy Officer
- To report an actual or suspected information incident:
  - 250-387-7000 or toll free at 1-866-660-0811 (select option 3)

For Access to Information (FOI) Advice and Support:

- Privacy and Access Helpline: Privacy.Helpline@gov.bc.ca or 250-356-1851
- Your Ministry Manager, Information Access

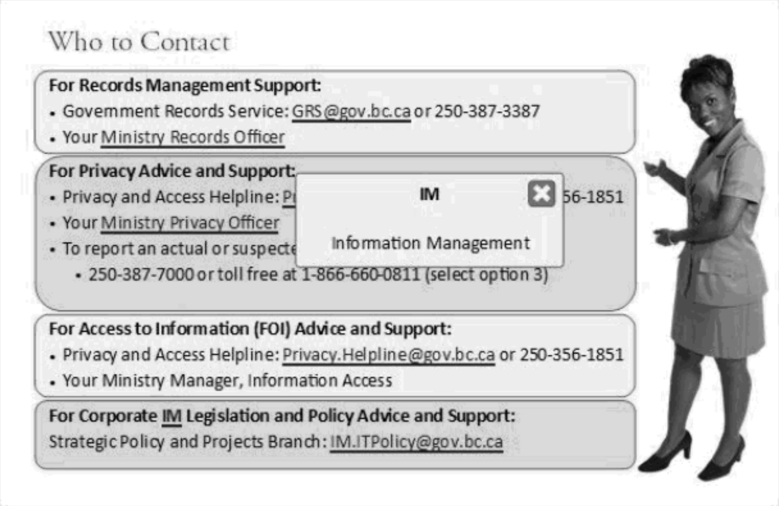
For Corporate IM Legislation and Policy Advice and Support:

Strategic Policy and Projects Branch: IM.ITPolicy@gov.bc.ca

Notes:

It is important to know that the Corporate Information and Records Management Office is here to support you in effectively managing your government information. Any questions you may have regarding records management, privacy, access to information or information management related policy or legislation can be directed to CIRMO using the relevant contact information listed on this page. You can also find this information in the resource section of this course.

IM (Slide Layer)



Who to Contact

For Records Management Support:

- Govemment Records Service: GRS@gov.bc.ca or 250-387-3387
- Your Ministry Records Officer

For Privacy Advice and Support:

- Privacy and Access Helpline: Pr 56-1851
- Your Ministry Privacy Officer
- To report an actual or suspecte
  - 250-387-7000 or toll free at 1-866-660-0811 (select option 3)

IM

Information Management

For Access to Information (FOI) Advice and Support:

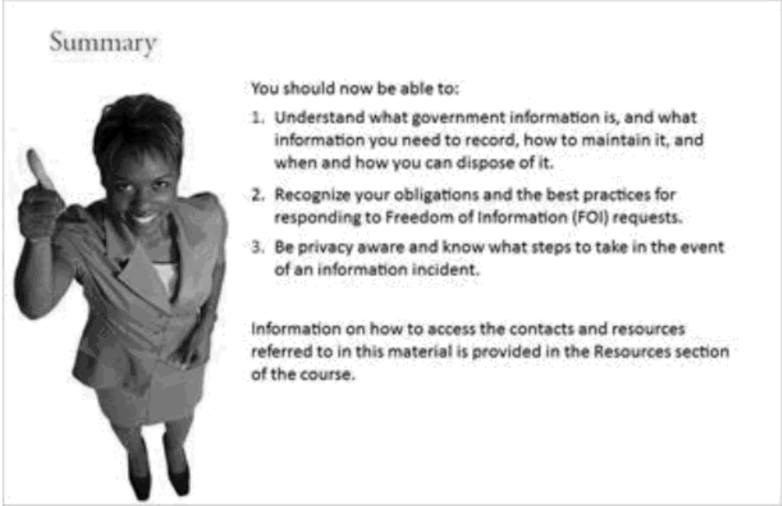
- Privacy and Access Helpline: Privacy.Helpline@gov.bc.ca or 250-356-1851
- Your Ministry Manager, Information Access

For Corporate IM Legislation and Policy Advice and Support:

Strategic Policy and Projects Branch: IM.ITPolicy@gov.bc.ca

6. Conclusion

6.1 Summary



Summary

You should now be able to:

1. Understand what government information is, and what information you need to record, how to maintain it, and when and how you can dispose of it.
2. Recognize your obligations and the best practices for responding to Freedom of Information (FOI) requests.
3. Be privacy aware and know what steps to take in the event of an information incident.

Information on how to access the contacts and resources referred to in this material is provided in the Resources section of the course.

Notes:

You should now have a better understanding of what government information is and how to manage it, including how to identify the most important information and treat it with the care it requires.

You’ve been introduced to good practices that will help you create information, and store and secure it so that it’s available for you and your colleagues to use when appropriate.

You also know what to do when you are asked to respond to an FOI request, and how to take steps to help make more information available outside of the FOI process.

You know how to identify personal information and other kinds of sensitive information, and what to do if you think these kinds of information have been inappropriately shared.

6.2 Congratulations

Click the Resources button to access links to more information.

Where ideas work

BROUGHT TO YOU BY THE
BC PUBLIC SERVICE AGENCY
YOUR ALLY *for* SUCCESS

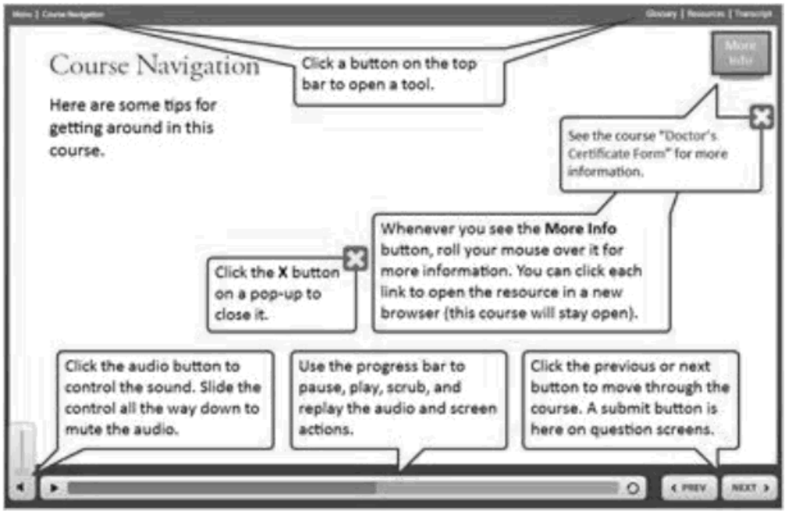
Notes:

Congratulations! You’ve completed the *Ministry of Finance -- Information Management* eLearning course!
In a world of rapid technology changes where Information Management is evolving as a discipline in the digital age, there will always be more to learn about effective Information Management. We hope that this course provides you with a start to your on-going learning.
Click the Resources button to access a link to the course content as a PDF.

Make sure to refer to the other information and courses available on MyHR when you need to.

7. Lightbox Slides

7.1 Course Navigation



Course Navigation

Here are some tips for getting around in this course.

Click a button on the top bar to open a tool.

See the course "Doctor's Certificate Form" for more information.

Whenever you see the **More Info** button, roll your mouse over it for more information. You can click each link to open the resource in a new browser (this course will stay open).

Click the **X** button on a pop-up to close it.

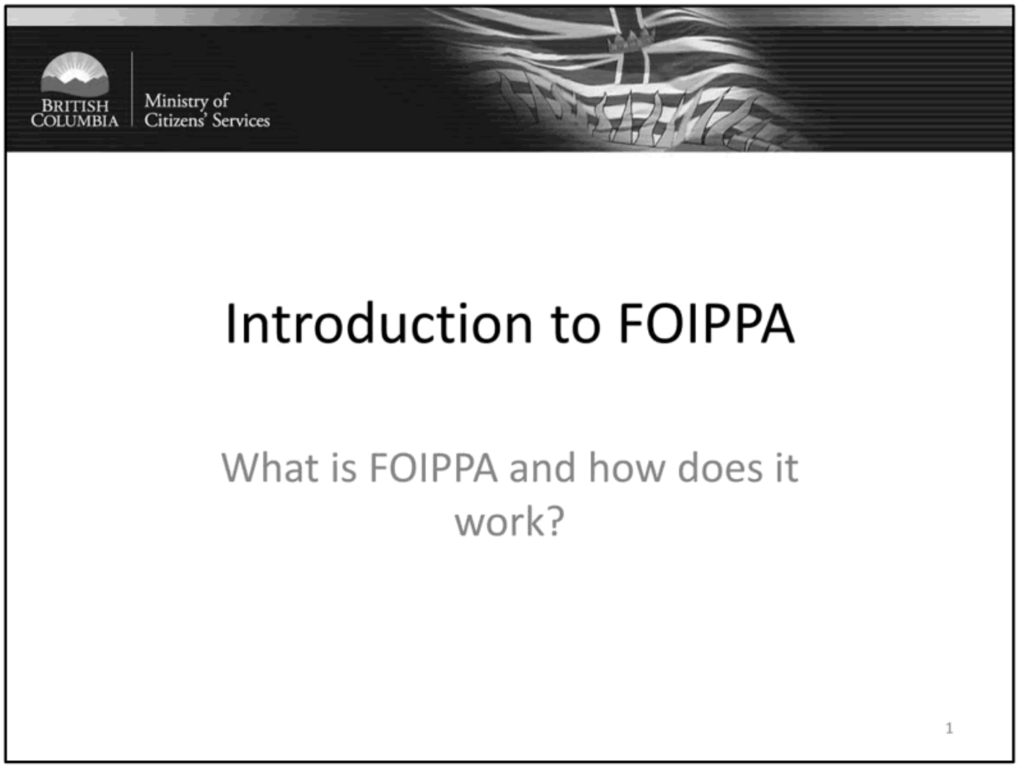
Click the audio button to control the sound. Slide the control all the way down to mute the audio.

Use the progress bar to pause, play, scrub, and replay the audio and screen actions.

Click the previous or next button to move through the course. A submit button is here on question screens.

Notes:

Here are some tips for getting around in this course.

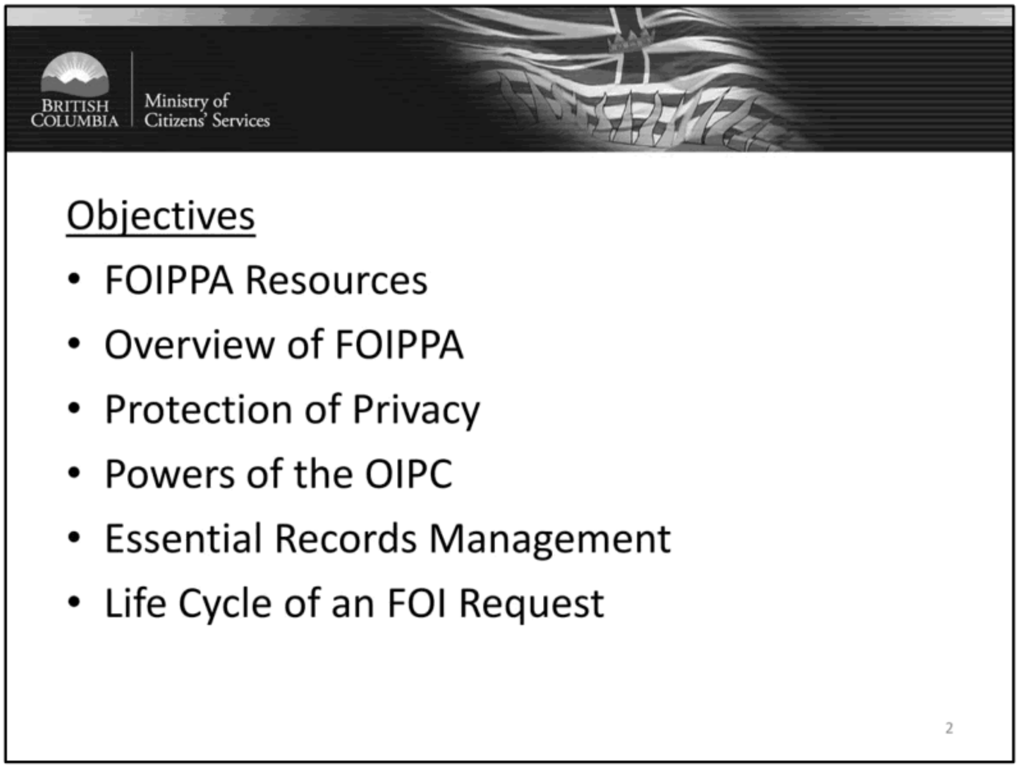


BRITISH COLUMBIA | Ministry of Citizens' Services

Introduction to FOIPPA

What is FOIPPA and how does it work?

1

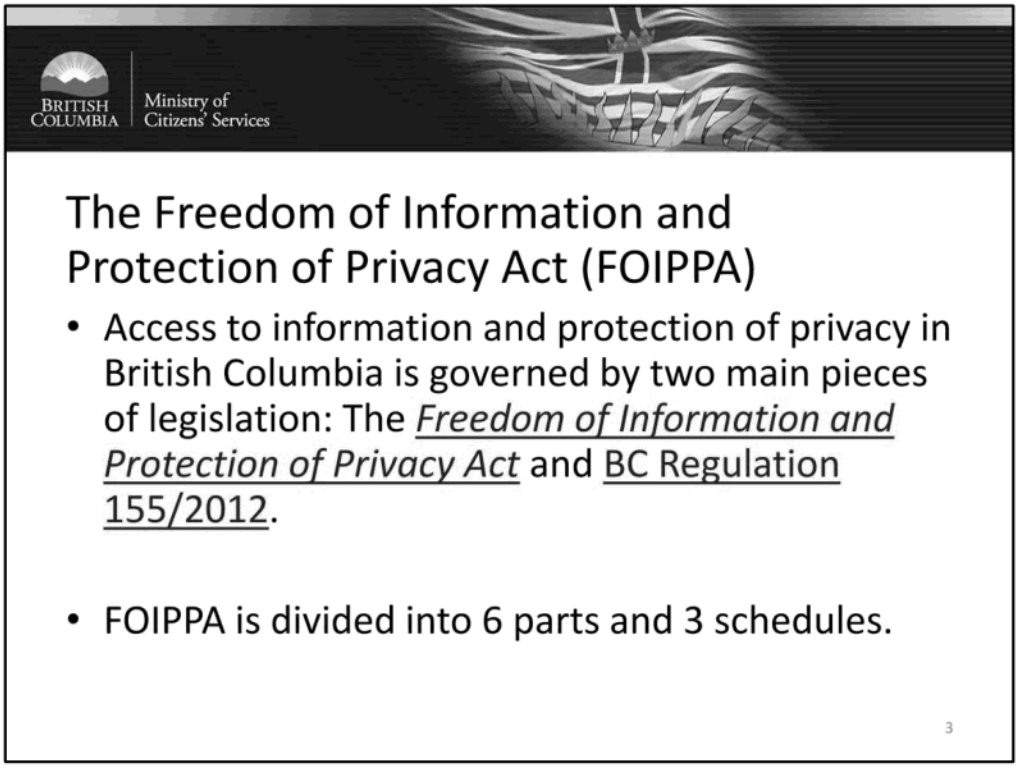


BRITISH COLUMBIA | Ministry of Citizens' Services

Objectives

- FOIPPA Resources
- Overview of FOIPPA
- Protection of Privacy
- Powers of the OIPC
- Essential Records Management
- Life Cycle of an FOI Request

