

Employee Privacy Training Records



Where ideas work

Report Date: 2018-10-31

Organization	REQUIRED COURSE	ATTENDANCE	GRAND TOTAL
BC Government - Ministries	Level 117	Completed	26473
		Enrolled	407
		Unregistered	2321
		Level 117 Total	29195
	GRAND TOTAL		29195

Learn more about what this report means, including HR data definitions, visit the [HR Analytics Wiki](#).

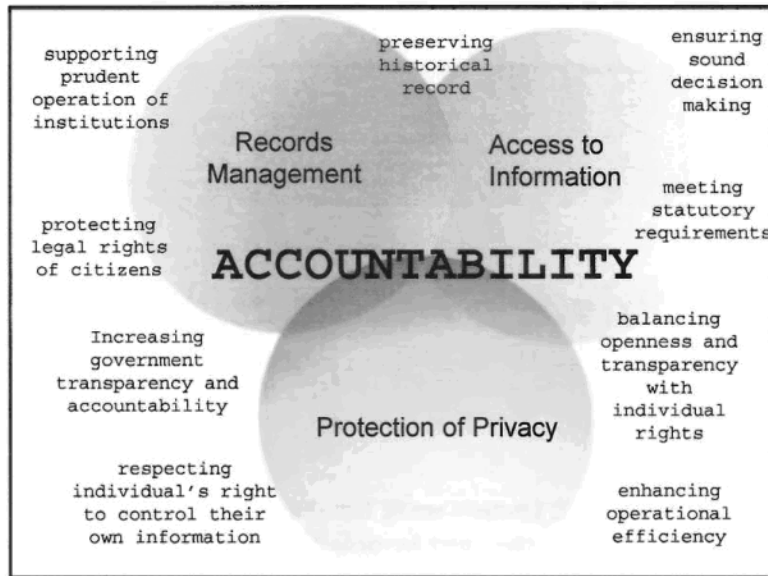
Download the detailed report by selecting the *Export option* on the *Actions* menu above the report title.



Ministry of
Citizens' Services

Privacy, Access and Records Management For Executives

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



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?

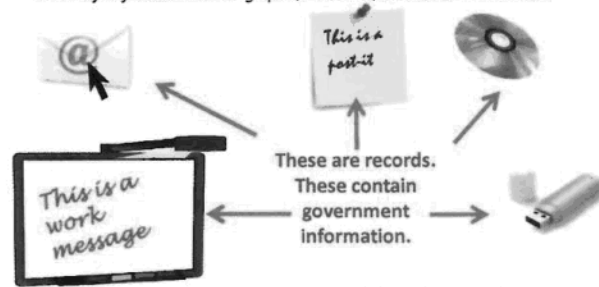
- Privacy principles

10

11

"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"



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



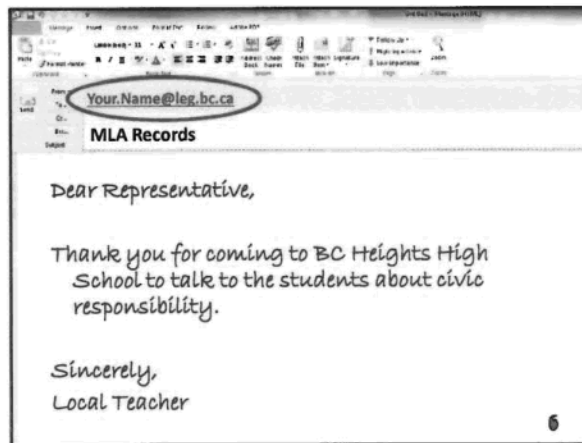
Types of Records

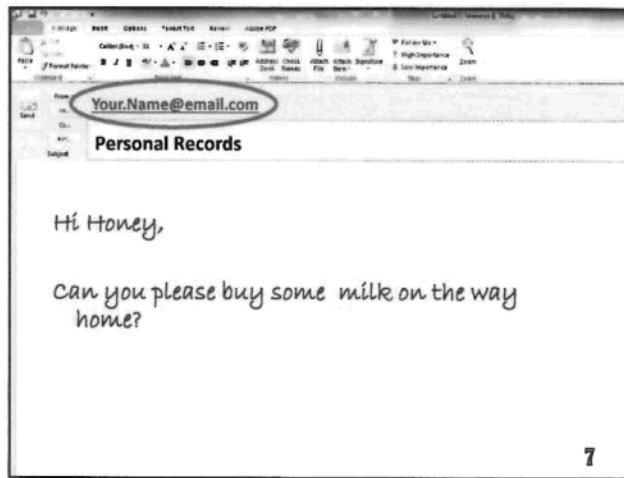
Types of Records in Minister's Offices

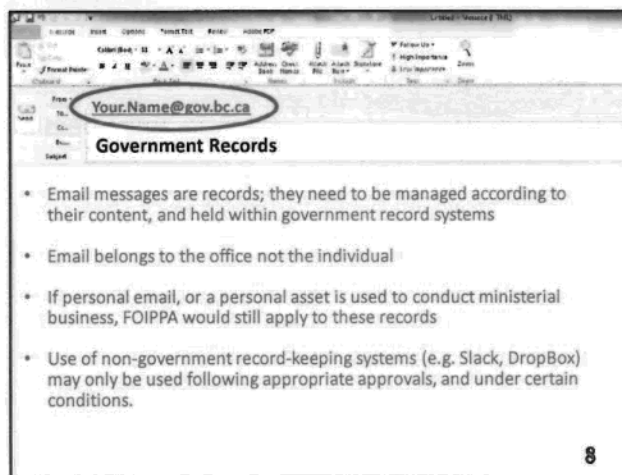
Three main types of records:

1. **MLA** (non-government – e.g. constituency, caucus, etc.)
2. **Personal** (non-government)
3. **Government information** (Ministry business, Cabinet, administrative, etc.)

5







December 27, 2016

27 **Calendars** Tuesday

8 am

9⁰⁰

10⁰⁰

11⁰⁰

12 pm

1⁰⁰

2⁰⁰

3⁰⁰

4⁰⁰

5⁰⁰

6⁰⁰

Previous Appointment

- 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

9

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

10



Ministère de la
Gouvernement du Canada



tran·si·to·ry

/ˈtrænzɪˈtɔːri, ˈtrænzɪˈtɔːri/

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

11

“

**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

Clearly Transitory

— Redundant Information

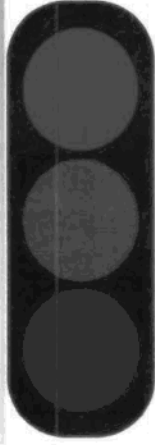
- Convenience copies, email superseded by later email in a string of messages, the received copies of a message received by a large audience, procedural emails that result in an official record being filed

— 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.

13


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

14



Using Your Judgement



- Does the record document substantive activities, decisions and/or the decision making process of the 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?

15

Freedom of Information



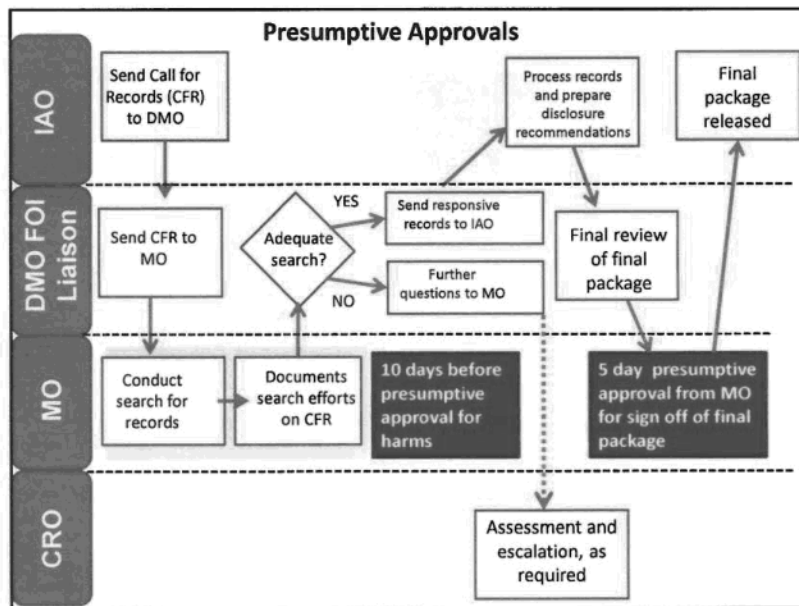
16



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

17





Proactive Disclosure

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



Open Information

“

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

- Gartner



BRITISH
COLUMBIA

Ministry of
Citizens' Services



Guiding Principles to Managing Sensitive or Confidential Information

- | | |
|--------------------------|---|
| Right Information | ➤ Managed based on the "need to know" and least privilege principles |
| Right Person | ➤ Access only to the minimum amount of personal information required to perform employment duties |
| Right Purpose | |
| Right Time | ➤ Access permissions should be assigned consistently and kept up to date |
| Right Way | |

21



BRITISH
COLUMBIA

Ministry of
Citizens Services

Information Incidents

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

22

“

...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



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

24



Ministry of
Citizens' Services





BRITISH
COLUMBIA

Ministry of
Citizens' Services

Supplemental Use Cases

26

USE CASE # 1: "What devices should I use in my role as a Government Official (and MLA)?"



Phone

1. Two phones: Government phone and a MLA phone (Recommended)
 - Any alternative arrangement must include a Government phone.

Computers and/or Tablets

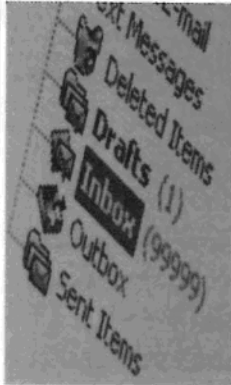
1. Two Computers: Government Computer and MLA Computer (Recommended)
 - Any alternative arrangement must ensure that documents are only accessed/stored on the appropriate respective systems (e.g. only access gov't records via VPN/DTS; don't store MLA documents on gov't device)

USE CASE # 2: "How do I compose and direct emails more effectively?"



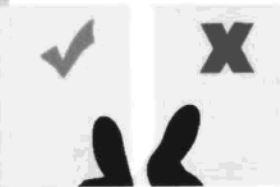
- Use descriptive subject descriptions
- Identify priority actions in the Subject Line (e.g. Urgent; For Action)
- Keep emails to a single topic where possible
- Assess the full email thread and subject heading before forwarding or responding
- Carefully define audiences between "To" and "CC" (general awareness no action required)

USE CASE # 3: "How do I best manage the volume of emails I receive?"



- Review email workflows with your MAs and DMs to ensure communication is efficient (e.g. formal document approvals)
- Any delegation of email box records management to staff should use MS Outlook's privileges
- Make classifying, filing and clearing emails part of your day
- Use folders to stay organized
 - A simple method is to establish a 'Retain Folder' for non-transitory records prior to filing in the official record keeping system
- Handle each email as few times as possible
 - When opening email: Deal with it; Delegate it or Delete it (consistent with information schedules)

USE CASE # 4: "My constituents and stakeholders don't distinguish between my roles as a Government Official and Elected Official and reach out directly through a variety of communications channels."



Best Practice – Government Role:

- Don't reply from non-govt account
- Forward to govt account to reply – if appropriate
- Avoid using other communications channels
- Be aware some communications tools are not compliant with policy and legislation
- Contact your DMO for information on the use of non-standard government tools

30

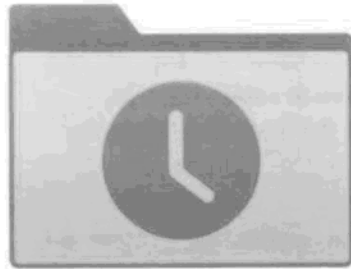
USE CASE # 5: "I've given most of my records to my DMO, now what?"



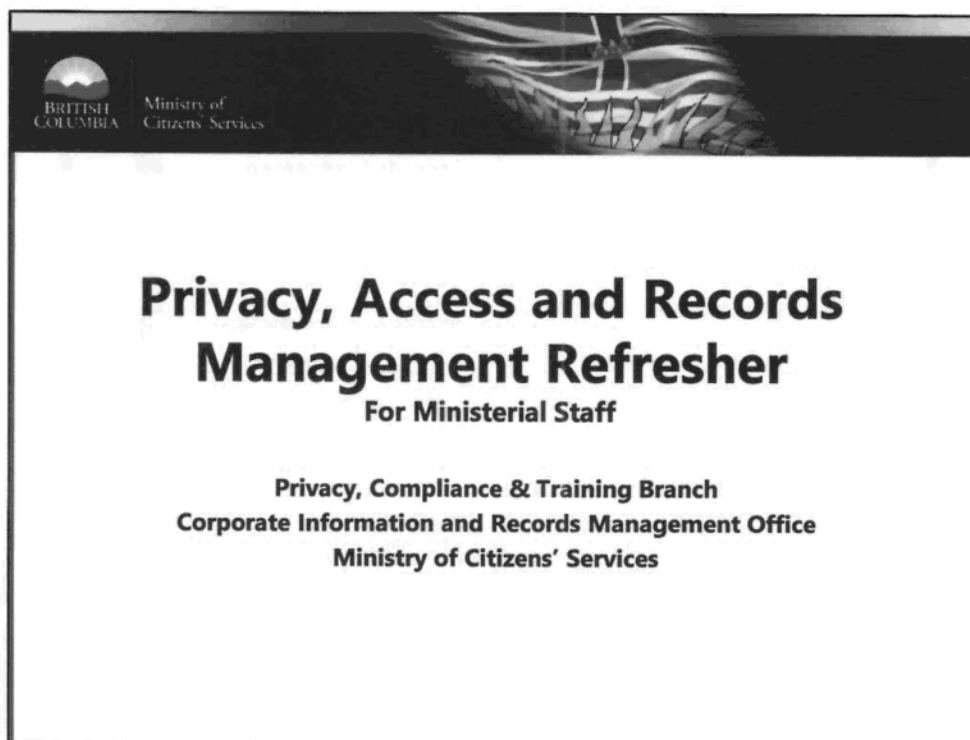
- Majority of records processed in an MO will eventually be retained by other offices
- In limited circumstances, the MO can expect to have to retain records, according to the Executive Records Schedule
- When you are not the OPR – the duty to assist is about connecting a requester with the records
- Document and communicate where records are routinely retained

31

USE CASE # 6: "I'm managing records on an initiative I just completed, how do I know which files are transitory?"