2



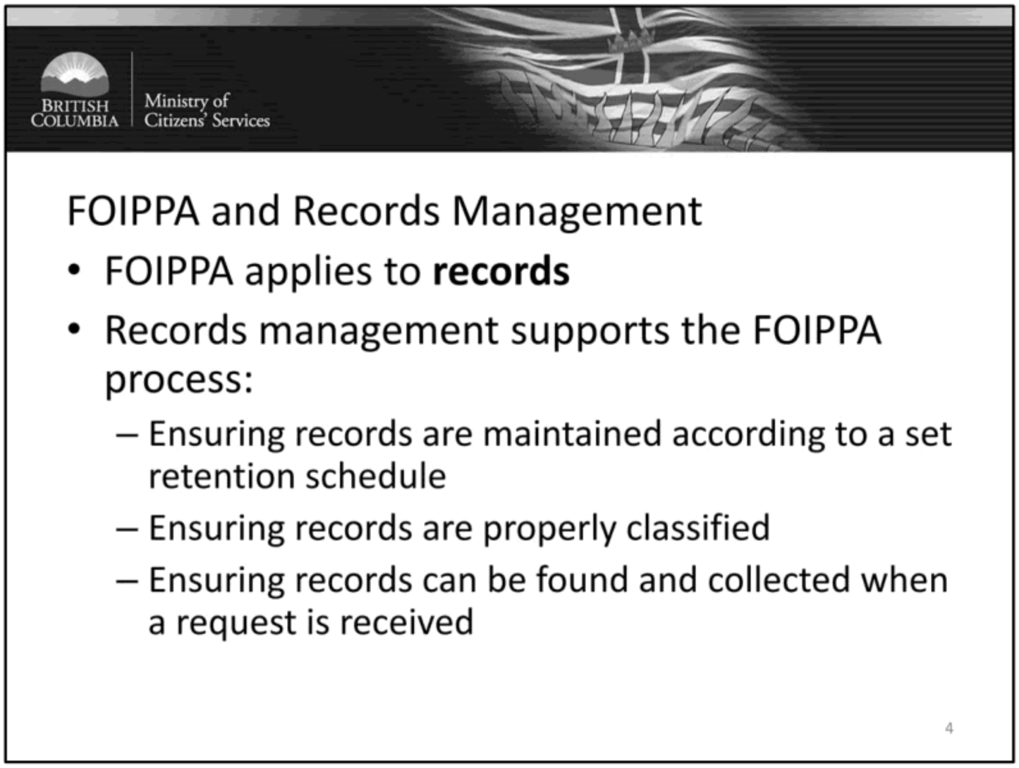
BRITISH COLUMBIA | Ministry of Citizens' Services

The Freedom of Information and Protection of Privacy Act (FOIPPA)

- Access to information and protection of privacy in British Columbia is governed by two main pieces of legislation: The *Freedom of Information and Protection of Privacy Act* and BC Regulation 155/2012.
- FOIPPA is divided into 6 parts and 3 schedules.

3

The FOI Corkboard has a link to FOIPPA, the FOIPPA Policy and Procedures Manual and the FOIPPA Regs. Read all of them. Take the time each day.

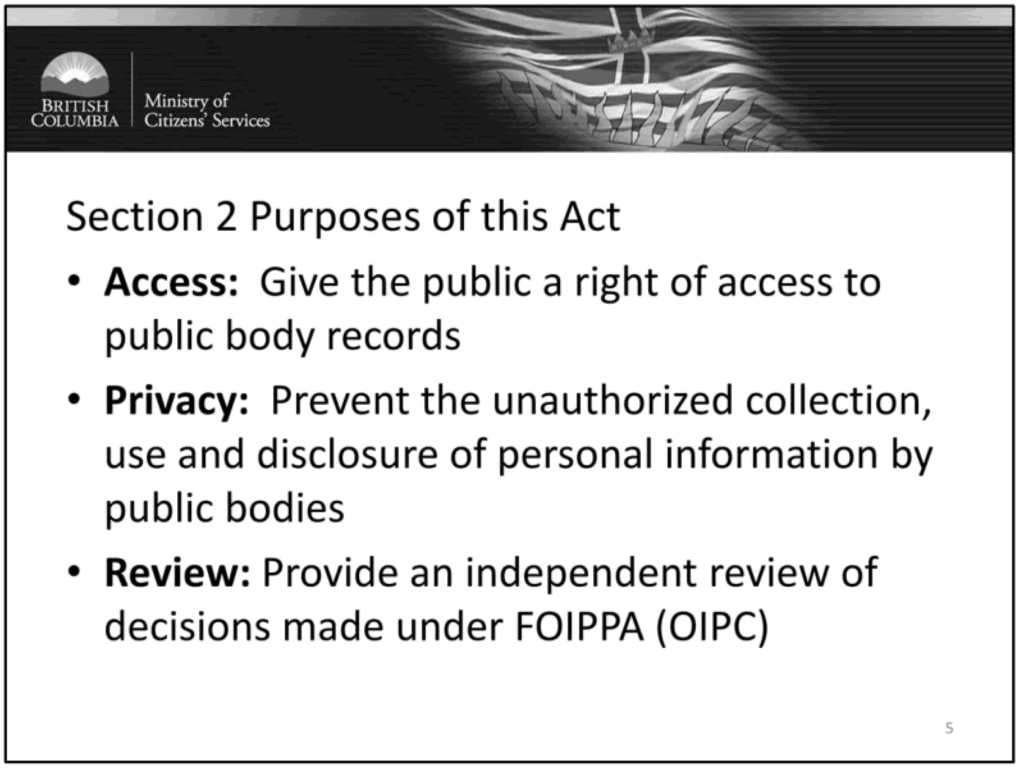


BRITISH COLUMBIA | Ministry of Citizens' Services

FOIPPA and Records Management

- FOIPPA applies to **records**
- Records management supports the FOIPPA process:
  - Ensuring records are maintained according to a set retention schedule
  - Ensuring records are properly classified
  - Ensuring records can be found and collected when a request is received

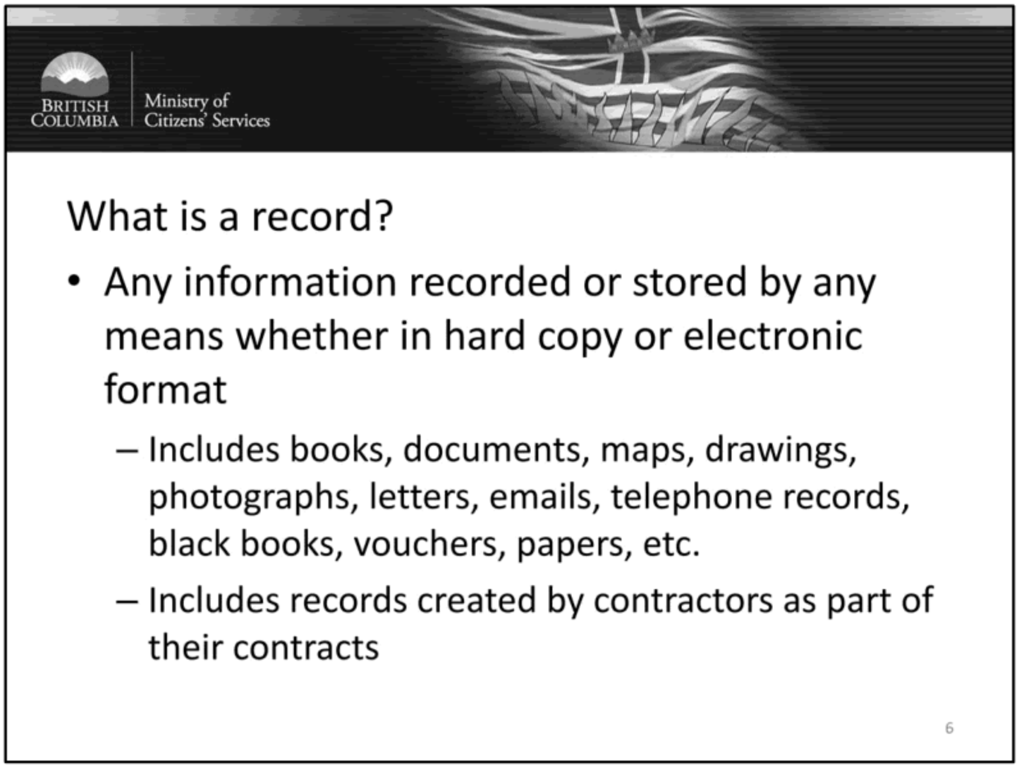
Government Records Service is a branch that works along side IAO.
https://sharedservices.gov.bc.ca/GRS/Pages/Home.aspx is a great place for RM resources.



BRITISH COLUMBIA | Ministry of Citizens' Services

Section 2 Purposes of this Act

- **Access:** Give the public a right of access to public body records
- **Privacy:** Prevent the unauthorized collection, use and disclosure of personal information by public bodies
- **Review:** Provide an independent review of decisions made under FOIPPA (OIPC)



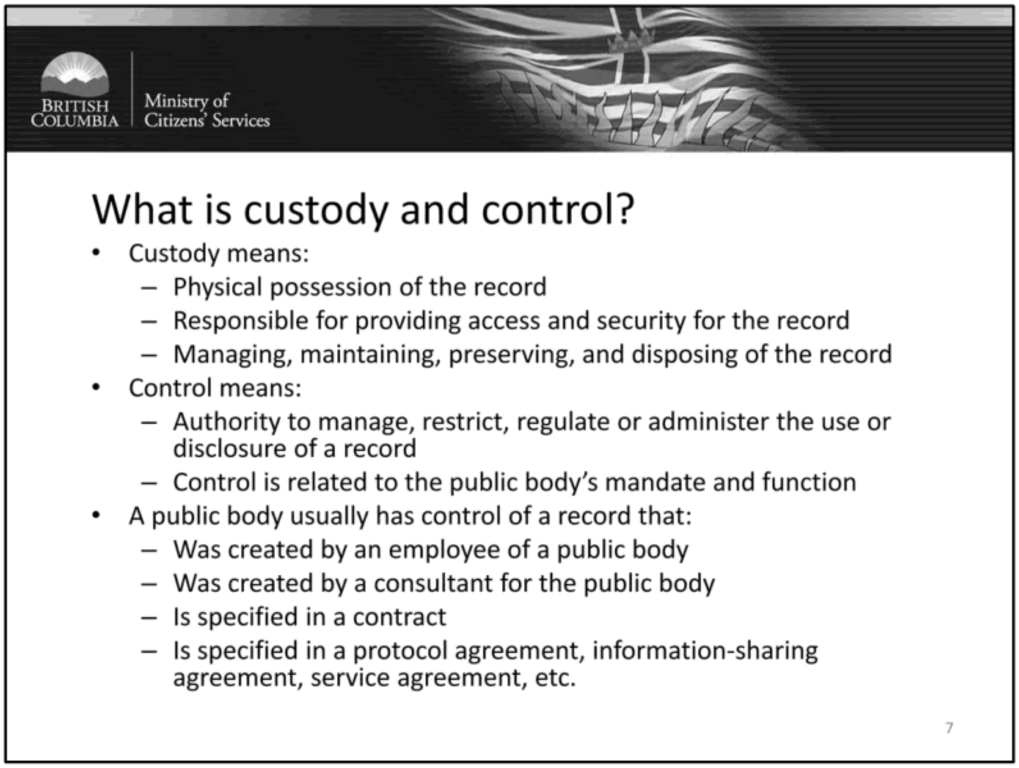
BRITISH COLUMBIA | Ministry of Citizens' Services

What is a record?

- Any information recorded or stored by any means whether in hard copy or electronic format
  - Includes books, documents, maps, drawings, photographs, letters, emails, telephone records, black books, vouchers, papers, etc.
  - Includes records created by contractors as part of their contracts

6

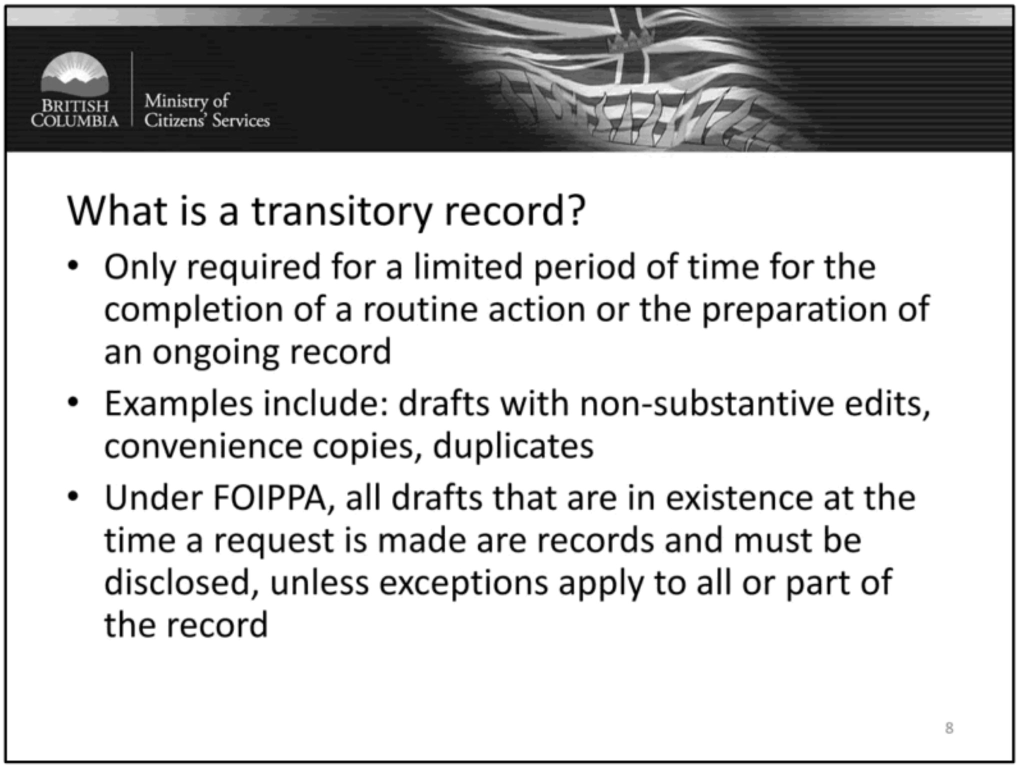
Any record that a public body has at the time of a FOI request received is NOT transitory and subject to release if it is responsive to the request even if it was transitory prior to the request being received. This includes drafts and records that belong to another public body, business, government, individual, interest group but are in the custody of the public body



BRITISH COLUMBIA | Ministry of Citizens' Services

What is custody and control?

- Custody means:
  - Physical possession of the record
  - Responsible for providing access and security for the record
  - Managing, maintaining, preserving, and disposing of the record
- Control means:
  - Authority to manage, restrict, regulate or administer the use or disclosure of a record
  - Control is related to the public body's mandate and function
- A public body usually has control of a record that:
  - Was created by an employee of a public body
  - Was created by a consultant for the public body
  - Is specified in a contract
  - Is specified in a protocol agreement, information-sharing agreement, service agreement, etc.

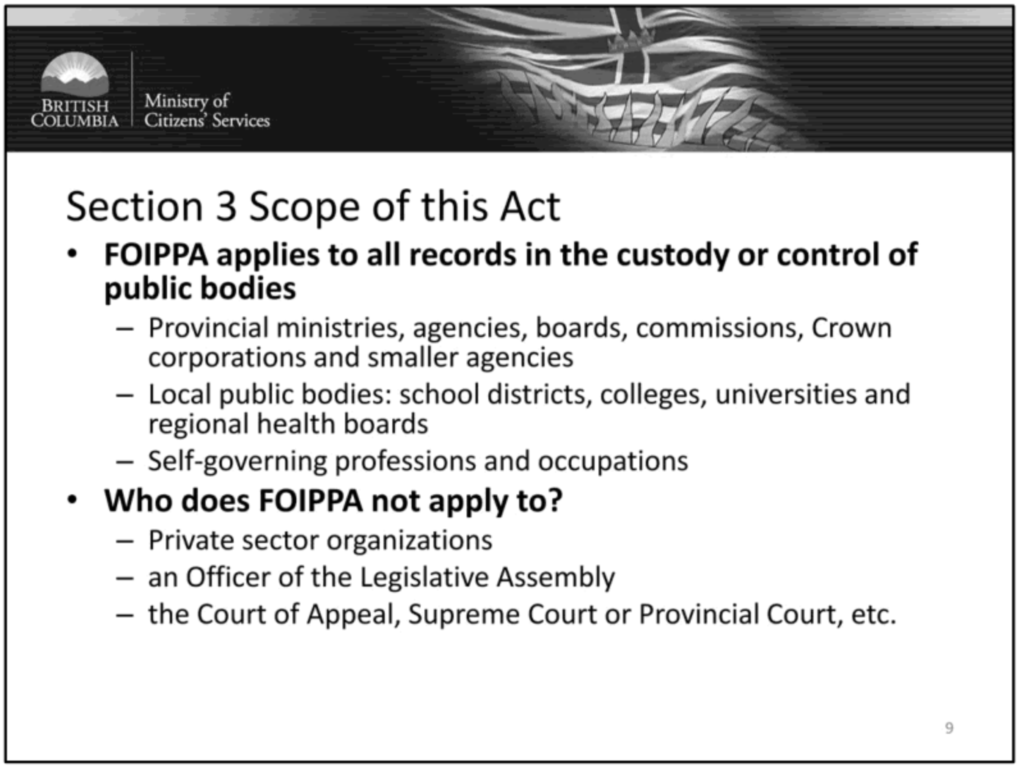


BRITISH COLUMBIA | Ministry of Citizens' Services

What is a transitory record?

- Only required for a limited period of time for the completion of a routine action or the preparation of an ongoing record
- Examples include: drafts with non-substantive edits, convenience copies, duplicates
- Under FOIPPA, all drafts that are in existence at the time a request is made are records and must be disclosed, unless exceptions apply to all or part of the record

8



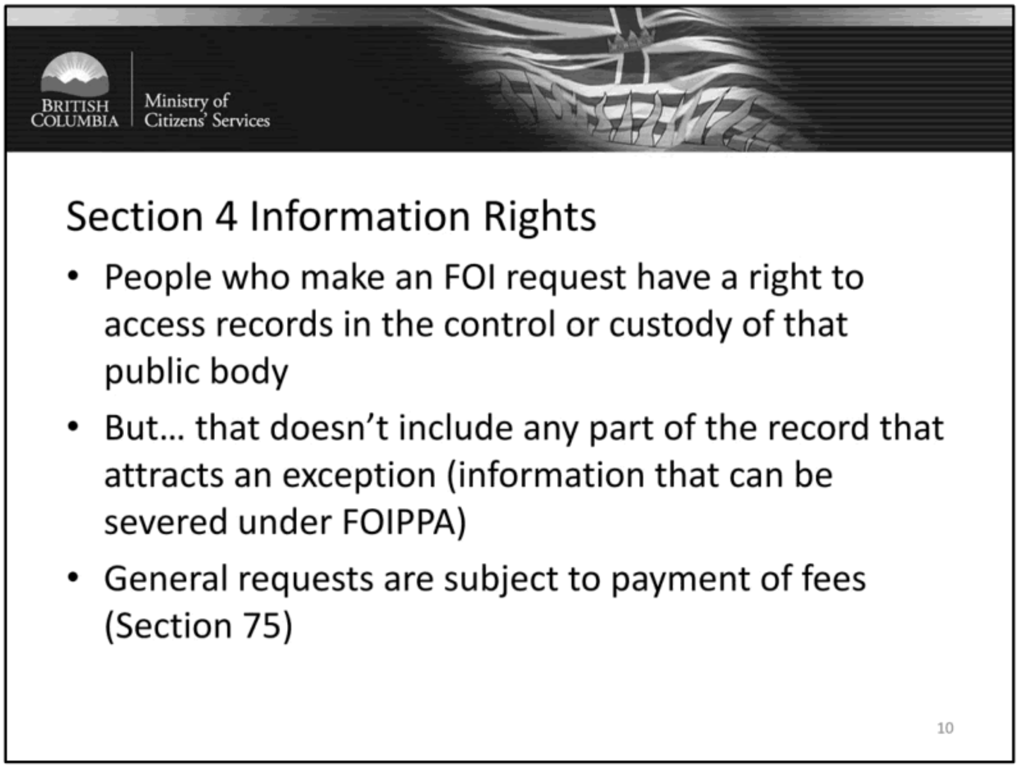
BRITISH COLUMBIA | Ministry of Citizens' Services

Section 3 Scope of this Act

- **FOIPPA applies to all records in the custody or control of public bodies**
  - Provincial ministries, agencies, boards, commissions, Crown corporations and smaller agencies
  - Local public bodies: school districts, colleges, universities and regional health boards
  - Self-governing professions and occupations
- **Who does FOIPPA not apply to?**
  - Private sector organizations
  - an Officer of the Legislative Assembly
  - the Court of Appeal, Supreme Court or Provincial Court, etc.

A list of the public bodies can be found in Schedules 2 and 3 of FOIPPA. Schedule 2 and 3 public bodies fall under FOIPPA but process their own FOI requests. Some have dedicated FOI analysts while others will hire an FOI contractor.

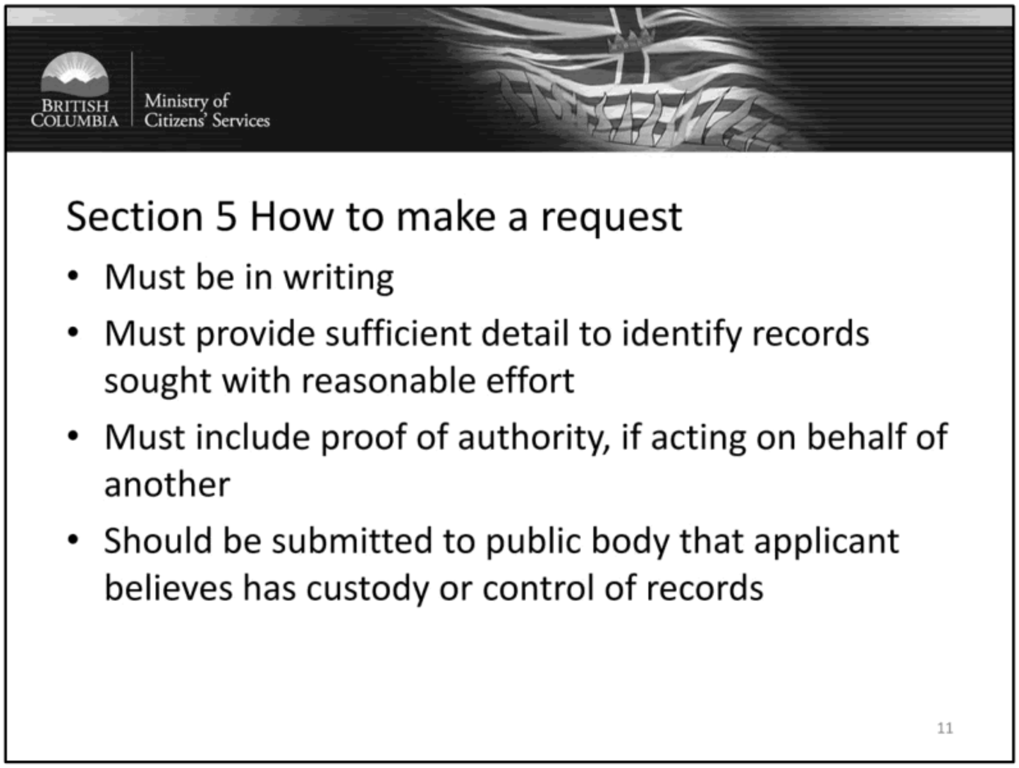
Section 3 has the full list of what FOIPPA does not cover. This means people can request items listed but IAO does not give out under FOIPPA.



BRITISH COLUMBIA | Ministry of Citizens' Services

Section 4 Information Rights

- People who make an FOI request have a right to access records in the control or custody of that public body
- But… that doesn't include any part of the record that attracts an exception (information that can be severed under FOIPPA)
- General requests are subject to payment of fees (Section 75)



BRITISH COLUMBIA | Ministry of Citizens' Services

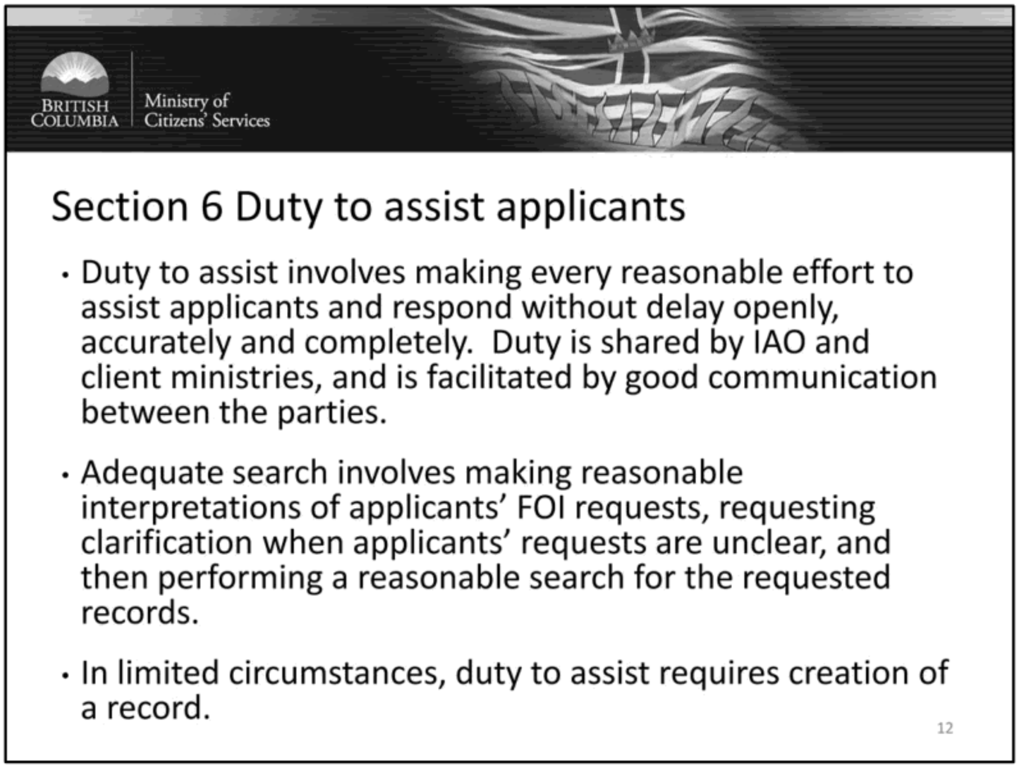
Section 5 How to make a request

- Must be in writing
- Must provide sufficient detail to identify records sought with reasonable effort
- Must include proof of authority, if acting on behalf of another
- Should be submitted to public body that applicant believes has custody or control of records

11

At IAO we get FOI requests through our online form, by fax, by mail, on old forms that they mail or fax, from the ministry who has received it an all these different forms months after they have received it.

Not all requests for information are requests under FOIPPA. Many requesters are looking for answers to questions. We advise we provide records and they should speak to the public body about their questions. Sometimes what they are asking for is publically available through a website. Sometimes what they are asking for is routinely releasable. Consolidated Intake has to do a lot of up front work to manage these types of situations.



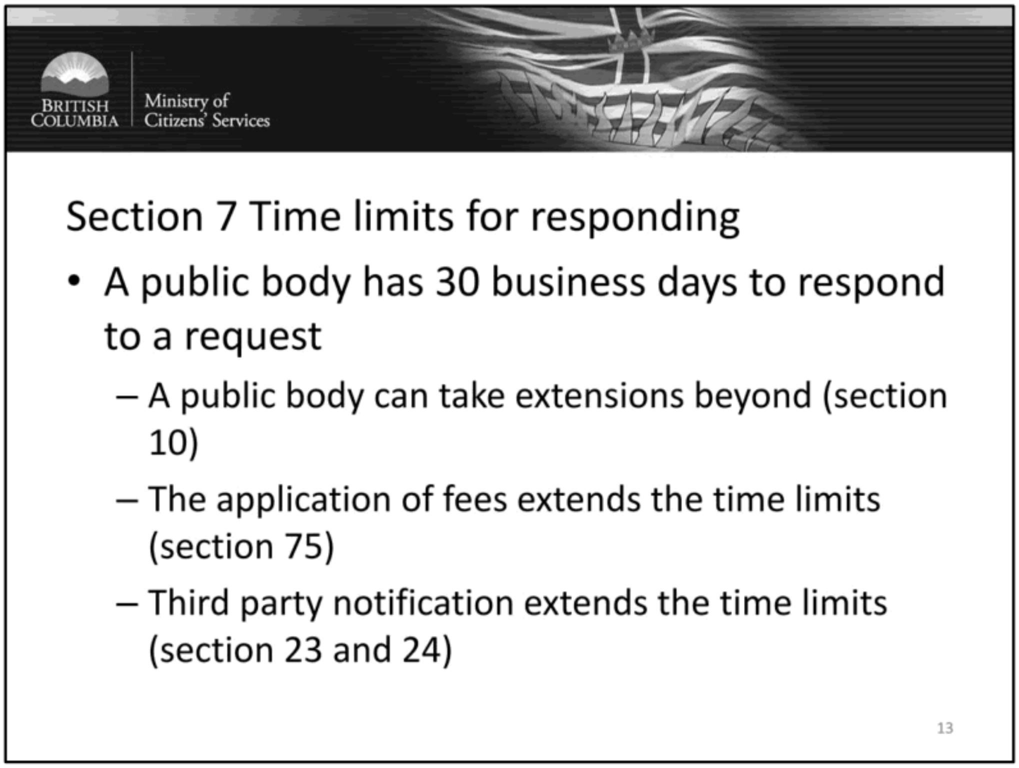
BRITISH COLUMBIA | Ministry of Citizens' Services

Section 6 Duty to assist applicants

- Duty to assist involves making every reasonable effort to assist applicants and respond without delay openly, accurately and completely. Duty is shared by IAO and client ministries, and is facilitated by good communication between the parties.
- Adequate search involves making reasonable interpretations of applicants' FOI requests, requesting clarification when applicants' requests are unclear, and then performing a reasonable search for the requested records.
- In limited circumstances, duty to assist requires creation of a record.

Failure to comply with section 6 leaves a public body open to OIPC review. IAO is also subject to section 6 in that we should not be taking unnecessary extensions or consultations for FOI requests.

However, a public body can apply to the OIPC to disregard requests that are frivolous or vexatious or because they would unreasonable interfere with the operations of a public body because of their repetitious or systematic nature – section 43.