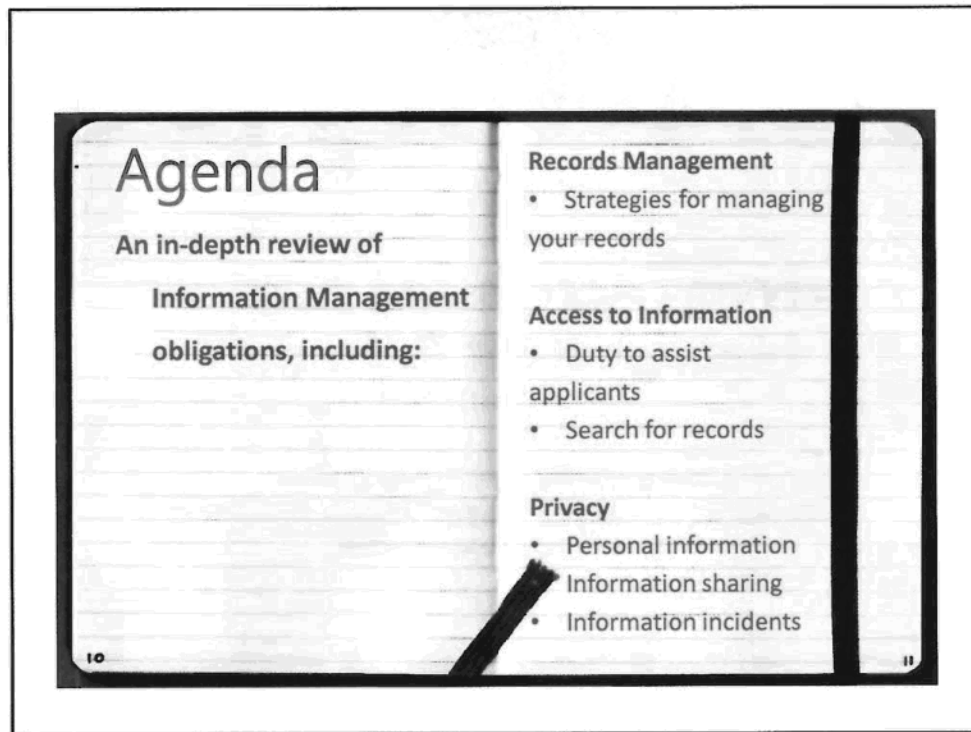
- Conduct the assessment discussed previously (red/yellow/green).
- Validate "yellow" records with someone else.
- Assess whether the remaining records represents a complete picture of the initiative – including its genesis, approval, funding, significant changes, and completion.
- If you are unsure, contact your DMO for referral to your Ministry Records Officer



Good morning/good afternoon. [personal introduction].

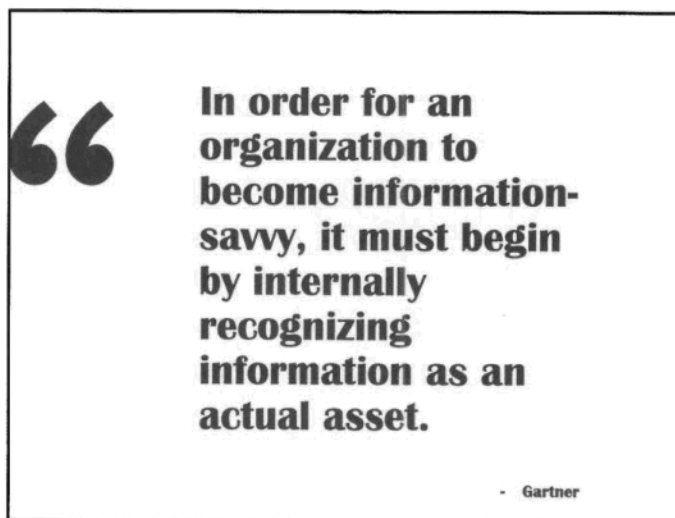
I am here representing the Corporate Information and Records Management Office, or CIRMO for short. This is the division that is responsible for **information management** in government. CIRMO was established in December 2015 to consolidate government's critical information management functions in order 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.

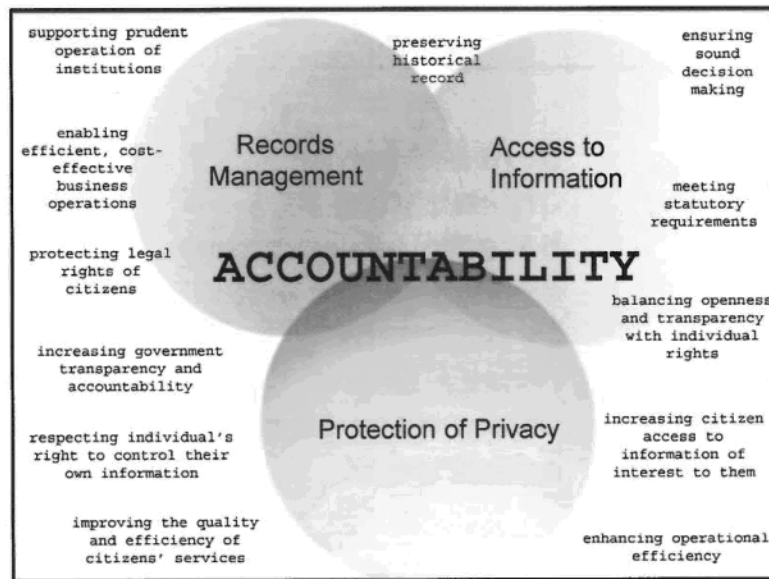


We are here today to get a bit of a refresher on our information management requirements and introduce new practices and controls that will improve information management practices and accountability. You have all received training on access, **or** said another way, on FOI - and you have all taken training 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**.

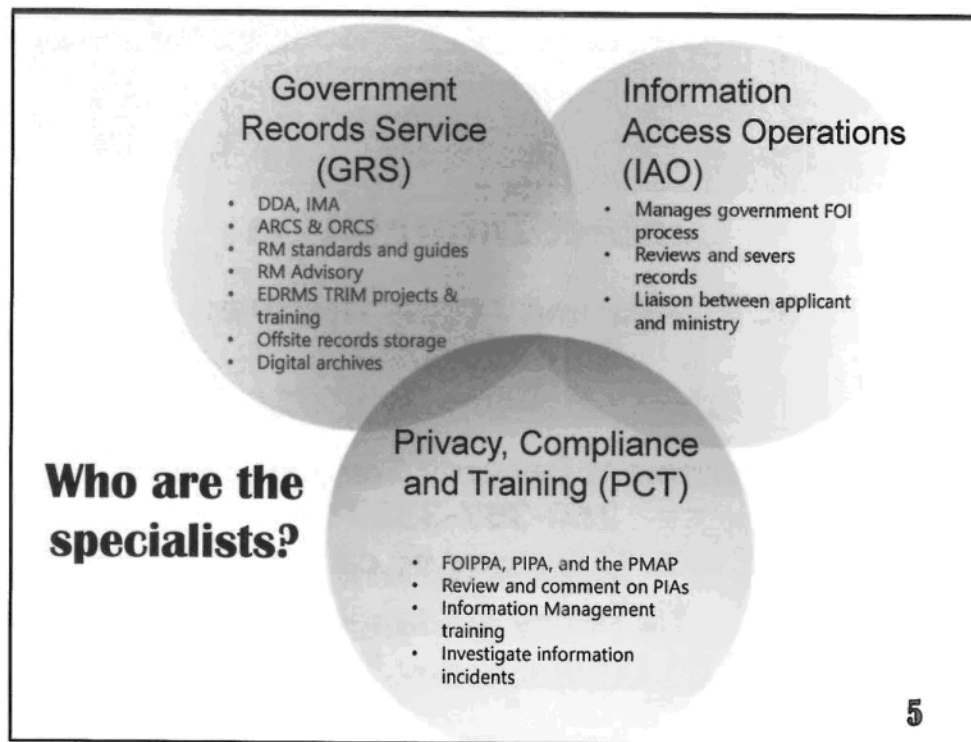


- We in the Ministry of Citizens' Services often speak of extending the culture that currently exists around protecting our physical or financial assets to the informational resources we have in government. The measures that are in place to monitor the expenditure of dollars, as an example, are extensive.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



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



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.



Contact Information

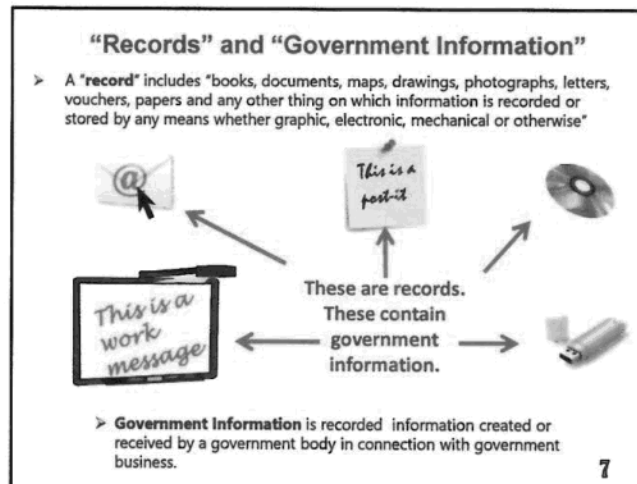
BC Privacy and Access Helpline:
250-356-1851
Privacy.Helpline@gov.bc.ca

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

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

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, 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.



- 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:

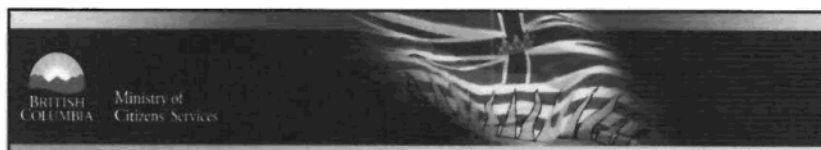
- A. TEXT MESSAGES
- B. LYNC MESSAGES
- C. STICKY NOTES
- D. HAND DELIVERED HARD COPIES
- E. ALL OF THE ABOVE

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.



Types of Records

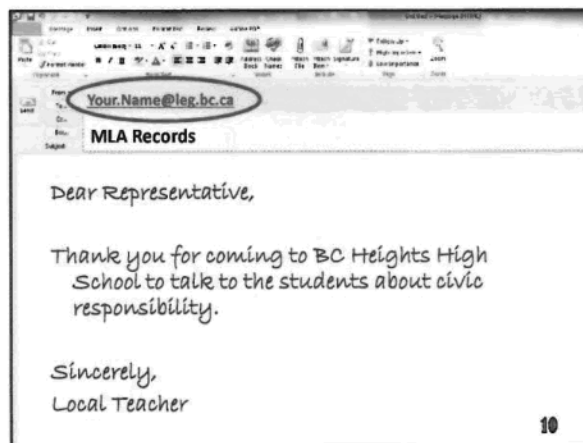
Types of Records in Minister's Offices

Three main types of records:

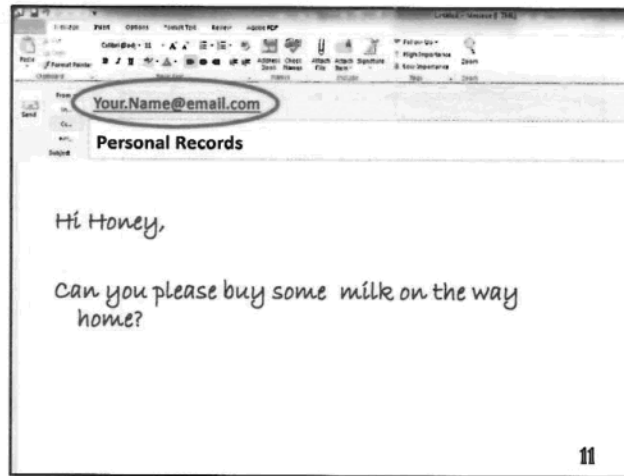
1. MLA (non-government – e.g. constituency, caucus, etc.)
2. Personal (non-government)
3. Government information (Ministry business, Cabinet, administrative, etc.)

9

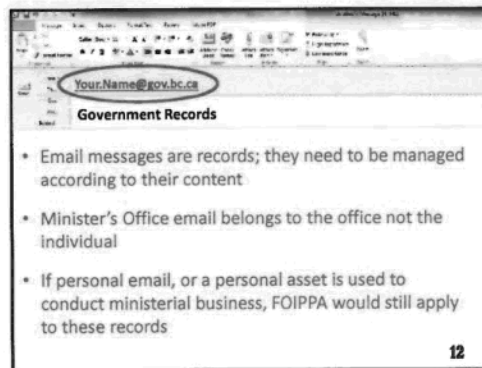
- In order to best understand our records management and access obligations we need to review the different types of record that your offices hold.
- In a Minister's Office there are three main types of records that you will deal with. I'm going to go into the details for each of these separately, but 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.



- 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.



- 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.



- 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.

The first 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.



Cabinet Submission - Request for Decision

Minister:

Ministry:

Date:

Title:

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).