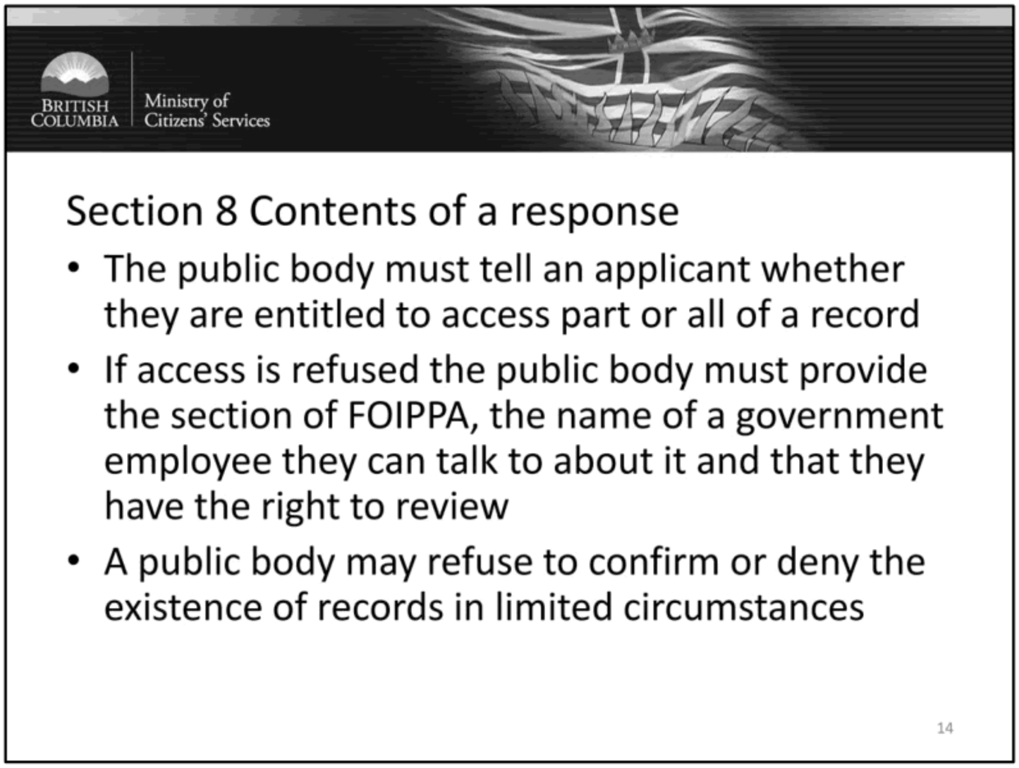


BRITISH COLUMBIA | Ministry of Citizens' Services

Section 7 Time limits for responding

- A public body has 30 business days to respond to a request
  - A public body can take extensions beyond (section 10)
  - The application of fees extends the time limits (section 75)
  - Third party notification extends the time limits (section 23 and 24)

30 business days is often enough to complete a request. However, an applicant could ask for many years of records or to include all the drafts. The records could be authored by a third party and contain their business information and we are considering releasing it. There are many reasons to take an extension and it is important to know your options.



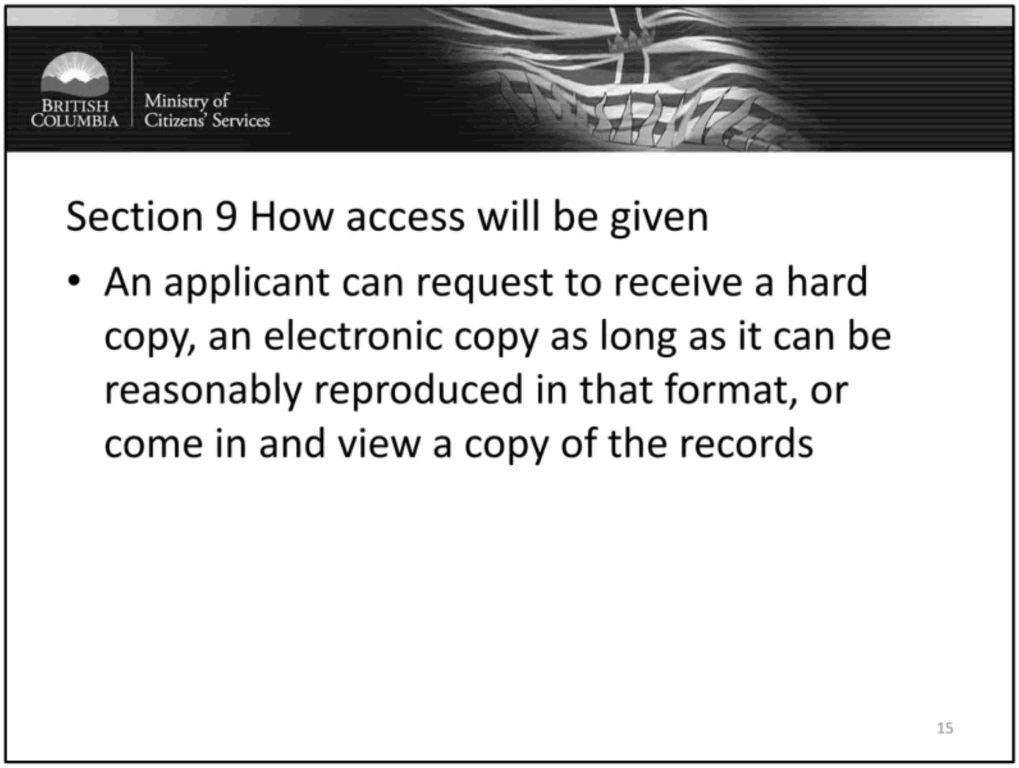
BRITISH COLUMBIA | Ministry of Citizens' Services

Section 8 Contents of a response

- The public body must tell an applicant whether they are entitled to access part or all of a record
- If access is refused the public body must provide the section of FOIPPA, the name of a government employee they can talk to about it and that they have the right to review
- A public body may refuse to confirm or deny the existence of records in limited circumstances

14

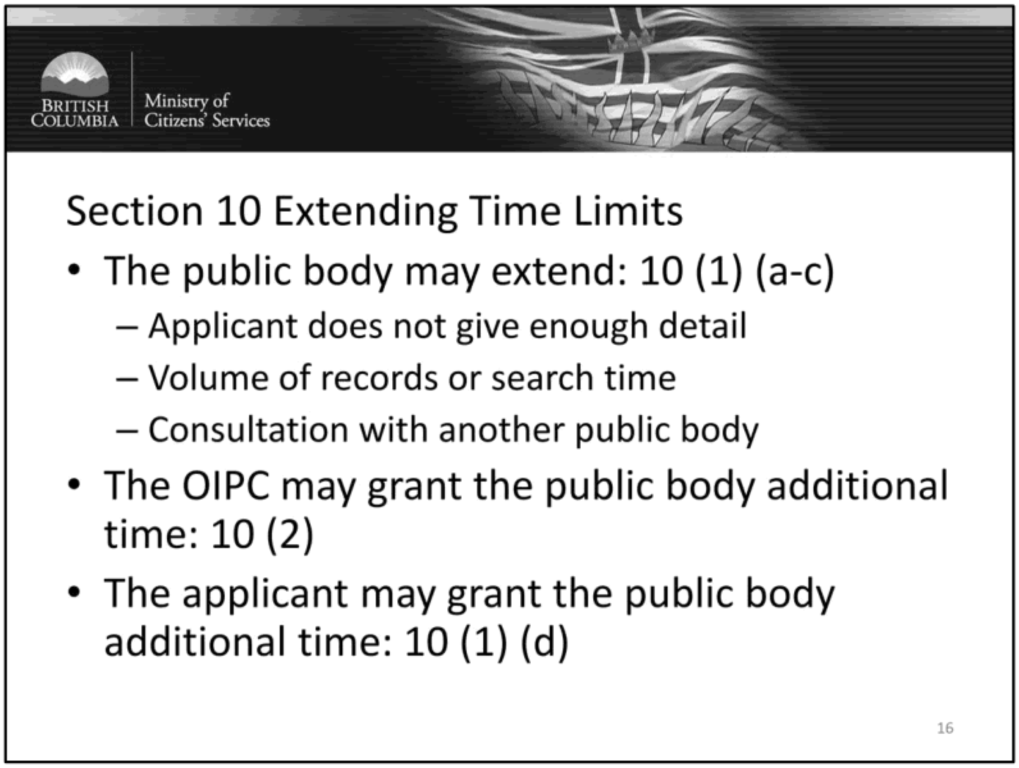
This section is the foundation of the templates used by IAO. There is a Template Team that goes over every word used in a letter. The Policy and Procedures Manual outlines, with even greater detail, our responses to an applicant. The OIPC has on occasion recommended improvements on how a public body should respond to applicants.


BRITISH COLUMBIA
Ministry of Citizens' Services

Section 9 How access will be given

- An applicant can request to receive a hard copy, an electronic copy as long as it can be reasonably reproduced in that format, or come in and view a copy of the records

IAO's practice is that general requests are more often than not sent out electronically – sometimes on disk if too large for email. Personal requests are more often than not printed and mailed (by trace). We want to guarantee that an individual is getting their personal records.



BRITISH COLUMBIA | Ministry of Citizens' Services

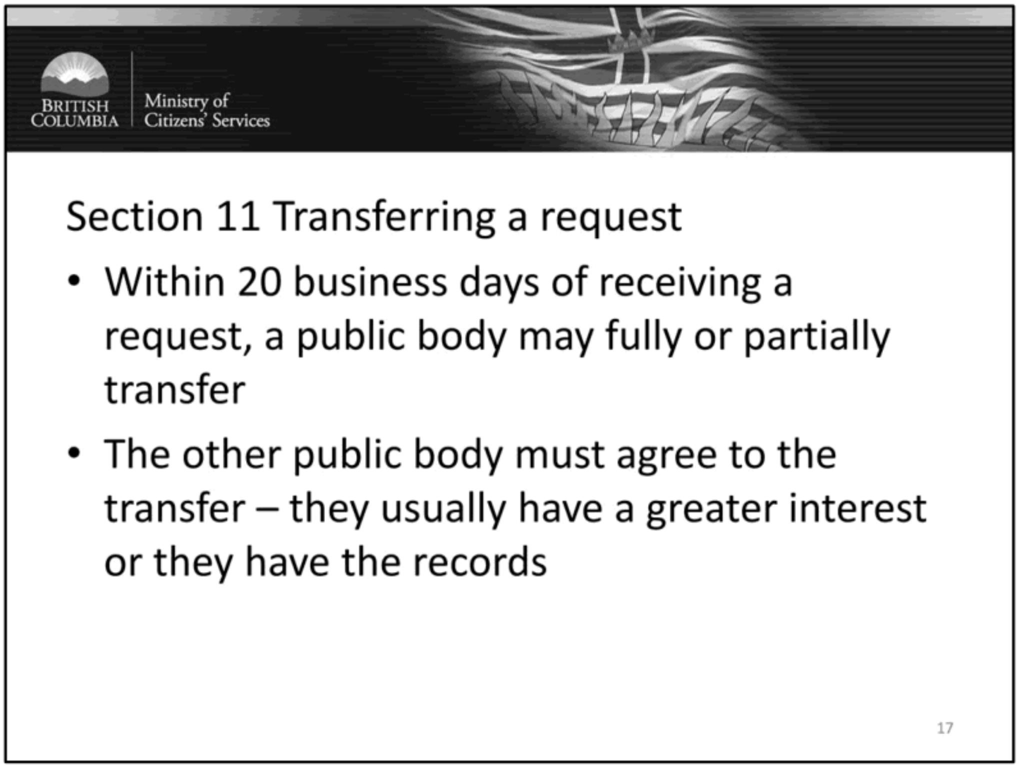
Section 10 Extending Time Limits

- The public body may extend: 10 (1) (a-c)
  - Applicant does not give enough detail
  - Volume of records or search time
  - Consultation with another public body
- The OIPC may grant the public body additional time: 10 (2)
- The applicant may grant the public body additional time: 10 (1) (d)

The first public body extensions are up to 30 business days.

Anything past 60 business days must be approved by the OIPC. There is an application form that IAO must fill out for each extension. The OIPC has their own set of guidelines to grant or deny extensions.

Applicant consent is a newer option that allows the public body to negotiate directly with the applicant on time lines. It is well worth an analysts time to develop trusting relationships with their applicant and ministry when pursing 10 (1)(d)s.

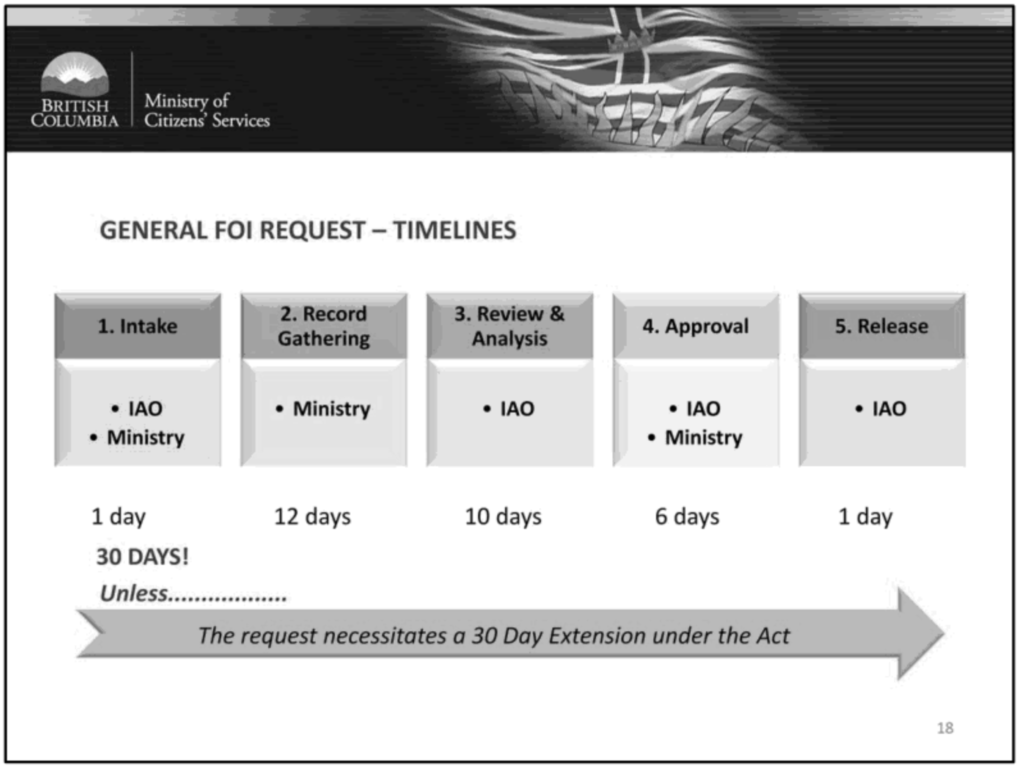


BRITISH COLUMBIA | Ministry of Citizens' Services

Section 11 Transferring a request

- Within 20 business days of receiving a request, a public body may fully or partially transfer
- The other public body must agree to the transfer – they usually have a greater interest or they have the records

Occasionally, the time limits for transferring have expired. In these cases it is administratively fair to advise the applicant in the response letter which public body may also have records on the topic they are requesting.



BRITISH COLUMBIA | Ministry of Citizens' Services

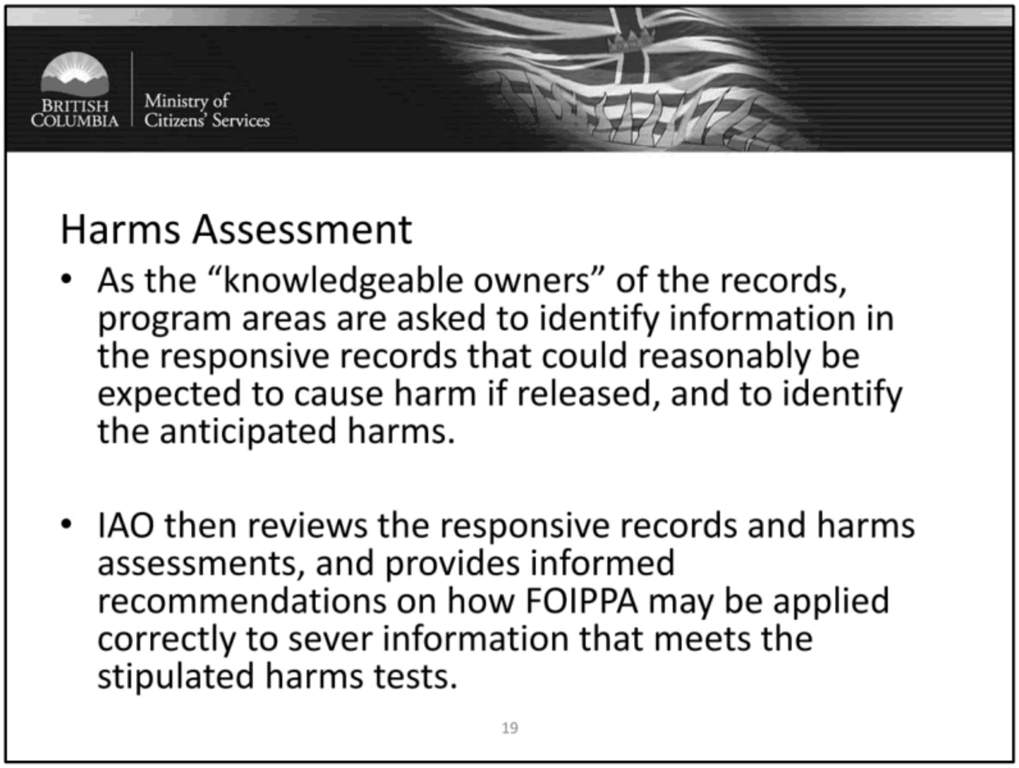
GENERAL FOI REQUEST – TIMELINES

1. Intake	2. Record Gathering	3. Review & Analysis	4. Approval	5. Release
• IAO • Ministry	• Ministry	• IAO	• IAO • Ministry	• IAO
1 day	12 days	10 days	6 days	1 day

30 DAYS!

Unless..................

The request necessitates a 30 Day Extension under the Act

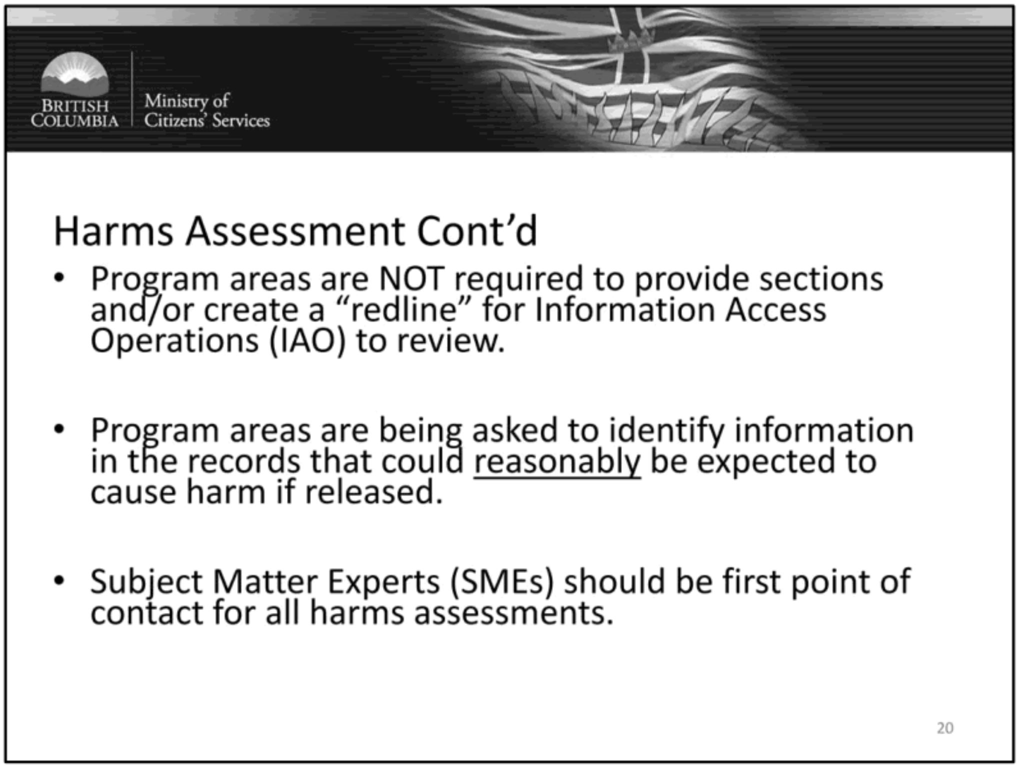


BRITISH COLUMBIA | Ministry of Citizens' Services

Harms Assessment

- As the "knowledgeable owners" of the records, program areas are asked to identify information in the responsive records that could reasonably be expected to cause harm if released, and to identify the anticipated harms.

- IAO then reviews the responsive records and harms assessments, and provides informed recommendations on how FOIPPA may be applied correctly to sever information that meets the stipulated harms tests.



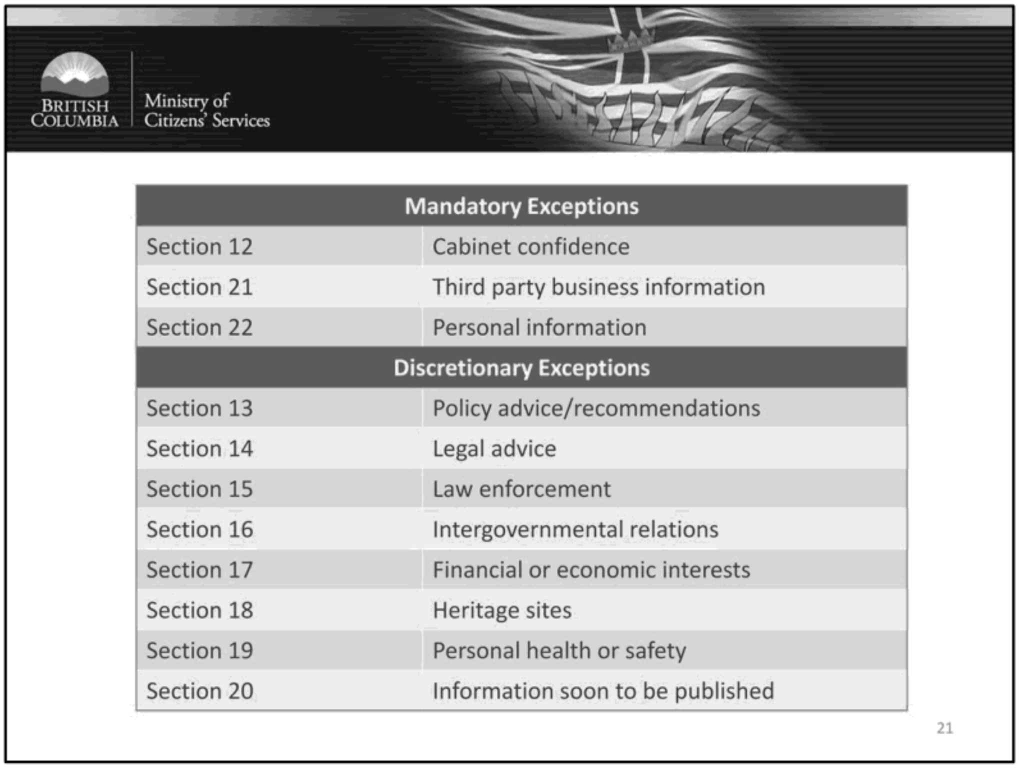
BRITISH COLUMBIA | Ministry of Citizens' Services

Harms Assessment Cont'd

- Program areas are NOT required to provide sections and/or create a "redline" for Information Access Operations (IAO) to review.
- Program areas are being asked to identify information in the records that could reasonably be expected to cause harm if released.
- Subject Matter Experts (SMEs) should be first point of contact for all harms assessments.

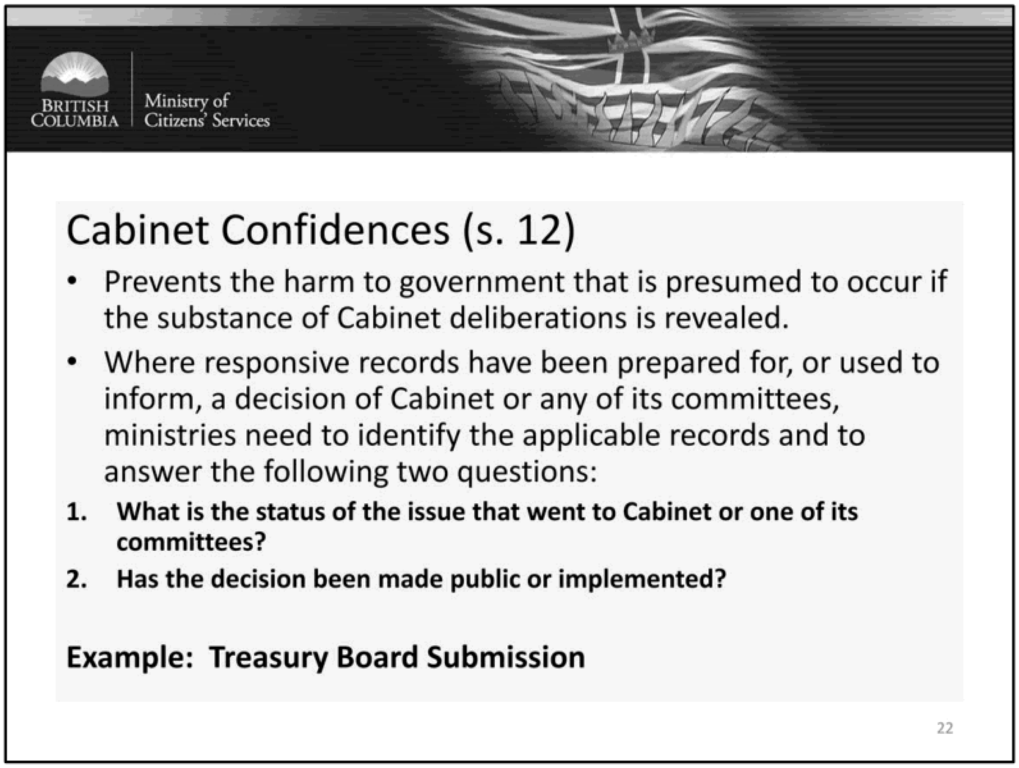
As the "knowledgeable owners" of your records, ministries are asked to identify information in the responsive records that could reasonably be expected to cause harm if released, and to identify the anticipated harms.

IAO then reviews the responsive records and harms assessments, and provides informed recommendations on how FOIPPA may be applied correctly to sever information that meets the stipulated harms tests.



BRITISH COLUMBIA | Ministry of Citizens' Services

Mandatory Exceptions	
Section 12	Cabinet confidence
Section 21	Third party business information
Section 22	Personal information
Discretionary Exceptions	
Section 13	Policy advice/recommendations
Section 14	Legal advice
Section 15	Law enforcement
Section 16	Intergovernmental relations
Section 17	Financial or economic interests
Section 18	Heritage sites
Section 19	Personal health or safety
Section 20	Information soon to be published



BRITISH COLUMBIA | Ministry of Citizens' Services

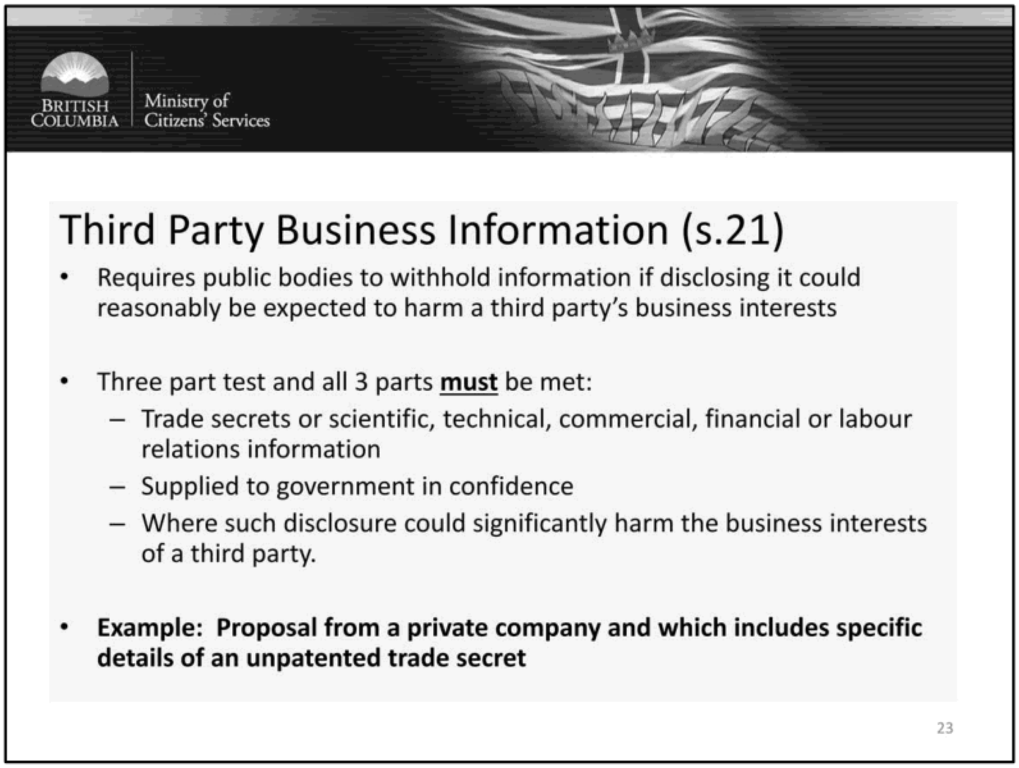
Cabinet Confidences (s. 12)

- Prevents the harm to government that is presumed to occur if the substance of Cabinet deliberations is revealed.
- Where responsive records have been prepared for, or used to inform, a decision of Cabinet or any of its committees, ministries need to identify the applicable records and to answer the following two questions:

1. **What is the status of the issue that went to Cabinet or one of its committees?**
2. **Has the decision been made public or implemented?**

Example: Treasury Board Submission

Example – Annual Submissions for Highway Capital Construction Program requires Treasury Board approval. Another example is Highway rehabilitation.