13

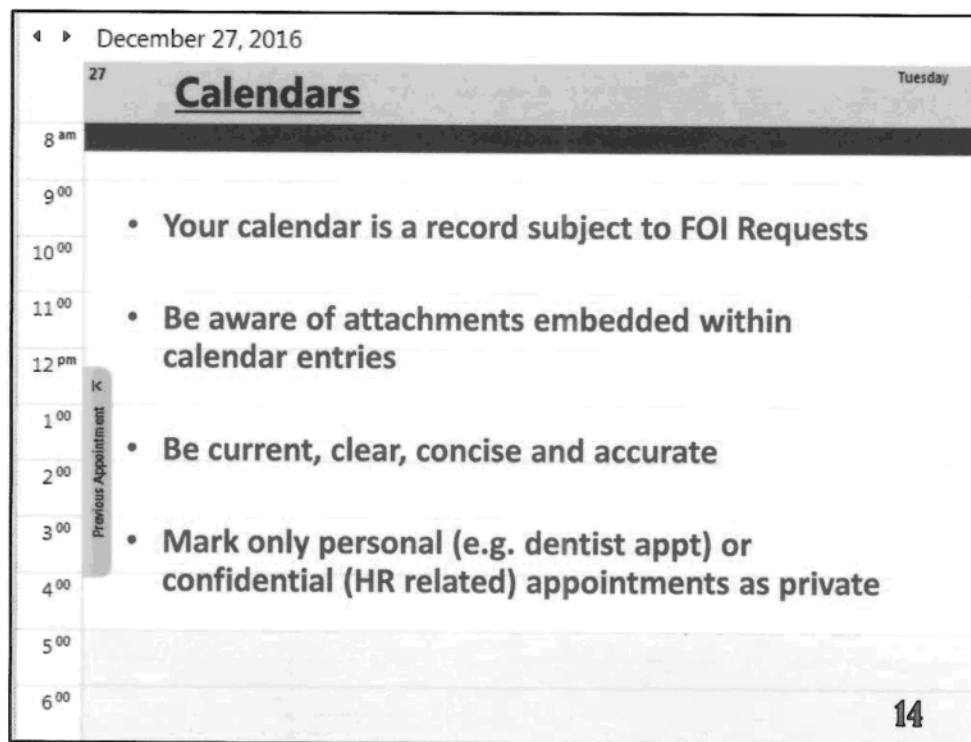
While we have spoke about how Cabinet records from previous administrations are treated, we must also speak about how Cabinet records created by the new government should be managed.

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.



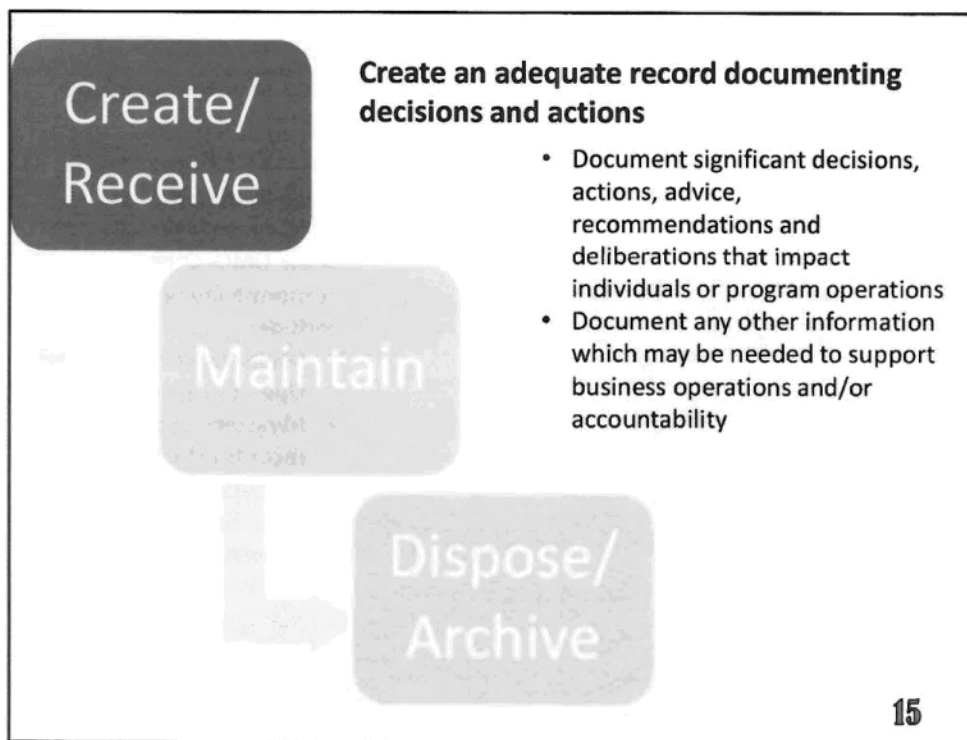
The final records example I wanted to highlight is Outlook calendars. As you may know, A Ministerial Directive under FOIPPA requires the monthly disclosure of calendars of Minister, Deputy Ministers, Associate Deputies, and Ministers of State. To facilitate consistency and ensure security in making these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

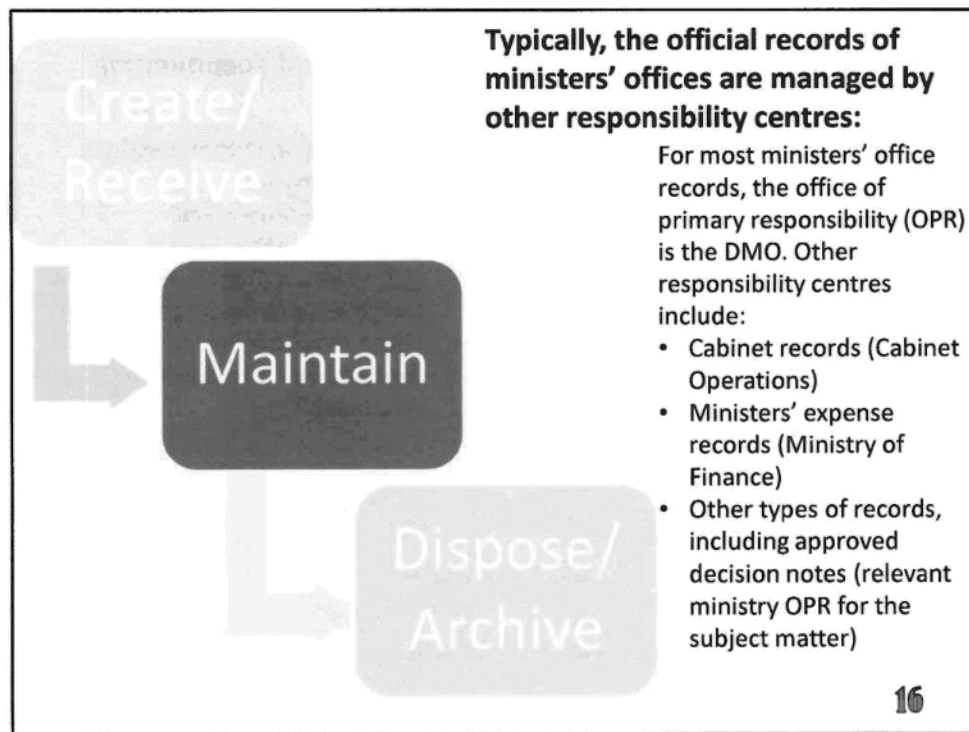


Now it's time to talk about what to do with government information, from the beginning to the end of its lifecycle. The lifecycle of government information is simple - information is created or received, you use and maintain it, and then the information is either disposed of or sent to the government 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.



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.

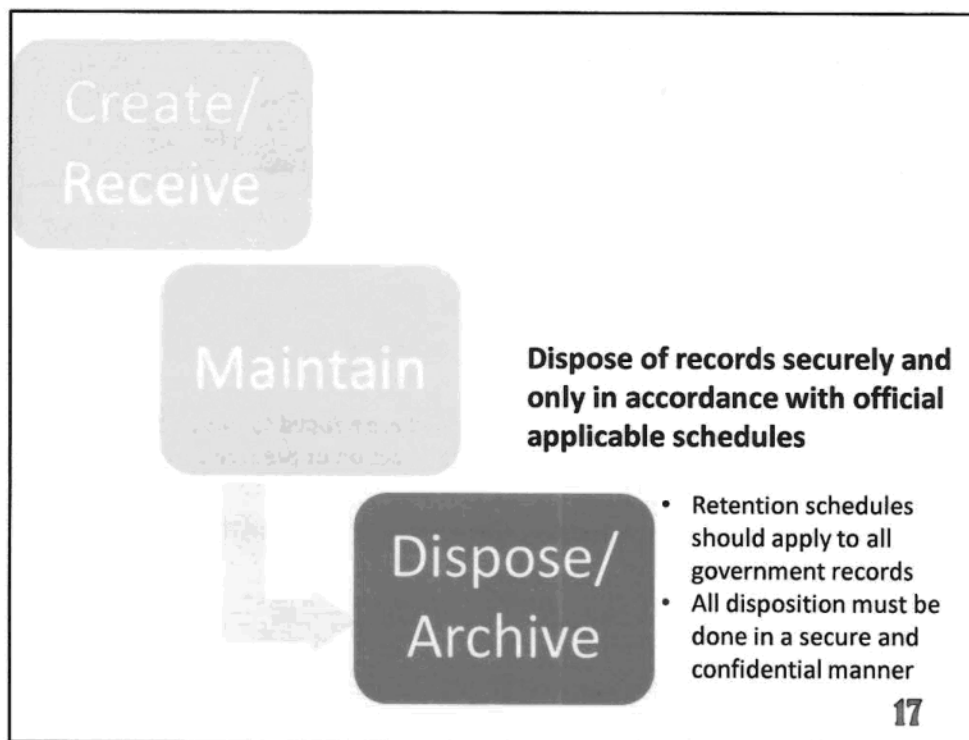
Your office may also use other information systems for recordkeeping. This is fine, as long as they have appropriate information management controls, including use of information schedules. These schedules specify how long each category of information must be kept. Within the office recordkeeping system 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.

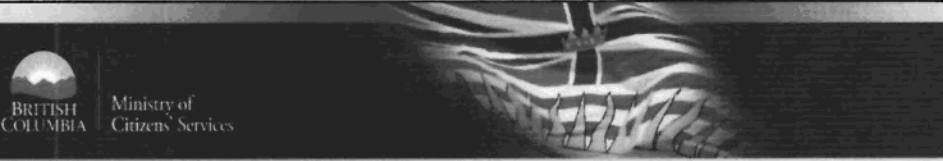


So, now that we know with whom and where records are maintained, we can talk about disposition. Information schedules provide timetables which tell us how long different types of information is needed and when the information may be disposed of or sent to the government archives.

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.



tran·si·to·ry
 /ˈtrænzəˌtɔːrē, ˈtranzəˌtɔːrē/
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

18

- 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**

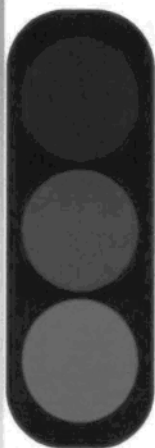
- Elizabeth Denham,
Information & Privacy
Commissioner

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



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.

21

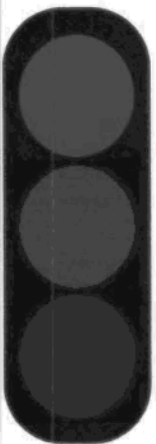
- So, how does your office determine if something is transitory? I am going to walk you through some examples to try to illustrate the decision making process in the context of the records that are produced in a Ministerial office.
- Duplicated information is a good example of what can be transitory. 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 **22**

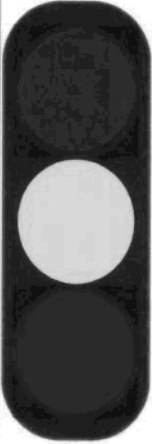
- On the other end of the spectrum, there are those records that are clearly **not** transitory.
- Information that is clearly not transitory would include incoming public correspondence, meeting minutes, and case files. You may, however, have copies of information such as meeting minutes that are transitory, 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?

23

- 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.



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

24

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

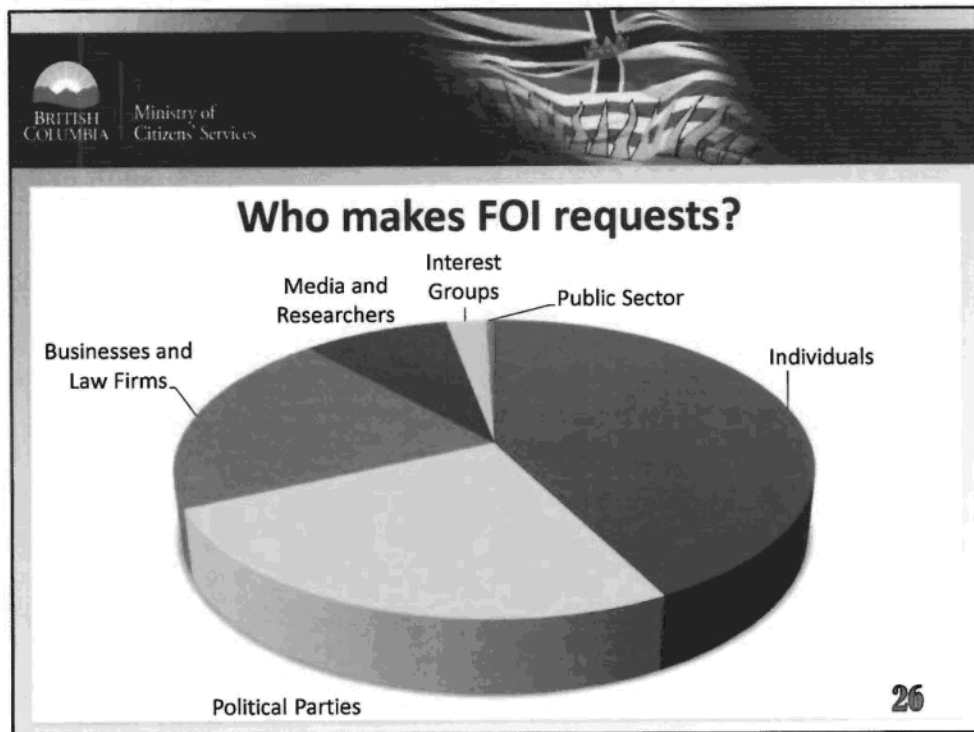
So why the focus on transitory records? We want to make sure that you are keeping the right records so that those records are available for accountability purposes. As the Commissioner recently said “Good governance and good record keeping go hand in hand”

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.