BRITISH COLUMBIA | Ministry of Citizens' Services

Third Party Business Information (s.21)

- Requires public bodies to withhold information if disclosing it could reasonably be expected to harm a third party's business interests

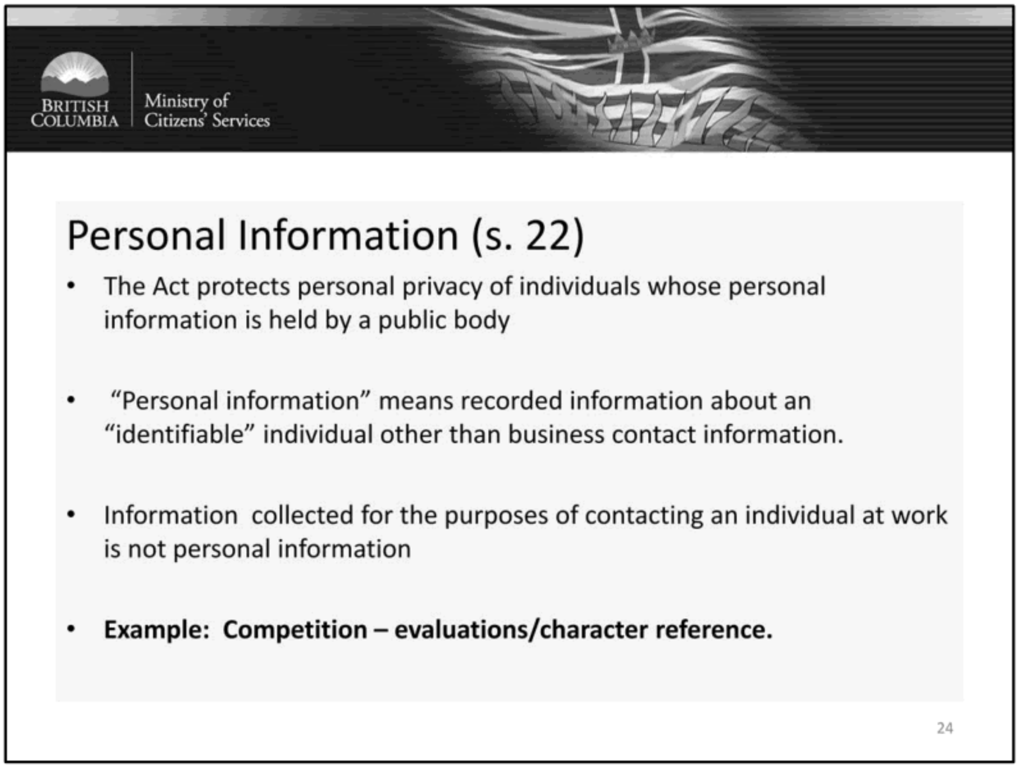
- Three part test and all 3 parts **must** be met:
  - Trade secrets or scientific, technical, commercial, financial or labour relations information
  - Supplied to government in confidence
  - Where such disclosure could significantly harm the business interests of a third party.

- **Example: Proposal from a private company and which includes specific details of an unpatented trade secret**

this is one of the most controversial and most difficult exception to apply. The one thing to remember if you plan to use this to withhold information from an applicant is that the 'harm' must be immutable, not speculative.

- It must be business information.
- It must be more than an assertion; the public body must have evidence (NOT negotiated in confidence)
- Watch for 'significant' harm to business interests

Proposal from a private company and which includes specific details of an unpatented trade secret
Assessment reports prepared by a Regulatory body which contain internal and confidential commercial, financial, technical information and/or trade secrets of a third party



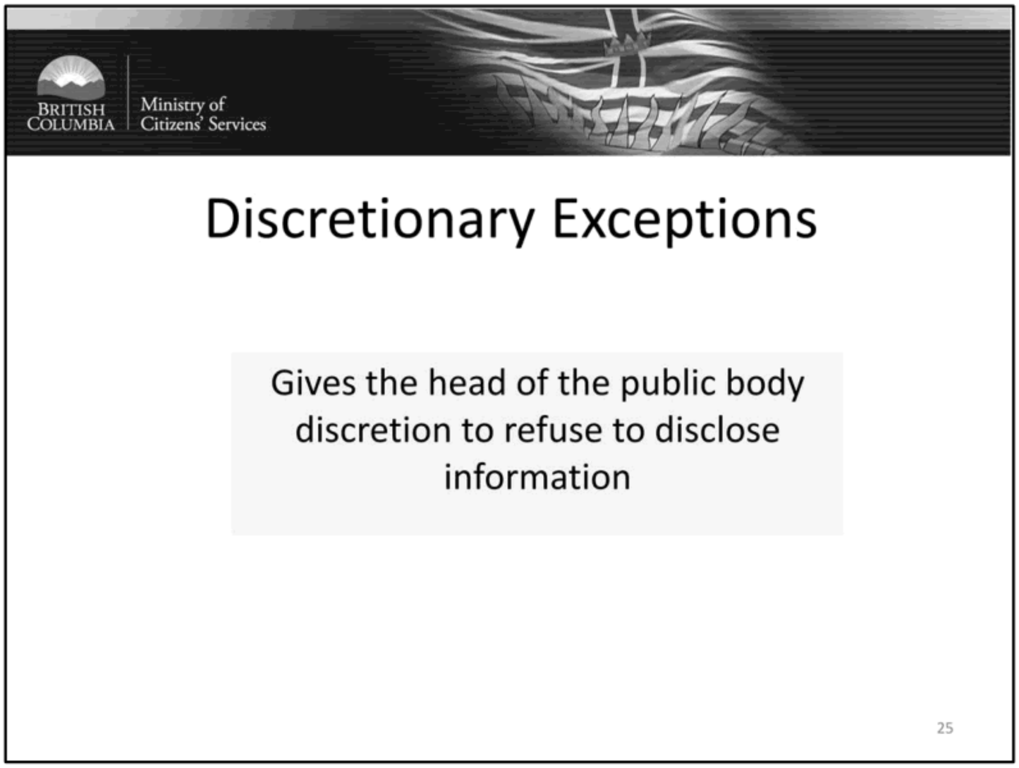
BRITISH COLUMBIA | Ministry of Citizens' Services

Personal Information (s. 22)

- The Act protects personal privacy of individuals whose personal information is held by a public body
- "Personal information" means recorded information about an "identifiable" individual other than business contact information.
- Information collected for the purposes of contacting an individual at work is not personal information
- **Example: Competition – evaluations/character reference.**

Always: express opinions about individuals carefully –Your opinion about another third party belongs to that individual. So write as if it will be released. keep to facts, omit opinions - Keep your 'personal' opinion out of recorded information as it could get captured in a FOI request.

e.g. Meeting notice from a staff member – "don't' forget your flack jacket'"
e.g. competition – evaluations/character reference. You could receive a FOI request from the third party the information is about to see what references said about them, it will go out unless you can infer who said it. References: can see what was said, not who said it



BRITISH COLUMBIA | Ministry of Citizens' Services

Discretionary Exceptions

Gives the head of the public body discretion to refuse to disclose information

Now we are into discretionary exception where it isn't the presumption of harm but rather it must meet a harms test.

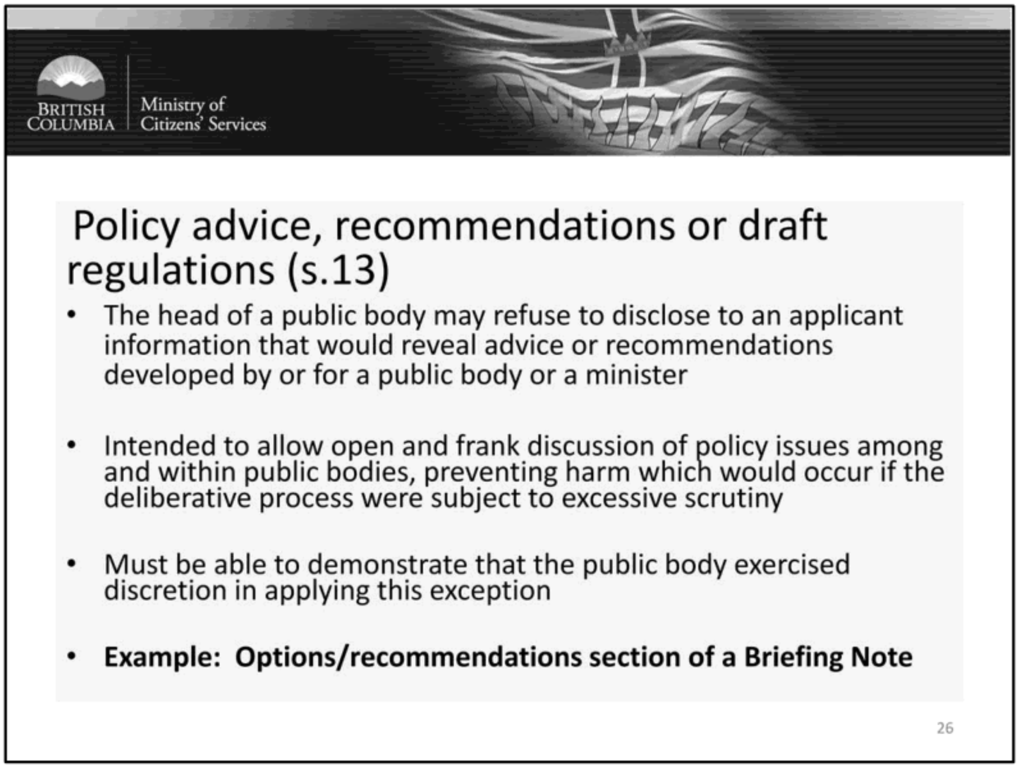
Read slide

What this means is that the public body must make a decision whether releasing the information could cause harm to the public body or a third party

Even if all of the requirements of the section are met, the information does not have to be severed. The head of a public body has discretion to **not** sever the information. (discretion = power to act in an official capacity in a manner that appears to be just and proper under the circumstances)

Two parts to applying exception:
•Does the exception apply?
•relevant factors in the exercise of discretion:

- The purpose of the Legislation
- Balance of interests (what is the purpose of exception?)
- could the request be satisfied by severing the record & providing as much information as is reasonably practicable?
- Historical practice
- Will disclosure increase public confidence?
- Age of the record
- Sympathetic or compelling need
- Previous orders


BRITISH COLUMBIA
Ministry of Citizens' Services

Policy advice, recommendations or draft regulations (s.13)

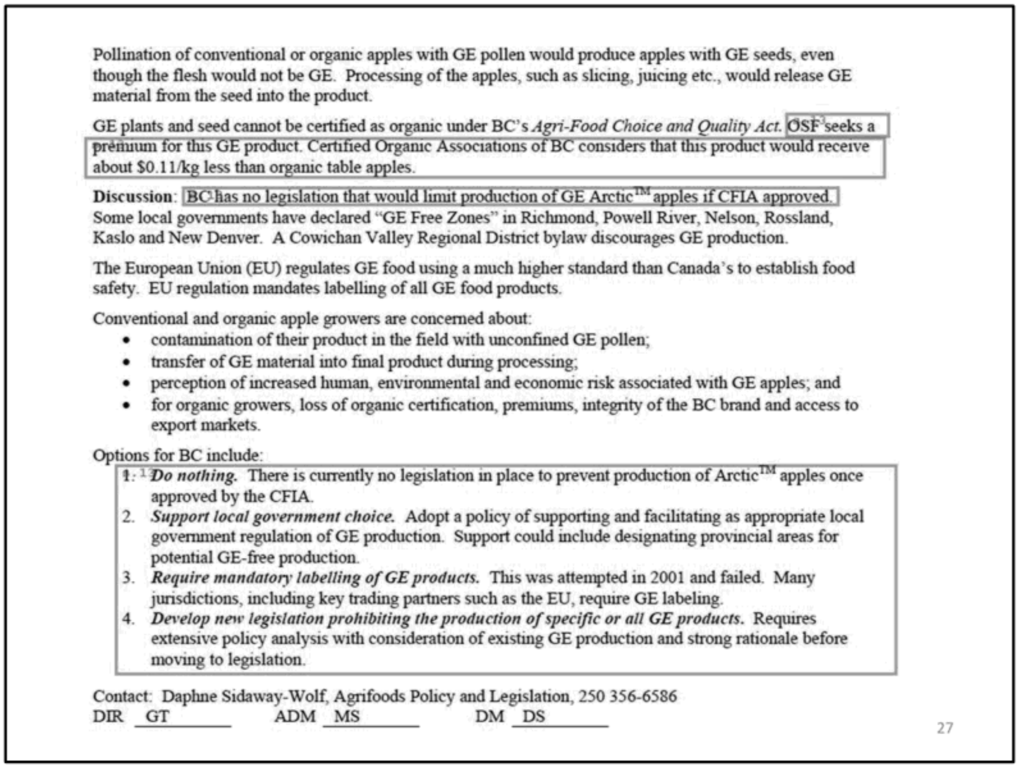
- The head of a public body may refuse to disclose to an applicant information that would reveal advice or recommendations developed by or for a public body or a minister
- Intended to allow open and frank discussion of policy issues among and within public bodies, preventing harm which would occur if the deliberative process were subject to excessive scrutiny
- Must be able to demonstrate that the public body exercised discretion in applying this exception
- **Example: Options/recommendations section of a Briefing Note**

Applied when a harm can occur if the decision-making body's deliberative process is subject to 'excessive scrutiny', esp. w/ advice, recommendations developed by/for p.b./minister. Clearly applies to internal recommendations and/or options for a particular project or service provider.

Obvious example is Briefing Note - this is why it is important to stick to the BN formats, Background usually contains facts of the case, then you have discussion, options/impacts then recommendations – if you have such information laced throughout the BN, it makes it more difficult to quickly locate and apply.
-- if it's not clearly labelled, we're going to come to you

But it isn't just BN's where s.13 can apply. Many times our email communications contain information subject to multiple provisions, this being one.

REMEMBER:
•This exception can only be applied where the information would reveal advice or recommendations.
•In exercising discretion, a relevant factor to consider would be whether disclosure would result in harm.
•The head must be able to demonstrate that s/he exercised discretion in applying the exceptions.



Pollination of conventional or organic apples with GE pollen would produce apples with GE seeds, even though the flesh would not be GE. Processing of the apples, such as slicing, juicing etc., would release GE material from the seed into the product.

GE plants and seed cannot be certified as organic under BC's *Agri-Food Choice and Quality Act.* OSF[3] seeks a premium for this GE product. Certified Organic Associations of BC considers that this product would receive about $0.11/kg less than organic table apples.

Discussion: BC[2] has no legislation that would limit production of GE Arctic™ apples if CFIA approved. Some local governments have declared "GE Free Zones" in Richmond, Powell River, Nelson, Rossland, Kaslo and New Denver. A Cowichan Valley Regional District bylaw discourages GE production.

The European Union (EU) regulates GE food using a much higher standard than Canada's to establish food safety. EU regulation mandates labelling of all GE food products.

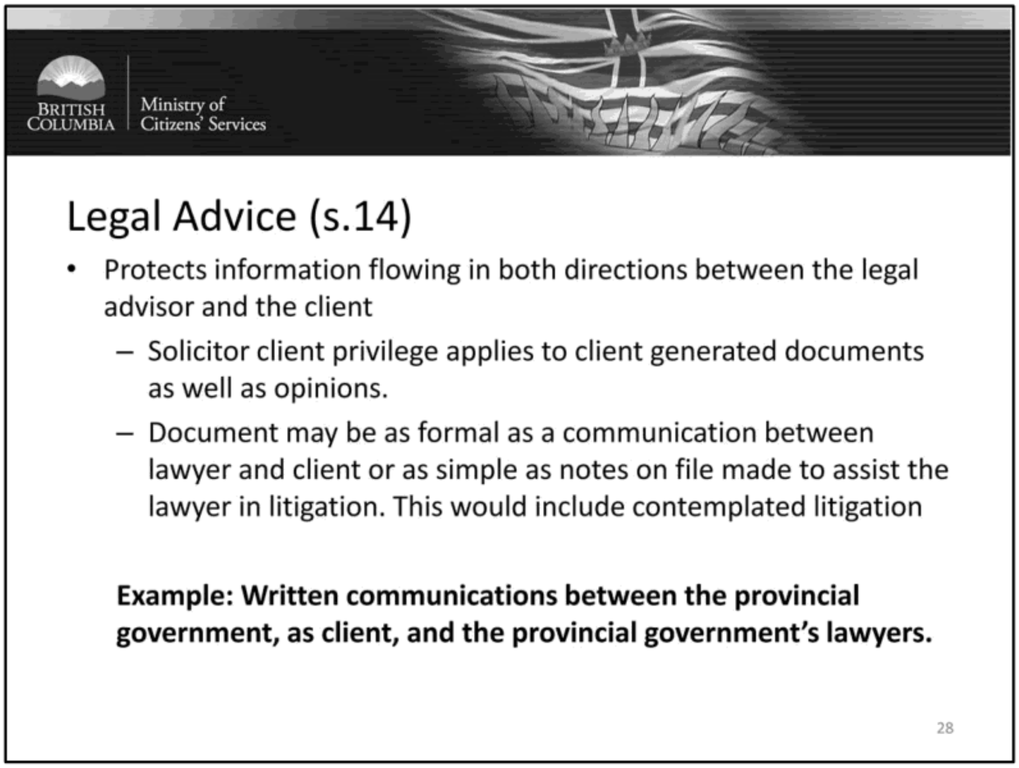
Conventional and organic apple growers are concerned about:

- contamination of their product in the field with unconfined GE pollen;
- transfer of GE material into final product during processing;
- perception of increased human, environmental and economic risk associated with GE apples; and
- for organic growers, loss of organic certification, premiums, integrity of the BC brand and access to export markets.

Options for BC include:

1. [1] ***Do nothing.*** There is currently no legislation in place to prevent production of Arctic™ apples once approved by the CFIA.
2. ***Support local government choice.*** Adopt a policy of supporting and facilitating as appropriate local government regulation of GE production. Support could include designating provincial areas for potential GE-free production.
3. ***Require mandatory labelling of GE products.*** This was attempted in 2001 and failed. Many jurisdictions, including key trading partners such as the EU, require GE labeling.
4. ***Develop new legislation prohibiting the production of specific or all GE products.*** Requires extensive policy analysis with consideration of existing GE production and strong rationale before moving to legislation.

Contact: Daphne Sidaway-Wolf, Agrifoods Policy and Legislation, 250 356-6586
DIR GT ADM MS DM DS



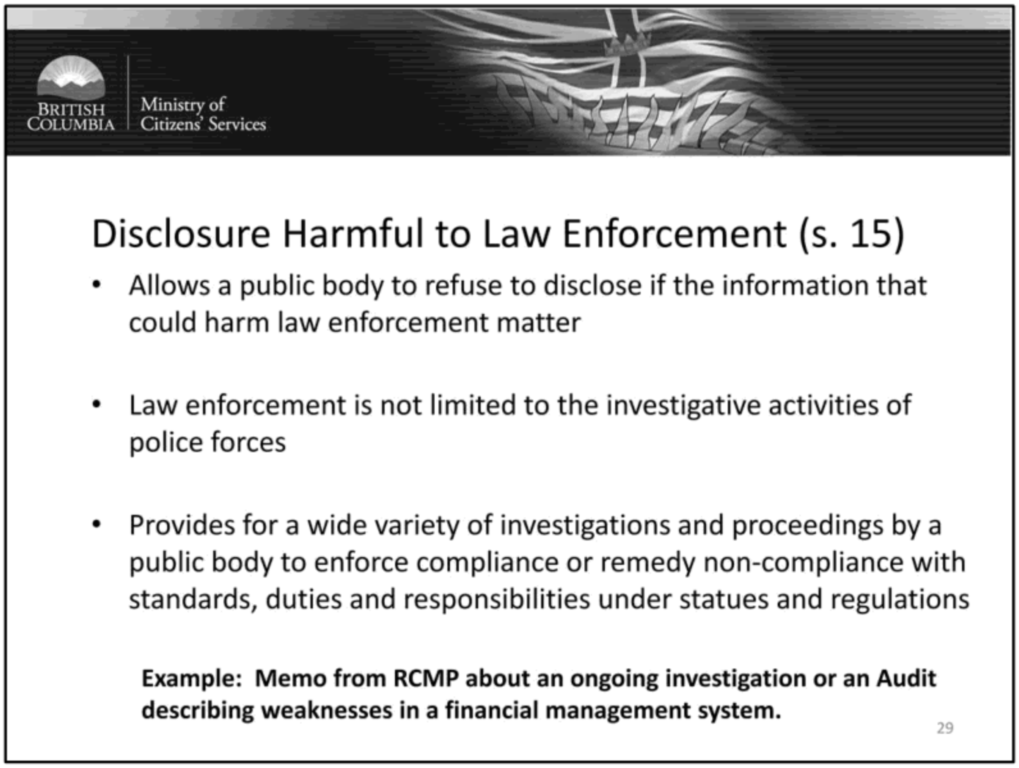
BRITISH COLUMBIA | Ministry of Citizens' Services

Legal Advice (s.14)

- Protects information flowing in both directions between the legal advisor and the client
  - Solicitor client privilege applies to client generated documents as well as opinions.
  - Document may be as formal as a communication between lawyer and client or as simple as notes on file made to assist the lawyer in litigation. This would include contemplated litigation

Example: Written communications between the provincial government, as client, and the provincial government's lawyers.

This section preserves the fundamental and common law right that communications b/n clients and their lawyers remain privileged and it Protects information flowing in both direction b/n client and solicitor.. The Public body has to be seeking advice.



BRITISH COLUMBIA | Ministry of Citizens' Services

Disclosure Harmful to Law Enforcement (s. 15)

- Allows a public body to refuse to disclose if the information that could harm law enforcement matter
- Law enforcement is not limited to the investigative activities of police forces
- Provides for a wide variety of investigations and proceedings by a public body to enforce compliance or remedy non-compliance with standards, duties and responsibilities under statues and regulations

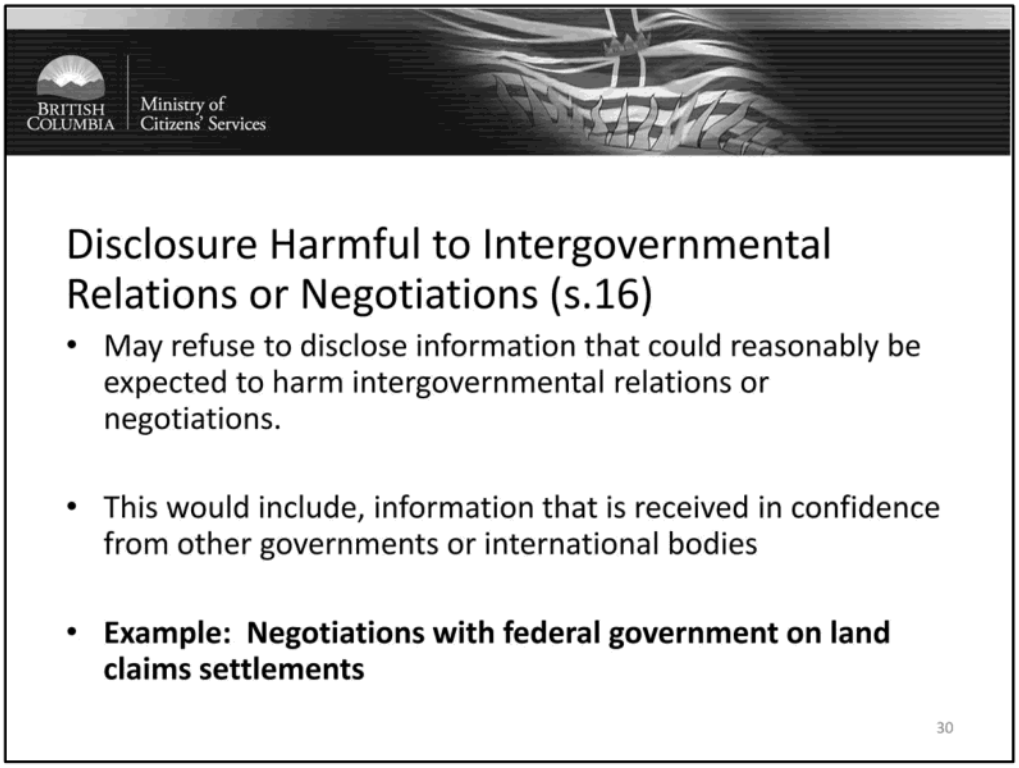
Example: Memo from RCMP about an ongoing investigation or an Audit describing weaknesses in a financial management system.

29

Law enforcement. This section allows a public body to refuse to disclose if the information could harm a law enforcement matter.
Cases may arise where there is the presumption of the Mosaic Effect. What this means is while one record by itself may appear to be harmless if put together with other or related records they may form part of a larger picture . For example Jericho Hill School was a provincially run school for the deaf and blind. There were accusations of sexual abuse. Former students were coming forward and suing the government.. The School kept daily ledgers documenting activities of individual students . One students file may say nothing but if you put all the student files together welll………

2nd bullet but it also read bullet. This area is not limited to police matters. This allows Student Services to perform audits or ESB to order determinations which includes investigations that lead or could lead to the imposition of a penalty or sanction either by the public body itself or another public organization such as a court. Moving right along

•investigation file of C&E while the investigation is in progress
•audit describing weaknesses in a financial management system
•name of a witness in a harassment investigation
•a teleconference ID number
•any sort of password or pass code



BRITISH COLUMBIA | Ministry of Citizens' Services

Disclosure Harmful to Intergovernmental Relations or Negotiations (s.16)

- May refuse to disclose information that could reasonably be expected to harm intergovernmental relations or negotiations.
- This would include, information that is received in confidence from other governments or international bodies
- **Example: Negotiations with federal government on land claims settlements**

Section 16 –This section can be applied if it could harm the relations between the Government of BC and other governments or their agencies. For example: Negotiations surrounding Treaties would fall under this section etc..It also Includes negotiations with municipal government, Relations between school boards and the Ministry of Education An example of interministry negotiations is when Skills Development and Labour was being transferred to the Ministry of HR. The negotiations surrounding the transfer of FTE's would be withheld. ....

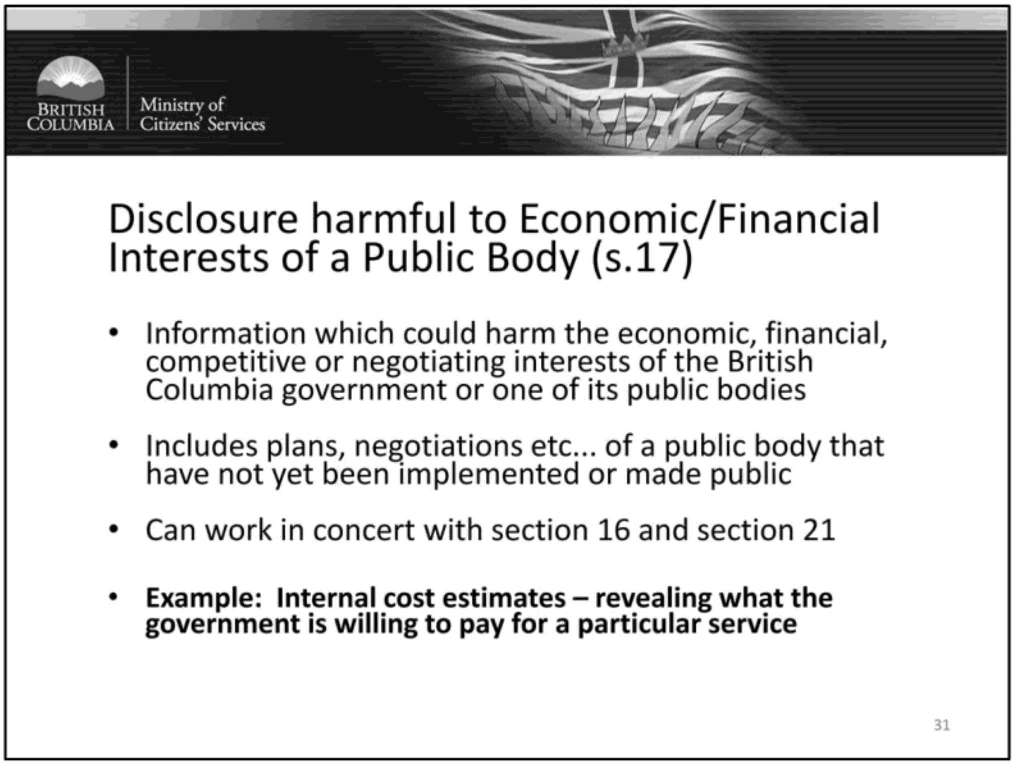
1) Is the record less than 15 years old?
2) Would disclosure:
    - Harm the conduct of relations between the provincial government and another government (federal, municipal, aboriginal or foreign)?
    - Reveal information received in confidence by another government?
    - Harm aboriginal self government or treaty negotiations?

It is difficult for Analysts to know the big picture: senior execs know what's going on

Minister's need to consult with intergovernmental secretariat. E.g., Washington State/B.C. borders

'reasonably harm' once again is the threshold – make sure you have informational backing to apply this section

e.g., memo from RCMP; letter from band chief regarding confidential negotiations



BRITISH COLUMBIA | Ministry of Citizens' Services

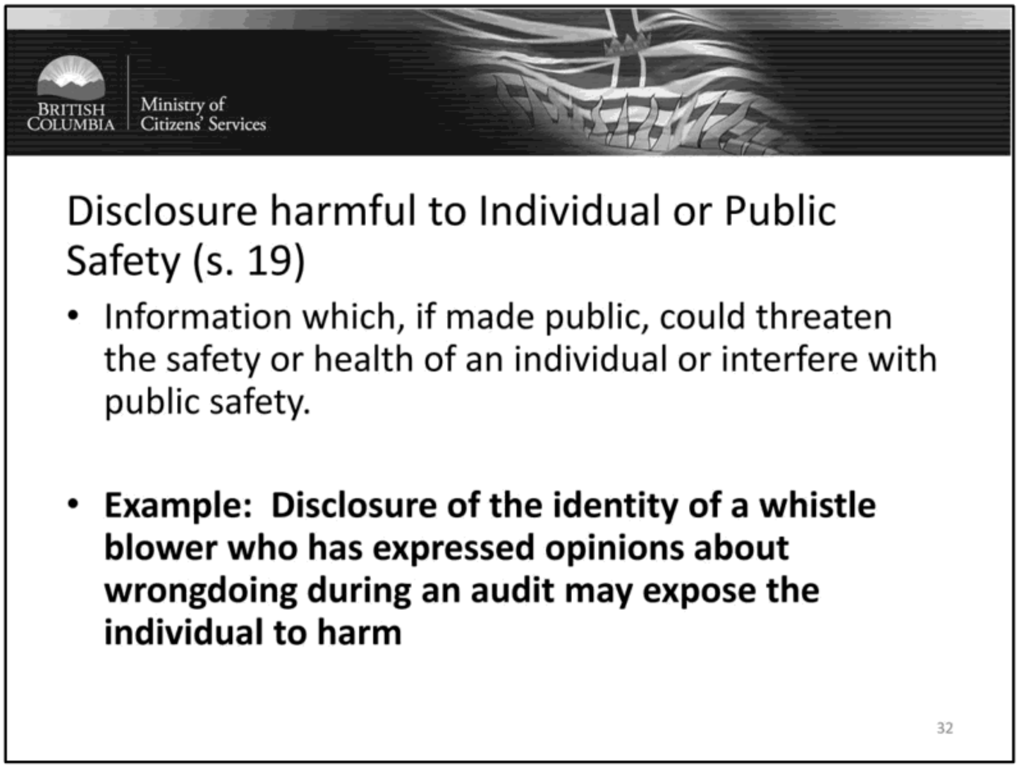
Disclosure harmful to Economic/Financial Interests of a Public Body (s.17)

- Information which could harm the economic, financial, competitive or negotiating interests of the British Columbia government or one of its public bodies
- Includes plans, negotiations etc... of a public body that have not yet been implemented or made public
- Can work in concert with section 16 and section 21
- **Example: Internal cost estimates – revealing what the government is willing to pay for a particular service**

The alleged harm must not be fanciful, imaginary or contrived but rather one which is based on reason.