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.

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"**

27

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.

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**

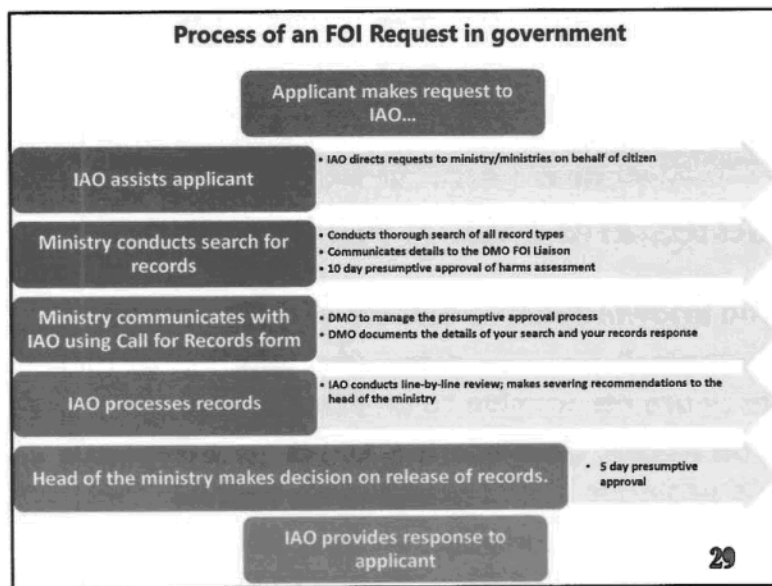
28

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.



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.



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."

31

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.



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

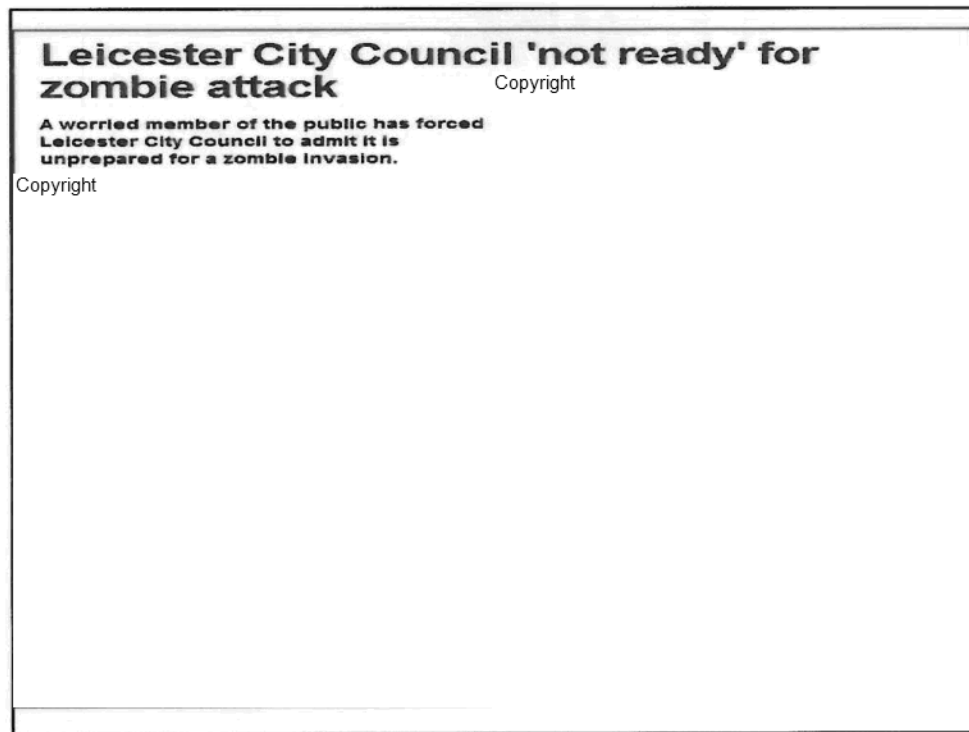
32

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.



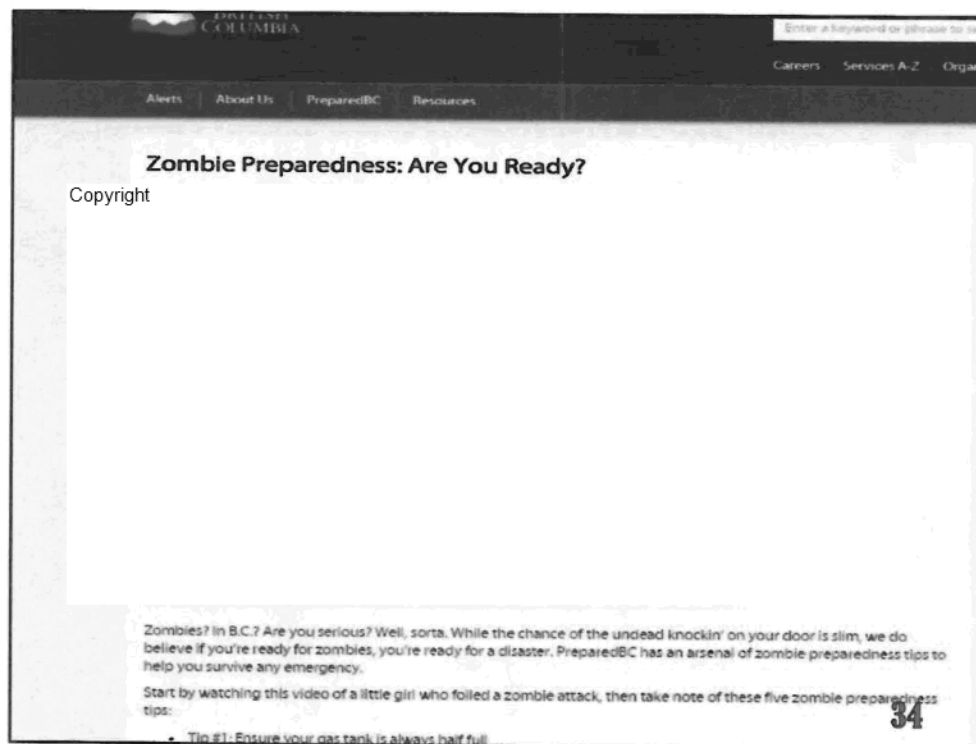
This is a real life example of an FOI request that demonstrates how we can exercise our duty to assist an FOI applicant.

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.



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

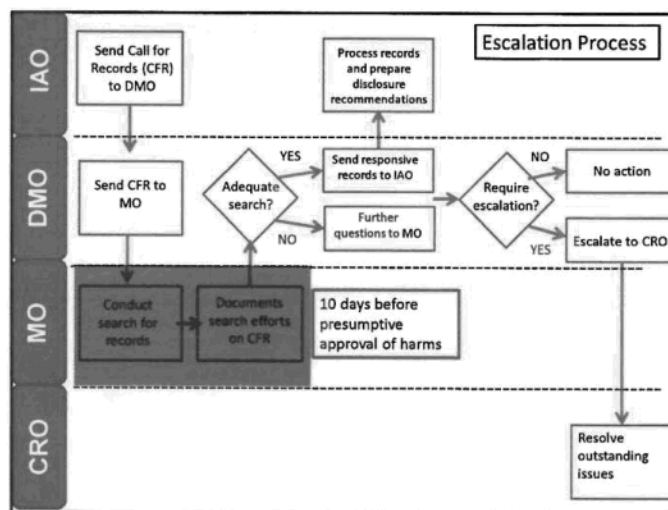
Read before quiz: One of the ways that we can **really demonstrate** that we are working to support applicants and meet our duty to assist is when it comes to searching for “responsive records”. “Responsive records” – when we’re talking about FOI - just means the records that respond to an FOI request.

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.



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.

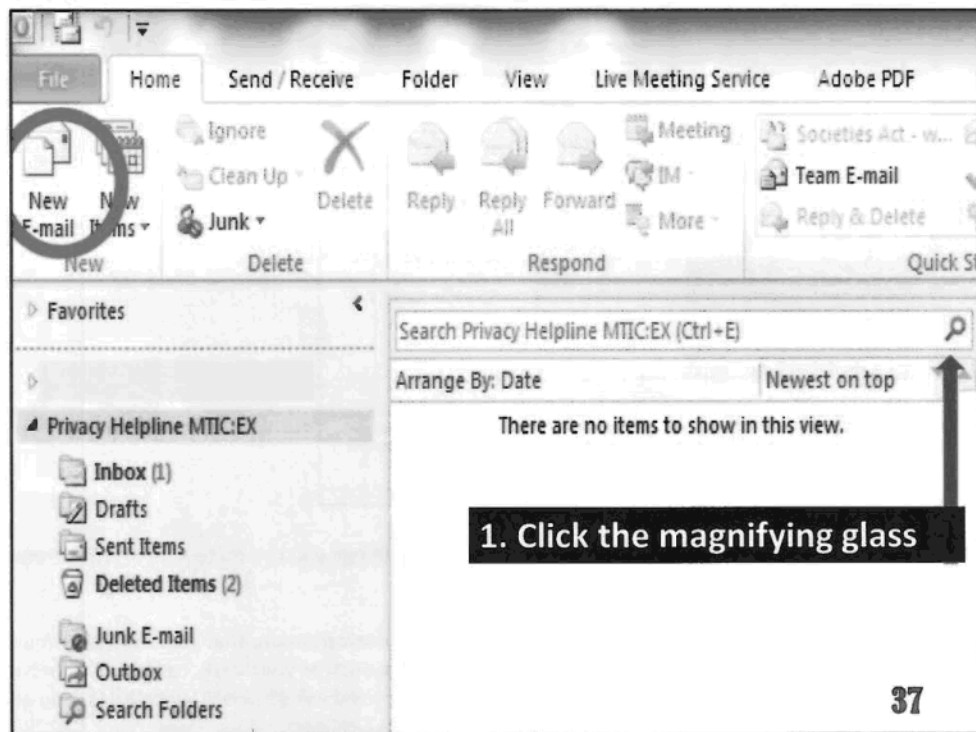
You are responsible for searching anywhere you or your office has stored recorded information, that includes your email, any SharePoint sites, your network drive, your electronic systems and devices and physical storage such as your desk, cabinet or notebook. You are the expert, you should **know** where 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.

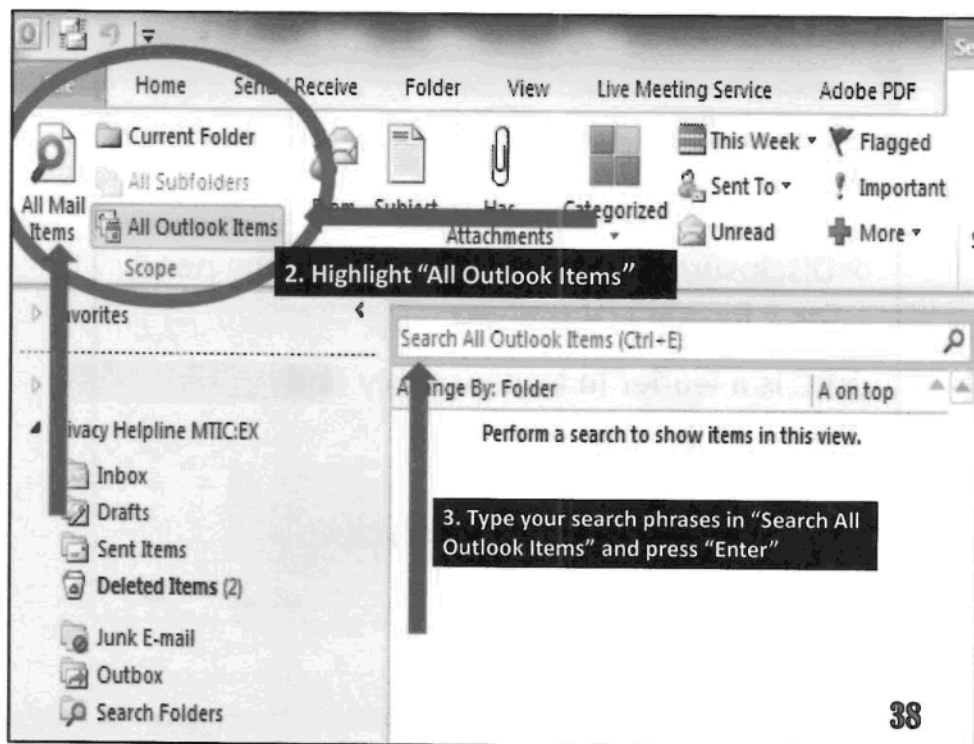


To help you get a leg up on an email search, I'm going to walk you through what a proper search in your Outlook folder should look like. To be clear, your email is only one place you need to search for records. But, I think this is a useful tip that not everyone necessarily knows about. It also demonstrates 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.




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.



Proactive Disclosure

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



Open Information

39

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, 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, Minister's receipted travel expense information, 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.



Proactive Disclosure – The Directives

Deadlines for Disclosure MUST be adhered to!

- Gaming Grants
- Calendars
- Directly Awarded Contracts
- Contracts > 10,000
- Open and Closed FOI Requests
- Travel Receipts
- Alternative Service Delivery Contracts

40

Under section 71.1 of the Act, Government has established several types of records that **MUST** be disclosed in accordance with the directives. These directives all have formal deadlines and compliance with them is mandatory. The Open Information Team at IAO is there to help you make sure your Ministry is in compliance with these deadlines.

Summaries of Gaming Grants are found in the Data BC catalogue, they are updated on a quarterly basis, and must be posted no later than 30 calendar days after the end of each quarter.

Ministers' and Deputy Ministers' calendars are found on the Open Information website. Calendars must be posted no later than 45 calendar days after the month in which they relate to.


Monthly Summaries of Directly Awarded Contracts are found on the Open Information Website. Directly Awarded Contracts must be posted no later than 60 calendar days after the month in which they relate to.

Summaries of Contracts over 10,000 dollars are found on the Open Information Website. These must be posted no later than 60 calendar days after the quarter in which they relate to.

For FOI Requests – there are two separate schedules and locations. Summaries of Closed FOI Requests are updated to Data BC on a quarterly basis, no later than 30 days after the quarter they relate. Summaries of Open FOI requests are updated on a weekly basis, and are found on the Open Information website.

Ministers' travel receipts and expense summaries are posted quarterly on the Open Information website, no later than 30 days after the end of the quarter. Deputy Ministers' expense summaries are posted on the second business day of the month, in the second month following the month the expenses relate to (ie: September expenses are posted second business day of November).

Summaries of Alternative Service Delivery Contracts are found on the Open Information website, and are updated on an annual basis, no later than 60 days after the end of the fiscal year they relate to.




BRITISH COLUMBIA
Ministry of
Citizens' Services

Proactive Disclosure

What are you responsible for?

- Minister's Calendar
- Minister's Quarterly Travel Expenses



Open Information

So now you might be asking – what do I have to do to make sure your Ministry is meeting your commitment to proactive disclosure?

For Minister's Offices, the two directives you will be most affected by are the Calendars, and the Quarterly Travel Expenses.

Calendars - At the start of every month, the Open Information team at IAO will send an email reminding all Ministries that their calendars are required to be provided to IAO no later than 10 calendar days after the month in which they relate (i.e. the Minister's September Calendar would be due to IAO no later than October 10th).

IAO processes these calendars for every Ministry, so your meeting these timelines are integral in ensuring there is adequate time to review each calendar to ensure each Ministry complies with the deadline for posting (45 days after the end of a calendar month).

IAO will send a copy with content that they believe should be removed – in other words, a "redline" - to the Ministry for review and approval. IAO strives to provide the redlined calendar to you to allow for adequate time to review - which is why meeting the deadline for records submission is so important!

Travel Expenses – Travel Expense summaries and receipts are posted quarterly, 30 days after the end of the quarter they relate to.

The Ministry of Finance compiles all travel expense summaries and receipts, and removes information from those records in accordance with their expense severing guidelines. The Ministry of Finance will submit these summaries to the MO for approval prior to submitting them to IAO for posting.

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

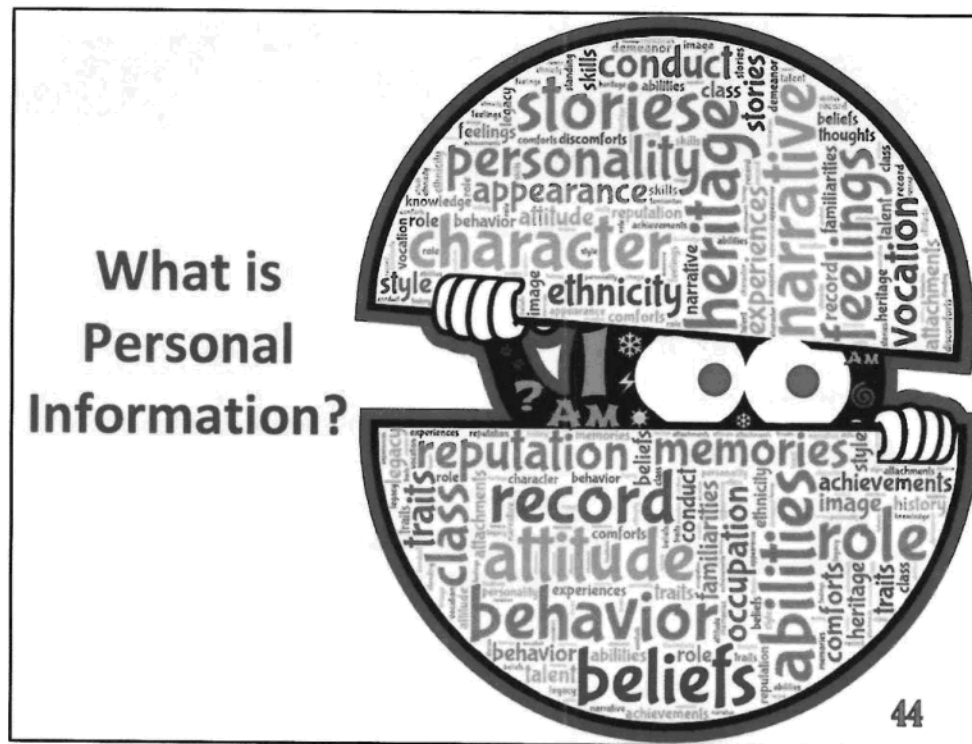
42

- 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.



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

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.

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.



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.

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.



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*

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!

48



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



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


Questions?




Ministry of
Citizens' Services




Supplemental Use Cases



BRITISH COLUMBIA
 Ministry of
 Citizens' Services



USE CASE # 1: "How do I compose and direct emails more effectively?"



- Use descriptive subject descriptions
- Identify priority actions in the Subject Line (e.g. Urgent; For Action)
- Keep emails to a single topic where possible
- Assess the full email thread and subject heading before forwarding or responding
- Carefully define audiences between "To" and "CC" (general awareness no action required)

54

There are a number of things that you can do to help keep your inbox under control.

It is important to treat inbox management as an everyday task.

Keeping emails to a single topic is important, particularly in the context of not mixing MLA, personal and government business into a single email. Records management is more straightforward when categories are separate, discrete and clear.

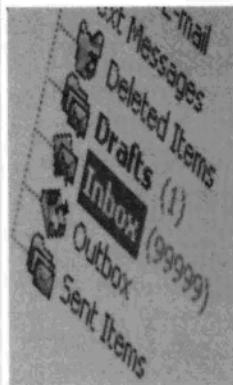
When you send an email, limit the main recipients to those who are expected to respond, take action, or make a decision. Use the cc' field for informational purposes only.

Use separate message chains for separate topics. Include clear and descriptive subject lines.

- You can make a habit of including in an email the necessary instructions for filing – for example – If you are replying to a question from the Minister about an approval – you could send to the Minister, and another MA, in an email that says "Minister, can you confirm your approval of XYZ action. MA is CC'ed to file confirmation under ABC program files"
- Also, use keywords to both support the searchability of emails, and to support filing of the emails too. If you think the email you are sending or expecting is going to be non-transitory, you can indicate in the subject heading or body of the email that the record should be retained.



USE CASE # 2: "How do I best manage the volume of emails I – or the Minister – receive? "



- Review email workflows between the Minister, MAs and DMs to ensure communication is efficient (e.g. formal document approvals)
- Any delegation of email box records management to staff should use MS Outlook's privileges
- Make classifying, filing and clearing emails part of your day
- Use folders to stay organized
 - A simple method is to establish a 'Retain Folder' for non-transitory records prior to filing in the official record keeping system
- Handle each email as few times as possible
 - When opening email: Deal with it; Delegate it or Delete it (consistent with information schedules)

55

There are a number of things that you can do to help keep your inbox under control.

It is important to treat inbox management as an everyday task. You need to make the classification, filing and clearing of emails a part of a normal work routine. If it is a monthly task, then it will be harder to do well. If you do it at the end of each day, the importance of each item will be fresh in your mind.

Folders are another great way to keep organized. Here are two different examples of how you could use folders:

Example 1:

- Create 2 folders (Retain from Inbox; Retain from Sent Mail); file accordingly
- Anything left in Inbox should be transitory
- Permanently file all emails in both folders. Contact Ministry Records Officer to support establishing records structure.

Example 2:

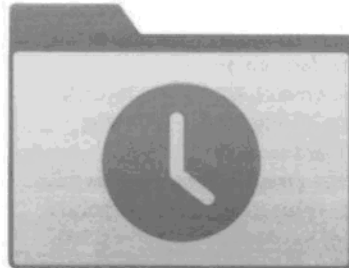
- Contact Ministry Records Officer to support establishing records structure
- Actively file any official records/emails into inbox folders and/or the LAN

In Outlook, you can also create automatic rules that will keep thing uncluttered. For example, regular newsletters or TNOs can be set to go to specific folders to keep your inbox streamlined. Also, if there are routine workflows or processes through your office, you can route those emails into folders dedicated to those processes.

Handle each email as few times as possible. When you open it, decide whether you need to Deal with it, Delegate it, or Delete it.

When you send an email, limit the main recipients to those who are expected to respond, take action, or make a decision. Use the cc' field for informational purposes only.
Use separate message chains for separate topics. Include clear and descriptive subject lines.

USE CASE # 3: "I'm managing records on an initiative that just completed, how do I know which files are transitory?"



- Conduct the assessment discussed previously (red/yellow/green).
- Validate "yellow" records with someone else.
- Assess whether the remaining records represents a complete picture of the initiative – including its genesis, approval, funding, significant changes, and completion.
- If you are unsure, contact your DMO for referral to your Ministry Records Officer


56

When a file is nearing completion or conclusion, you should do an assessment of the records that you have on hand. Can you demonstrate the life cycle of that initiative through the records that your office holds? If not, do you know where that lifecycle of records is? If the answer to both of these questions is NO, then you need to re-assess what records are available, and who has them. The onus is on the public service to demonstrate accountability for the key actions and decisions of government. If you don't have an adequate record, you may want to consider keeping records that you would normally delete.

If you do not know who your Ministry Records Officer is, you should find out – through your DMO. Once you have this contact, you may want to invite the Records Officer to your office to speak specifically about the filing and records practices of your office. Each office is different and may have different processes, but you should walk through these processes with someone who can help you on the granular and detailed issues.

BRITISH COLUMBIA Ministry of Citizens' Services


USE CASE # 4: "I am interested in using an app on my government device"



- First consider default government services for these purposes (e.g. email, text, calendars, etc.).
- There are privacy, access and records management implications to using non-standard tools.
- Ensure that government processes have been met respecting implementation and use of tools (e.g. PIA, Appropriate Use, etc.).
- More restrictive internal policies can be set within work units or organizations.

57


- First consider default government services for these purposes (e.g. email, text, calendars, etc.).
- There are privacy, access and records management implications to using non-standard tools.
 - Make sure you check with the required offices to ensure you understand how a tool must be used in order to be compliant
- Ensure that government processes have been met respecting implementation and use of tools
 - e.g. PIA, Appropriate Use, etc.
- More restrictive internal policies can be set within work units or organizations.



BRITISH
COLUMBIA

Ministry of
Citizens' Services

USE CASE # 5: "What devices should a Minister use in their role as a Government Official (and MLA)?"



Phone

- Two phones: Government phone and a MLA phone (Recommended)
 - Any alternative arrangement must include a Government phone.


Computers and/or Tablets

- Two Computers: Government Computer and MLA Computer (Recommended)
 - Any alternative arrangement must ensure that documents are only accessed/stored on the appropriate respective systems (e.g. only access gov't records via VPN/DTS; don't store MLA documents on gov't device)

58



Additional notes:

- use of VPN/DTS and ensure access to government drives (e.g. LAN)
- Ensure that you do not have govt documents saved to the device, if you are only using one
- Currently there is no phone available that would allow for 2 SIM cards and would meet government information security requirements.
- May contact PremTech for assistance
- Two computers is an inconvenience, but it allows full access to respective systems and functionality in a reliable and secure manner.
- Sending emails to the correct email accounts actually supports more streamlined device usage as well. Although email is accessible (through a web browser) from other accounts, it is not as convenient. Thus, ensuring all mail is in the appropriate account means more efficient access from the appropriate device.
- It may be appropriate, if you have delegated access to email accounts, to ensure that messages are forwarded to the account that a response will come from (e.g. if someone emails the Minister (for constituency business) on their government account, that email should be forwarded to the Legislative account for response – from a Legislative device).



BRITISH COLUMBIA Ministry of Citizens' Services

USE CASE # 6: "Constituents and stakeholders don't distinguish between my Minister's roles as a Government Official and Elected Official and reach out directly through a variety of communications channels."

Best Practice – Government Role:

- Don't reply from non-govt account
- Forward to govt account to reply – if appropriate
- Avoid using other communications channels
- Be aware some communications tools are not compliant with policy and legislation
- Contact your DMO for information on the use of non-standard government tools

59

We can't control where people email or communicate with us – but we do control what we do with those messages after we receive them.

If communication relates to government business, you need to move it to a government record keeping system.

The first step is to not reply to any government email from another account. It is easy to simply reply; or reply and tell them to email you somewhere else – but the best practice is to forward the email to your government account *first* and then to reply to it. This will ensure that a) the original email is in a government record keeping system, and b) that response and subsequent emails are all in a government system too.

There are numerous communications tools that are available – and we would suggest that you use these with caution. Be aware that there are alternative tools that are not compliant with policy and legislation. Before using, or endorsing the use of any alternative tools within your office, you should have someone confirm with CIRMO that these tools are approved for use.

- Political staff need to support the Minister in their separation of devices and accounts
 - Acknowledge whether a meeting/consultation/correspondence/other communications are with "government stakeholders" or with "constituency stakeholders", as an example. Or that the Minister needs to sign a letter going out from the Minister, or from the Minister as MLA. Explicitly orienting interactions to the role the Minister holds at the time will support clear separation of accounts.
- For Sr. MAs – establish clear guidelines in the MO around expectations and communications. For example, you may choose to prohibit the use of alternative communications tools within the MO. These tools may be useful, however, it is far easier to manage records if they all exist within email and texting channels already approved for use. Prohibiting alternative channels reduces the number of venues you need to search for records, and demonstrates very clearly how compliance will be met and managed.