e.g. public body trade secrets – financial and/or technical information – internal cost estimates – revealing what the government is willing to pay for a particular service

e.g., softwood lumber agreement method re: negotiations from a coalition group
e.g., compensation for turning land into parks, a mill is going to close



BRITISH COLUMBIA | Ministry of Citizens' Services

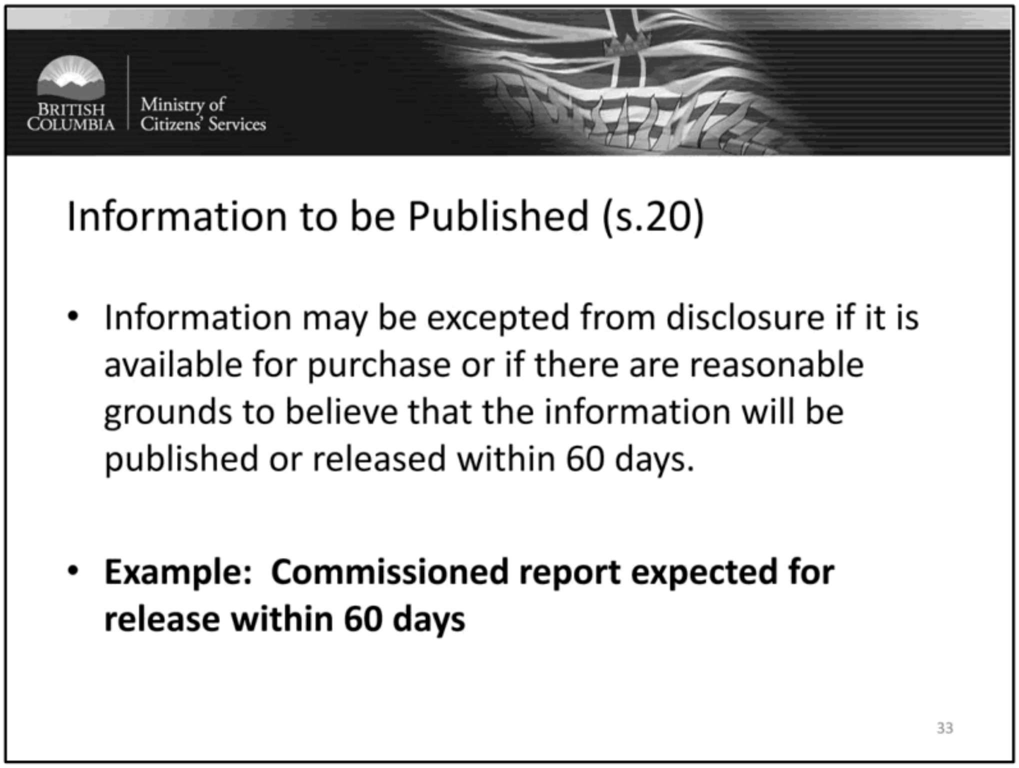
Disclosure harmful to Individual or Public Safety (s. 19)

- Information which, if made public, could threaten the safety or health of an individual or interfere with public safety.

- **Example: Disclosure of the identity of a whistle blower who has expressed opinions about wrongdoing during an audit may expose the individual to harm**

This may even include the applicants own information For example – if a psychiatric evaluation, stating that the applicant was a high risk for suicide, was released to the individual it could push them over the edge. Or Harrassment cases would be an area where section 19 would apply. - letter written by staff about hostile client - may be withheld from client to protect safety of staff.

•E.g., in MFOR, ‘trapper’ names are not released because of animal rights activists

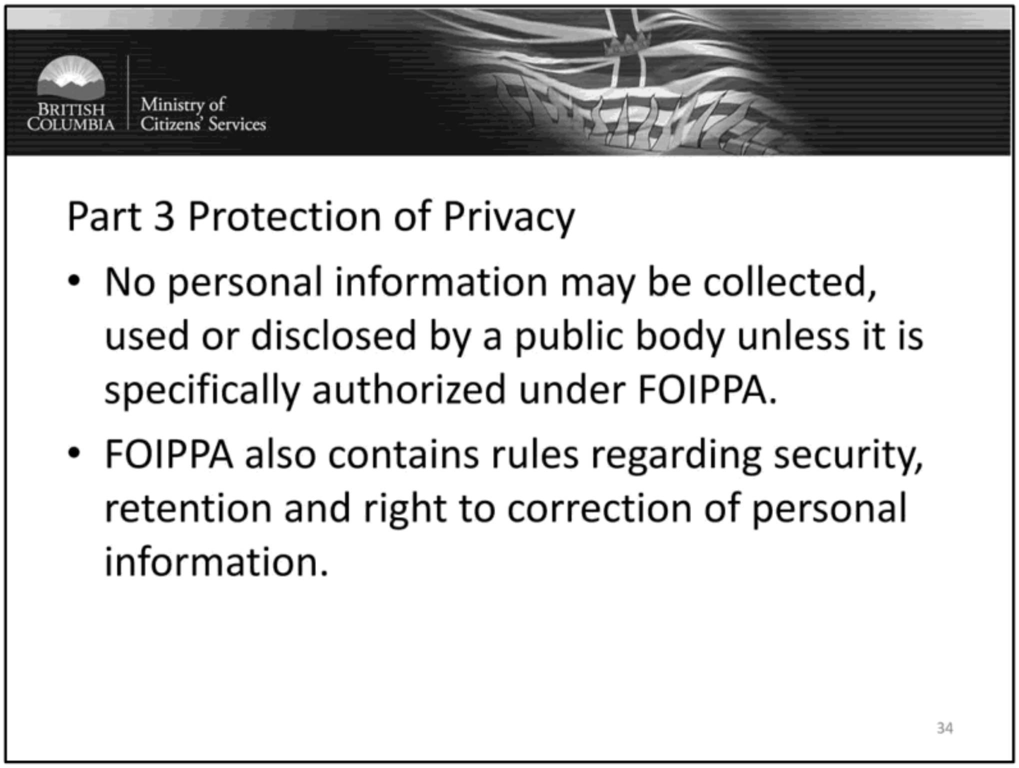


British Columbia | Ministry of Citizens' Services

Information to be Published (s.20)

- Information may be excepted from disclosure if it is available for purchase or if there are reasonable grounds to believe that the information will be published or released within 60 days.

- **Example: Commissioned report expected for release within 60 days**



BRITISH COLUMBIA | Ministry of Citizens' Services

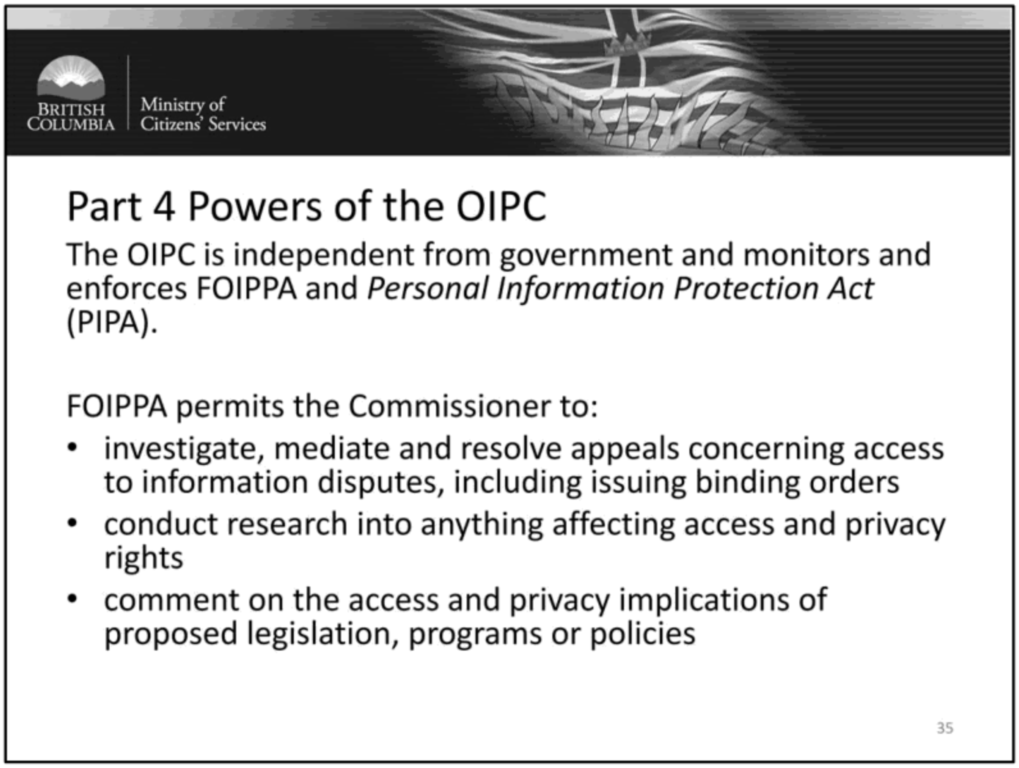
Part 3 Protection of Privacy

- No personal information may be collected, used or disclosed by a public body unless it is specifically authorized under FOIPPA.
- FOIPPA also contains rules regarding security, retention and right to correction of personal information.

34

When collecting personal information a public body must inform the individual why they are collecting it, their legal authority to collect it, and the name and contact information of an officer if they have questions. Usually see a disclaimer on form.

A public body many not use the collected personal information for anything other than the stated purpose. Public body may not sell personal information to a third party.



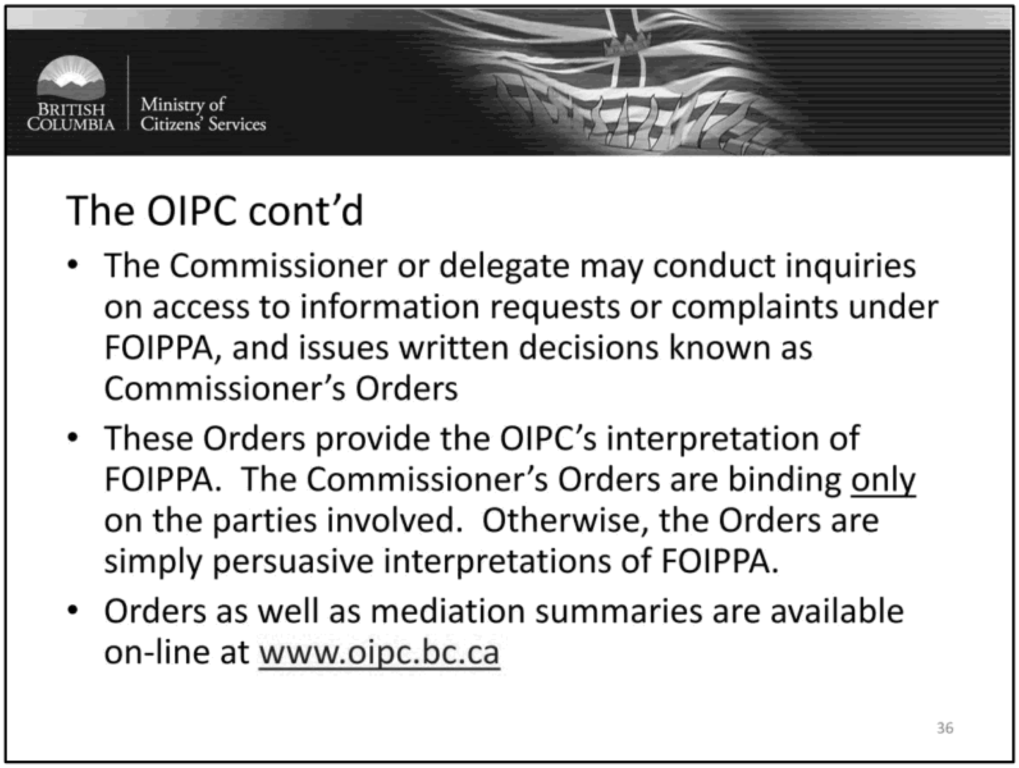
BRITISH COLUMBIA | Ministry of Citizens' Services

Part 4 Powers of the OIPC

The OIPC is independent from government and monitors and enforces FOIPPA and *Personal Information Protection Act* (PIPA).

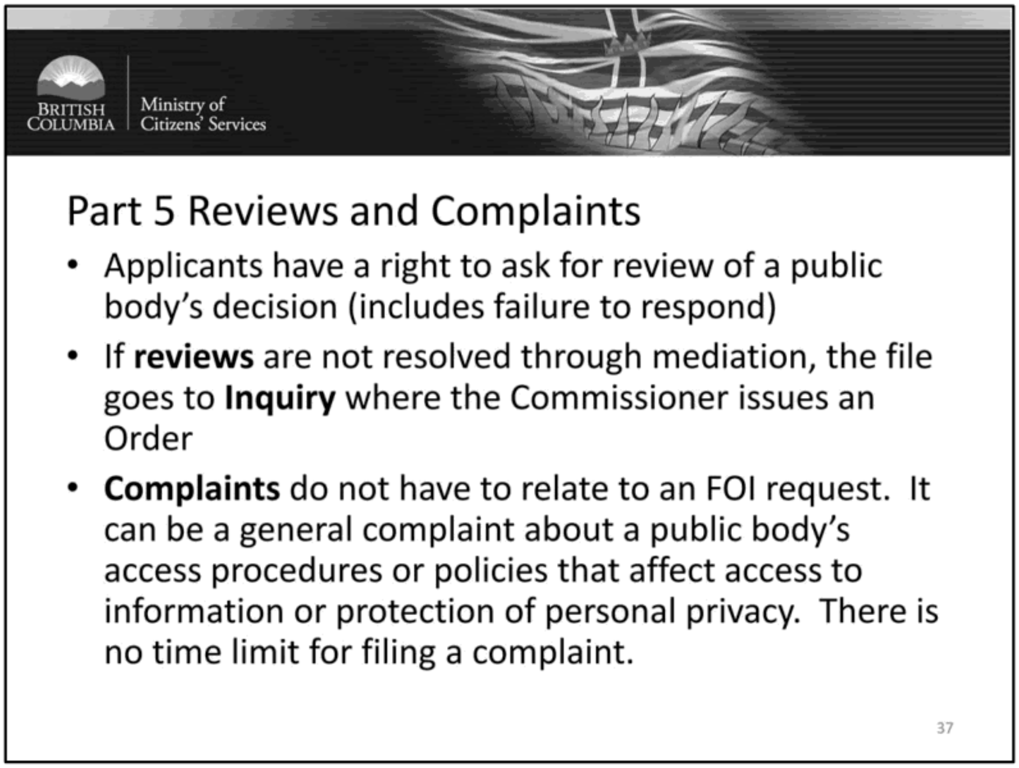
FOIPPA permits the Commissioner to:

- investigate, mediate and resolve appeals concerning access to information disputes, including issuing binding orders
- conduct research into anything affecting access and privacy rights
- comment on the access and privacy implications of proposed legislation, programs or policies



The OIPC cont'd

- The Commissioner or delegate may conduct inquiries on access to information requests or complaints under FOIPPA, and issues written decisions known as Commissioner's Orders
- These Orders provide the OIPC's interpretation of FOIPPA. The Commissioner's Orders are binding only on the parties involved. Otherwise, the Orders are simply persuasive interpretations of FOIPPA.
- Orders as well as mediation summaries are available on-line at www.oipc.bc.ca



BRITISH COLUMBIA | Ministry of Citizens' Services

Part 5 Reviews and Complaints

- Applicants have a right to ask for review of a public body's decision (includes failure to respond)
- If **reviews** are not resolved through mediation, the file goes to **Inquiry** where the Commissioner issues an Order
- **Complaints** do not have to relate to an FOI request. It can be a general complaint about a public body's access procedures or policies that affect access to information or protection of personal privacy. There is no time limit for filing a complaint.