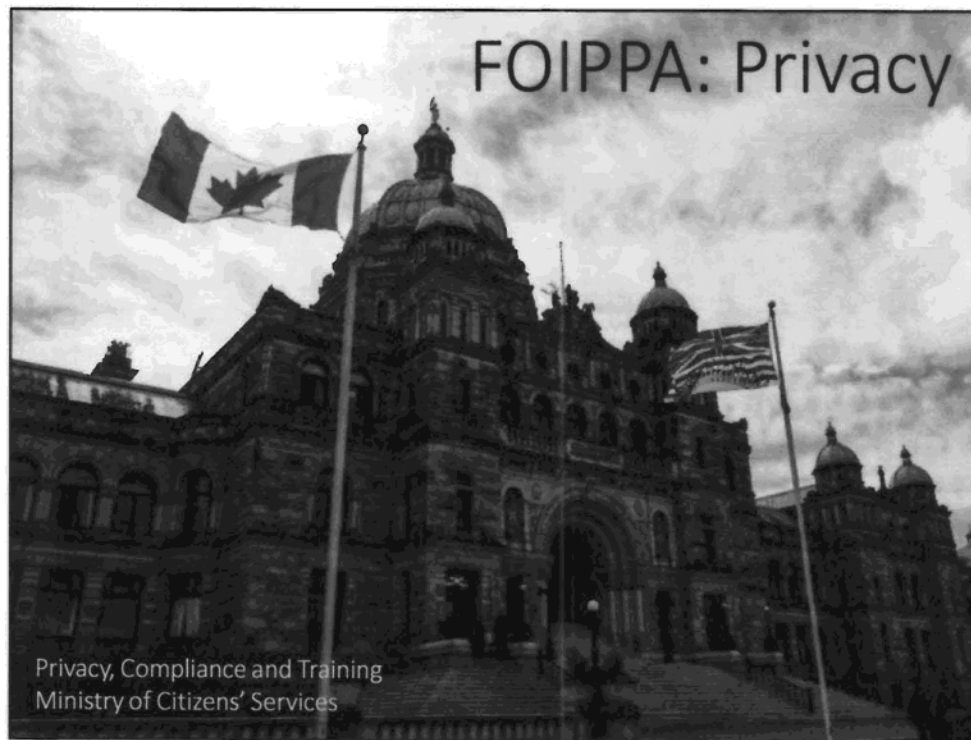
USE CASE # 7: "I've given most of the Minister's records to the DMO, now what?"



- Majority of records processed in an MO will eventually be retained by other offices
- In limited circumstances, the MO can expect to have to retain records, according to the Executive Records Schedule
- When you are not the OPR – the duty to assist is about connecting a requester with the records
- Document and communicate where records are routinely retained

60

Imagine that you are having to train a new staffer within your office. One of the things that would be most useful for them is a documented process around which records are kept, to whom are they given, and when are they sent. If you document your internal processes, this will a) support new staff, but, more importantly, will serve to ensure consistency and clarity within your office as to how records will be managed. If you send most/many of your records to the DMO, do you have that documented somewhere, so that if you win the lottery, the person who takes your place will a) know where past records are kept, and b) know where to send new records.



Welcome!

Intro

- Names

Housekeeping

- Mention where bathrooms are
- Mention that we'll take a morning break at around 10:30 and a lunch break at 12:00
- Mention that some of the content might be overlap from previous BCIP session
 - We are reviewing content that is valuable and worth repeating
 - Tell audience to provide in their feedback: if there are things you didn't need to hear again, please let us know
- If people attended the full day FOIPPA session in October in Victoria, they won't need to stay for this one

No program specific questions!

- Can use other resources – take it off line, email us (privacy helpline), call us (privacy helpline)
- Resources/links page at the end
- But do ask questions if you don't understand something or need some clarification
 - "It depends"

Bridge In

- Possible ideas:
 - Could take a copy of the act and say how you're going to make it applicable to people's jobs
 - Could talk about recent news on privacy (e.g. <https://theintercept.com/2018/06/27/immigration-families-dna-testing/>)



- Go over agenda

- For trainer:

Course description

The *Freedom of Information and Protection of Privacy Act* (FOIPPA) is a complex piece of legislation that governs privacy protection in over 2,900 B.C. public bodies. This course will help take the mystery out of Part 3 of FOIPPA, which covers collection, use and disclosure of personal information.

During this in person, 3-hour course, participants will learn the following:

- What personal information, including how to identify personal information through the mosaic effect;
- Collection, use and disclosure of personal information;
- Accuracy and correction of personal information;
- Data residency requirements; and
- Security requirements under FOIPPA.

Image source: https://cdn.pixabay.com/photo/2016/03/01/11/07/paper-1230086_960_720.jpg



PCT is government's
corporate privacy office.

PCT

Corporate Information and Records Management Office

Essentially, our branch = government's "corporate privacy branch"

- Experts on FOIPPA
- Lead strategic privacy initiatives across government
- Establish government policy, standards and guidelines on access and privacy issues
- Provide services, support and leadership to assist ministries and other public bodies in complying with FOIPPA
- Provide input and advice on legislative proposals and reviews
- Provide privacy training across the province

The importance of knowing who we are is knowing how we fit into a privacy management program.

Are we a support for you? Should we be? If you are within a ministry – do you understand our overall role within government?

-ask audience where they are from

-Public? Private?



OIPC

- established in 1993
- Commissioner (OIPC) provides independent oversight and enforcement of BC's access and privacy laws

Michael McAvoy is the Information and Privacy Commissioner

What OIPC does:

- Conducts reviews and investigations to ensure compliance with FOIPPA
- Mediates FOI disputes
- Comments on FOI and privacy implications of proposed legislative schemes or public body programs
- Provides useful resources regarding previous decisions/orders
- Where organizations outside the BC gov can go for help with PIAs
 - Ministries are required to come to PCT

-explain that OIPC can only be reactive if they aren't kept informed
-e.g. should consult with them on surveillance projects, projects dealing with vulnerable populations

Similar to our branch – how does the OIPC fit into a privacy management program?

They are obviously a regulator or watchdog for all of us (in BC), but for organizations not bound by FOIPPA, they also review PIAs, or answer routine questions from you.

Freedom of Information and Protection of Privacy Act (FOIPPA) Personal Information Protection Act (PIPA)

Personal Information Protection and Electronic Documents Act (PIPEDA) Access to Information Act Privacy Act

FOIPPA

- Public sector access and privacy legislation
- Applies to “public bodies” in BC

Before 1982

- No uniform rules on access to information and privacy

After 1982

- FOIPPA passed

- Perfects a private sector model of up from unauthorized collection, use and disclosure of personal information

- Has to cover all public bodies for all things
 - So isn't going to explicitly cover technologies like cloud
 - Covers huge number of public bodies

PIPA

- Private sector privacy legislation
- Applies to “organizations” (more than just businesses) in BC
 - e.g. non-profit organizations, charities
- “Common sense” rules for collection, use, disclosure of PI – consent-based
 - FOIPPA = authority based

PIPEDA

- Applies to federal works, undertakings or businesses
 - banks, airlines, and telecommunications companies
- PIPA BC specific

Canada's *Access to Information Act* and *Privacy Act*

- Federal equivalents to BC's FOIPPA
- Applies to Federal Gov't institutions and federally regulated institutions

What privacy legislation governs...

- the Ministry of Education?
- the corner mom and pop shop?
- a bank?
- a charity?
- the Blueberry Industry Development Council?
- you as a BC government worker?

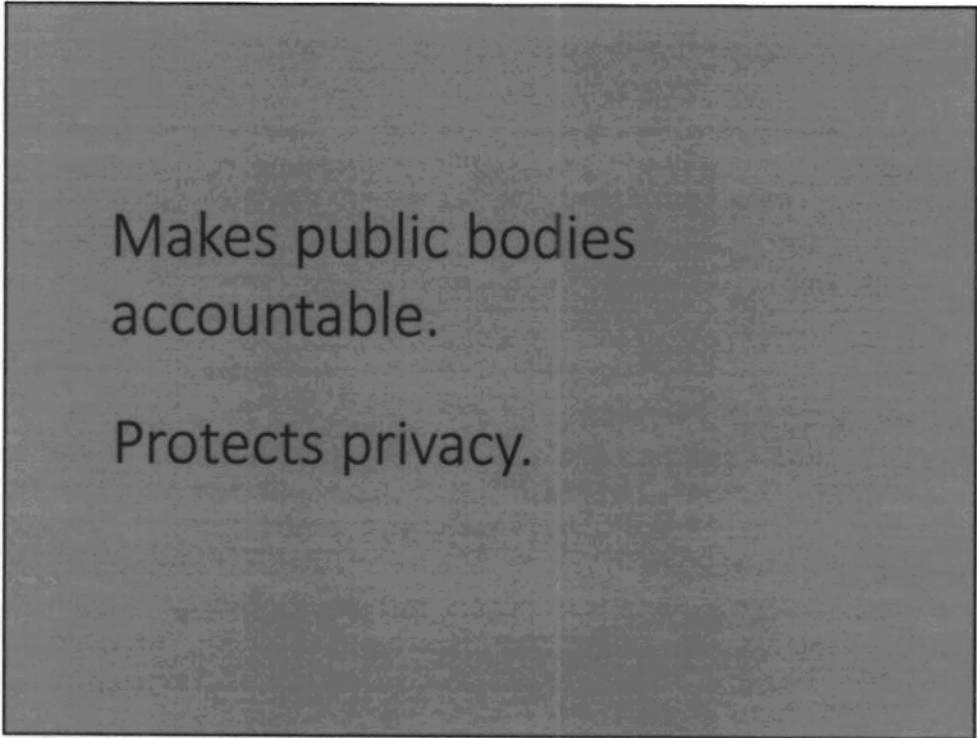
- Questions for audience:
 - What privacy legislation governs the Ministry of Education? (FOIPPA)
 - My corner mom and pop shop? (PIPA)
 - My bank? (PIPEDA)
 - The charity I donate to? (PIPA)
 - The Blueberry Industry Development Council? (FOIPPA – it's a Schedule 2 public body)
 - You as a gov worker?

Public bodies are governed by FOIPPA.

- Those that work for a public body, you are governed by FOIPPA
- FOIPPA applies to the public sector in BC
 - over 2,900 public bodies
 - Examples:
 - Ministries of the Province, Crown Corporations, Agencies, Boards, Commissions
 - Local public bodies
 - local government bodies, health care bodies, municipal police and educational bodies
 - Governing bodies of professional organizations
 - Examples:
Governing bodies of teachers, doctors, nurses, lawyers, engineers

Part 1 – Introductory Provisions
Part 2 – Freedom of Information
Part 3 – Protection of Privacy
Part 4 – Office and Powers of
Information and Privacy Commissioner
Part 5 – Reviews and Complaints
Part 6 – General Provisions
Schedule 1 – Definitions
Schedules 2 and 3 – List of public bodies

- We'll be covering Part 3 today
- Regarding the structure of FOIPPA
 - Organized into Parts and Divisions
 - Within each Division there are sections and subsections
 - Regarding the Schedules (read slide)
 - Schedules 2 and 3 don't provide exhaustive list
 - Entities such as the Blueberry Industry Development Council and the B.C. Raspberry Industry Development Council are included here (good to know when you're dealing with these councils)
- Freedom of Information and Protection of Privacy Regulations
 - Covers who may act for a minor
 - Who may act for a deceased individual
 - Lays out how consent must be obtained
 - Has a fee schedule for FOI requests (we will touch on later)



Makes public bodies
accountable.

Protects privacy.

Purposes of FOIPPA

Accountable to the public:

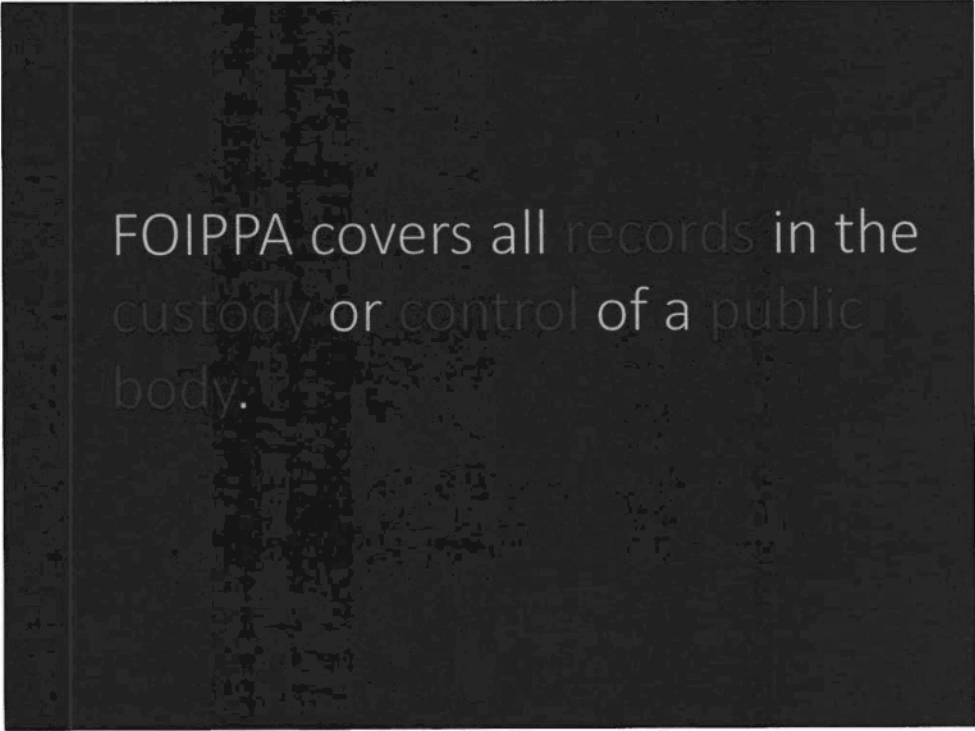
what Part 2 covers (Freedom of Information)

- Giving the public a right of access to records
 - FOIPPA will specify limited exceptions to the rights of access
- Giving individuals a right of access to their own personal information
 - And giving them a right to request correction of their own personal information

Protects privacy:

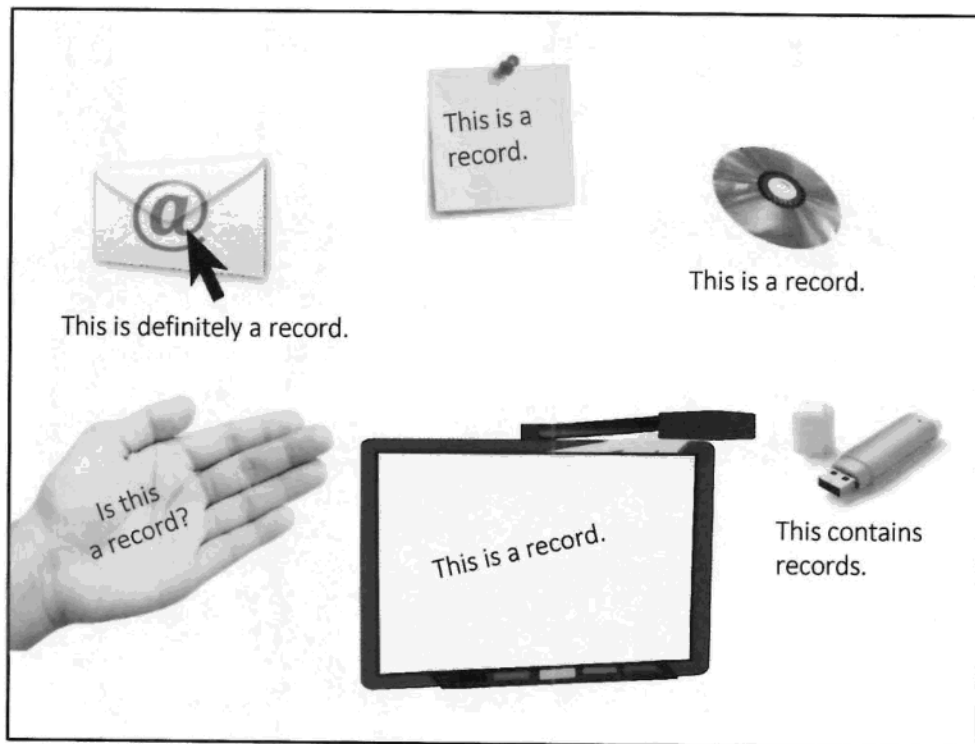
what Part 3 covers (Protection of Privacy)

- Preventing unauthorized collection, use, or disclosure of PI by public bodies

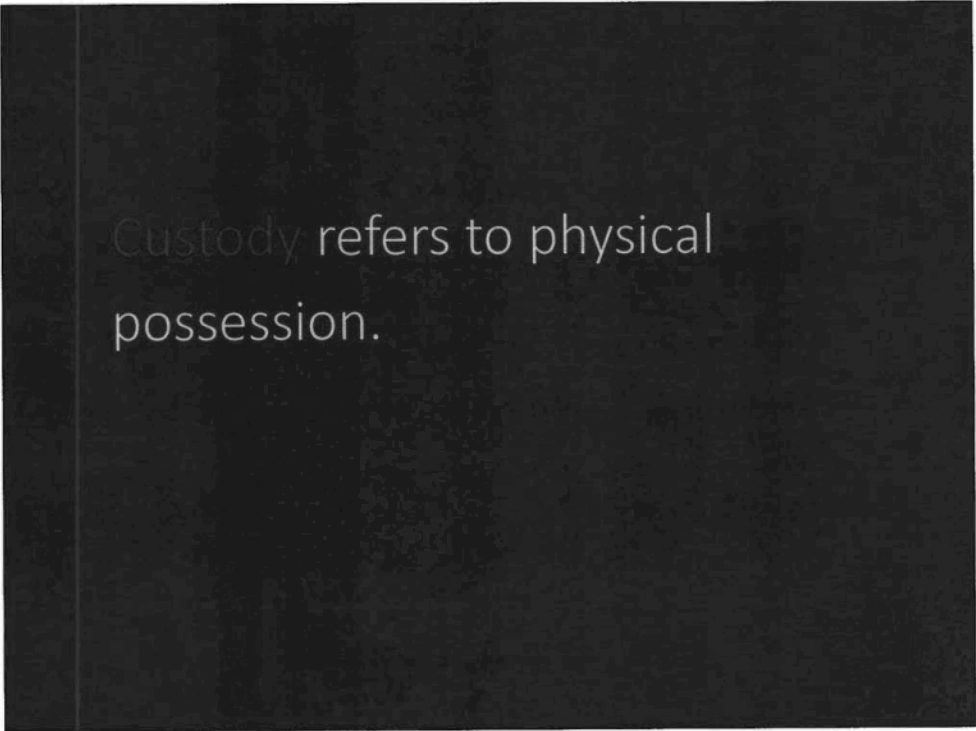


FOIPPA covers all records in the
custody or control of a public
body.

- FOIPPA covers all records in the custody or control of a public body
- We'll go through each of the terms in red



- 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”
- Emails and text messages are records



Custody refers to physical possession.

Physical possession

- Paper document / in-tray / desk
 - Word/ Excel / desktop / LAN
 - Post-it note on your computer
-
- May not be responsible for content
 - BUT...Responsible for providing access to and security of the record
 - Responsible for managing, maintaining, preserving and disposing of the record

Control refers to the power or authority to manage the record throughout its lifecycle.

- Authority to manage, restrict, regulate or administer the use or disclosure of a record
- Indicators of control:
 - Created by an employee of a public body
 - Created by a consultant for the public body
 - Specified in a contract
 - Subject to inspection, review or copying by the public body under contract

And what is control?

- Power or authority to **manage** the record throughout its life cycle, including:
 - Restricting, regulating and administering its use or disclosure

Difference between custody and control (babysitter example)

Babysitter = custody:

- Feeds
- Reads
- Puts to bed

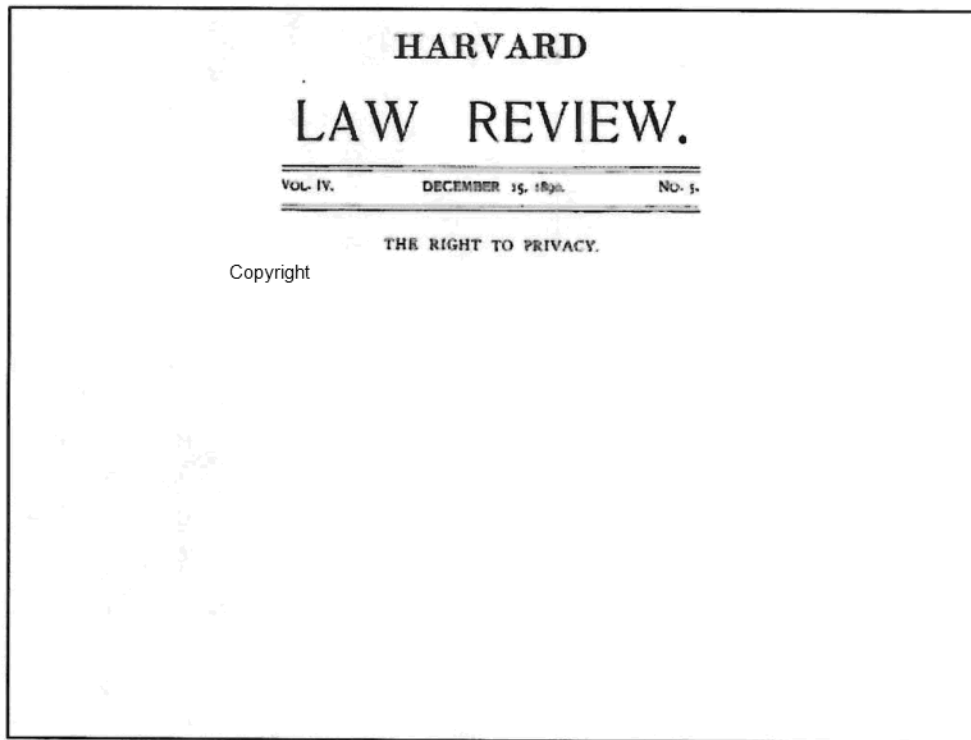
Parent = control:

- What the child gets fed
- Which stories
- What bedtime

Potential activity:

- Throw this one out to the audience
 - Use the flip board again to write out responses
 - This and next slide could be a 10-15 min conversation depending on audience
 - Ask audience to define privacy
-
- Point is that no one walks around with a definition of what privacy is
 - We typically think of privacy only when it's infringed upon
 - None of the statutes define "privacy" but aim to achieve it with rules for how personal info is to be collected, used and disclosed

Image source: <https://pixabay.com/en/boy-child-confused-person-61171/>



- 1890, law review article written by Samuel Warren and Louis Brandeis and published in the *Harvard Law Review*
 - Considered to be influential and the first publication in the US to advocate a right to privacy
 - Defined privacy as the **right to be let alone**
 - Especially in relation to photography and appearing in newspaper stories

- Today privacy is more about **informational self-determination**
 - You get to choose what happens to your information
- Informational self-determination is not the law, but is the underlying principle
 - E.g. if you robbed a bank, your physical description (personal info) is now handed over by witnesses to the police – even though that individual doesn't want their personal info out
- Privacy is about having a choice
- But with choice comes the need to weigh options
 - Think of how much of our privacy we'll give up for convenience, fame, etc.

Pictures demonstrate this:

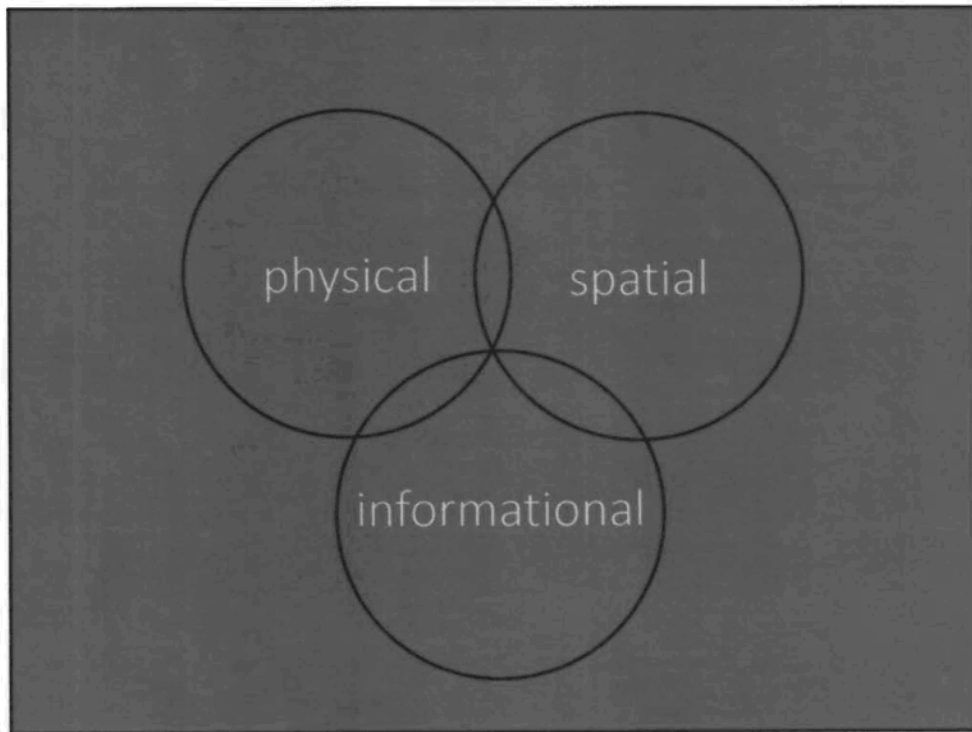
- Top left: performance artist had attendees at an Brooklyn arts festival trade their private info (image, fingerprints or social security number) for a cookie; people even proudly tweeted about it
- Top right: celebrity culture and the attempt to get back lost privacy
 - Think of how privacy was previously defined as the right to be let alone
- Bottom left: person using their sweater as a privacy screen
- Bottom right: tourists on Hollywood Blvd gave away their passwords on live TV for a split-second of fame on Jimmy Kimmel Live
 - <https://www.youtube.com/watch?v=opRMrEfAII> (start video at 0:42)

Privacy is:

- Subjective
- Contextual
- “Negative”

Privacy is:

- Subjective
 - Different to me than to someone else
 - How I feel about privacy, working in the field, is very different to my 11-year old who just wants to play his online game already(doesn't care if game is tracking his location)
- Contextual
 - Different across cultures, time, generations, etc.
 - E.g. privacy for a 70 year old will differ from a teenager's view of privacy
 - 70 year old may focus more on right to be left alone (closes curtains)
 - Teenager will think about the settings on their phone and social media
 - Can flux depending on personal vs work life
- Negative form of privacy
 - You're often not aware of your privacy until it gets infringed upon
 - Examples: airport body scan, bag search
- You'll often hear our office say “it depends” when asked a privacy question
- Privacy solutions can't be taken out of their context
 - What works in one situation may not be appropriate for another – all factors need to be taken into account
- FOIPPA provides direction, but there is also problem solving and risk assessment that goes into “doing” privacy



- There are types of privacy:
 - Physical (bodily integrity)
 - Drug testing, body scan at airport
 - Spatial (territorial)
 - Locker search, video surveillance
 - Informational (records with personal information)
 - Health record, bank record
- These types may overlap
 - E.g. hydro bill:
 - Informational – bill shows how much hydro you use
 - Spatial – can infer your activities by how much you use and when (can determine when you are home or if you have a grow op)

Right information.
Right person.
Right purpose.
Right time.
Right way.

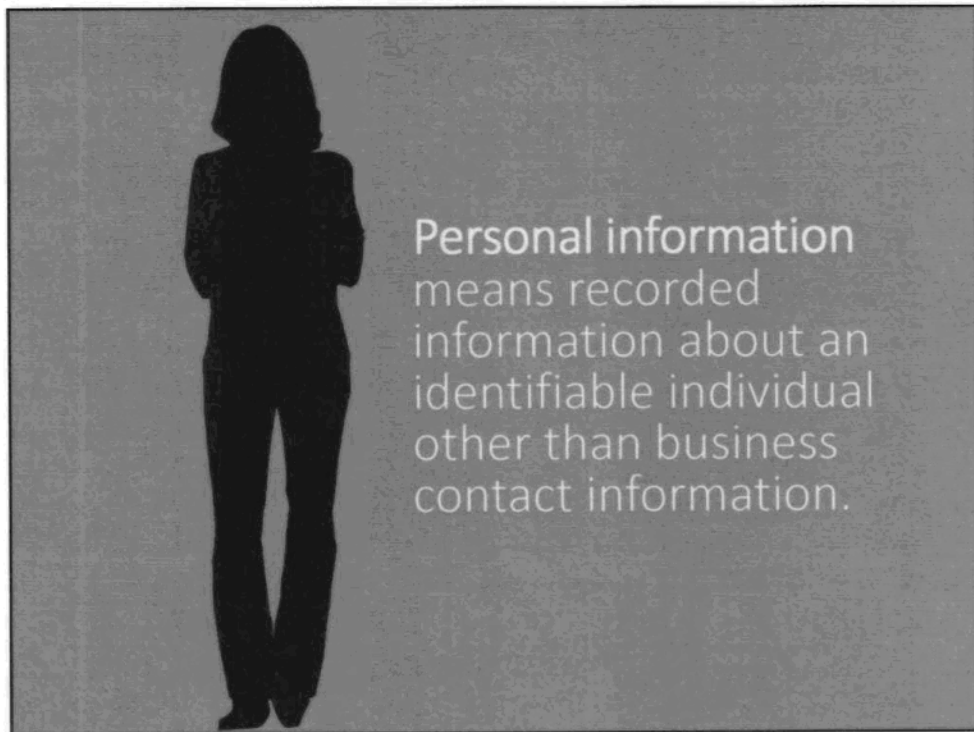
- Remember that privacy and security is not an add on
 - It needs to be embedded in everything we do

Mantra that helps:

- Right info: what info do you need to do your work?
 - e.g. do you need a SIN to sign people up for an event?
- Right person: who has access to what info?
 - do they know how to handle that info appropriately?
 - e.g. does everyone in your office need access to the person info in the report you alone are producing?
- Right purpose: use info for purposes for which it was intended
 - e.g. looking up health records of friends and family because you're curious
- Right time: is the info available in a timely way to allow you to do your job?
- Right way: how do we use the info?
 - do we maximize security?
 - e.g. do we leave sensitive client files on our desk when we leave for the day so anyone can look at them?

Story to illustrate mantra:

- Border Guard story
 - Collect sensitive info to allow people to cross the border
 - Collect info for national defense
 - Border guard contacted person on his off hours, through Facebook and asked her out
- Note for presenter: each principle can be highlighted when talking about the story (in terms of what went wrong)



- Good place to start with privacy is to determine what personal information is
- "Personal information" means recorded information about an identifiable individual other than contact information"
 - Definition in FOIPA used to include examples, but people read it as an exhaustive list
 - The privacy legislation in BC has a purposefully short, vague definition – accounts for the subjective and contextual nature of privacy

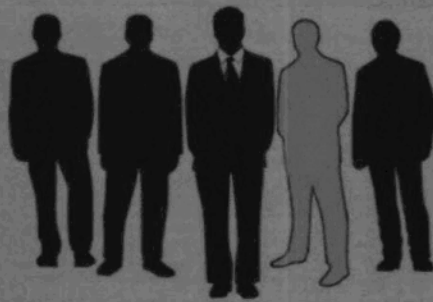
Examples

- Race, national/ethnic origin, skin colour
- Religious or political beliefs or associations
- Age, sex, sexual orientation, marital status
- Fingerprints, blood type, DNA information, biometrics
- Health records; educational, financial, criminal, employment history
- Your opinions
 - If your opinion is about someone else, then that is the other person's personal info

"contact information"

- Information to enable an individual at a place of business to be contacted
 - E.g. name, title, business telephone number, business address, business email or business fax number
- Discussion point: contextual personal info
 - Home business example (home address when ordering diapers vs applying for home owner grant)
 - Business card example
 - Give it to you during this training, it's business contact
 - Put it in draw, it's personal contact information

Mosaic Effect



- Remember, personal information is recorded information about an **identifiable** individual
- Mosaic effect: when information taken by itself doesn't point to an individual but when taken together, identifies an individual
 - E.g. I have the following bits of data: male, in his 20s, drives Honda Civic, lives in Vancouver
 - I'm drawing from a huge pool of people so will not identify an individual
 - In contrast, if I have these bits of data: male, in his 80s, drive a Rolls Royce in small town BC
 - I've now narrowed my pool considerably. And everyone knows that's Joe

Public bodies need an authority to collect under section 26.

- Section 26 recognizes a public body's need to collect personal info in order to carry out its mandate and to provide services
 - But it restricts that collection to a defined set of purposes
 - Authorized under an Act
 - For law enforcement
 - **Related directly to and is necessary for a program or activity of the public body (have to talk about this)**
 - Necessary for planning or evaluating a program or activity of a public body
 - The information is collected by observation at a public and voluntarily attended presentation, ceremony, performance, sports meet or similar event
 - Other authorities (domestic violence, provincial identity services)
- **Authorized under an act** – Motor Vehicle Act
- **"law enforcement"** definition is quite broad:
 - (a) policing, including criminal intelligence operations,
 - (b) investigations that lead or could lead to a penalty or sanction being imposed, or
 - (c) proceedings that lead or could lead to a penalty or sanction being imposed
 - E.g. Conservation Officers do law enforcement work (investigate environmental or wildlife violations)
- **Directly related to and necessary for**
 - E.g. an applicant's work history is directly related to the assessment of that person's qualifications against the basic requirements of a job
 - This info can be collected for use in screening applications to determine a shortlist for a competition
- **Planning or evaluating**
 - Surveys fall under this purpose
- **Observation**
 - Permits a public body to collect pi through observation at public events (e.g. hospital opening, sports competition or awards ceremony)
 - Previously there was no authority to take pictures of people at public events
 - Important notes: event has to be open to everyone (like a sporting event) and has to be an "event" (can't just be people on a public sidewalk)

Public bodies can't rely on consent for collection.

- Important note on privacy and public bodies is that public bodies can't rely on consent to collect personal info
- FOIPPA is authority based – meaning, you need an authority under the act to collect, use and disclose (share) personal info
- Some of you may have noticed that s. 26(d) allows consent for collection, but let me provide clarification:
 - Consent for collection under 26(d) is for a prescribed purpose
 - Any time “prescribed” is used in an act, we have to look to the act's Regulation for direction
 - Section 9 of the FOIPPA Reg deals with “Purposes for collection of personal information”
 - Those prescribed purposes are then listed:
 - a) To record or update a person's name or contact info under the Name Act
 - b) If the person is acting for a deceased individual and the purpose has to do with receiving a death notification (to provide or cancell benefits or services related to the deceased)
 - So this is consent for collection for a VERY specific purpose
 - Our office rarely if ever sees s. 26(d) used
- Remember that public bodies can't rely on consent for collection
- This is one of the main ways PIPA is different than FOIPPA
 - PIPA – for private sector – is consent based (collection, use and disclosure is done with consent of the individual)
 - FOIPPA is authority based
- Idea is that if you don't have authority to collect personal info in the first place, then you can't do troubling things with it
- Helps to assess your program and every element of info:
 - Is everything in your survey necessary and relevant for the program (e.g. address – we may not need to mail our clients materials, but we need to divide them geographically)

Copyright

- Introduce cartoon: example of not being able to hoard info

Section 27 governs how personal information can be collected:

collect **directly** from the individual.

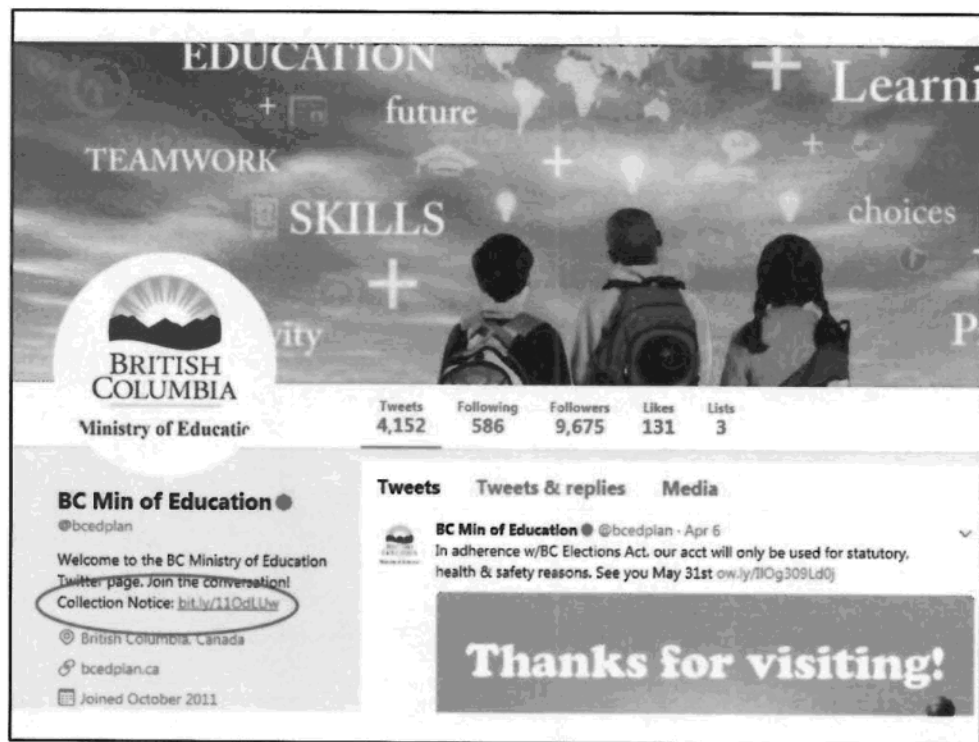
- Section 26 tells you what you're allowed to collect
- Section 27 tells you how you must collect that info
- Information must be collected **directly from the individual**
 - Except in limited circumstances
- Examples of indirect collection allowed under s. 27:
 - Authorized by another enactment
 - E.g. Tax Act says that the Ministry of Finance can collect income tax information from the Canada Revenue Agency
 - The collection is necessary for medical treatment of an individual and it isn't possible to collect information directly from the individual
 - E.g. Joan is collapsed on the floor and I'm on the phone to the dispatcher – I have to give the dispatcher Joan's personal info to help her survive
 - For law enforcement
 - E.g. if you're a thief and you've robbed a bank, police will collect your personal info from an eye witness
 - Makes more sense because thief wouldn't give the police that info (needs to be collected indirectly)
 - If individual has authorized the indirect collection:
 - E.g. I give you my references so they can tell good things you about me
- When indirect collection isn't ok:
 - Taking vacation photos and putting them in a travel agency pamphlet (or there's Joe in his bathing suite)
 - Looking up a job applicant on Facebook
 - In our day-to-day life, we view this as public info – if person has their Facebook account open to the public
 - But public body needs an authority to collect that info – and Facebook page isn't part of the resume process
 - Note that the OIPC has guidance on this

This information is collected by [public body] under section 26(c) of the *Freedom of Information and Protection of Privacy Act*. The information collected will be used to [purpose].

If you have any questions about the collection, use or disclosure of your personal information, please contact:

Position title
Physical address
Phone number

- Moving back to collecting directly from individual:
 - Must provide notice
- Not having a collection notice makes your org look bad at privacy
 - Usually the first thing client's see when encountering a program/service
 - Also first thing Privacy Commissioner will see when encountering gov services
 - PCT uses this as our radar for how well an org or ministry is doing – whether or not they post collection notices
- Notice is simple thing to do – an easy win for privacy
- On the screen is all the elements needed for collection notice
 - 3 pieces of info:
 - a) purpose for collecting it
 - b) legal authority for collecting it
 - c) the title, business address and business telephone number - who can answer questions about the collection
- Purpose needs to be descriptive enough
 - E.g.
- Put your collection notice at the point of collection, e.g. on the survey, on the application form, on the blog, on the phone line



- This is a good example of how you can fit this in a social media context
 - Solution focused
 - Working with small space so they put link to a separate page to post full collection notice

How do you handle overshares?

- **Note for presenter: this example allows us to talk about s. 27.1**

- As part of your citizen engagement project you have a social media presence
- Let's say you want engagement on a new bridge project
- Lo and behold, someone included inappropriate photos in their post

Question:

- Is the org authorized to collect all of this information?
- If not, what steps should they take now that the photos have been submitted?
- Under s. 27.1 you can delete the photos
- s.27.1 for administration (when people send things that you didn't intend to collect)
- Public body dictates what they want so that anything that falls outside (in this case, comments on bridge's infrastructure problems) can be deleted
- Overshares will always happen, but you're minimizing your org's liability or vulnerability
- Consider this:
 - If you leave in photos and there's a FOI request, you'll have to redact those photos
 - And you've stored that personal info (inappropriate photos) that whole time! – info you never needed for your project
- Important note: viewing of information is considered collection
 - Ruling by Privacy Commissioner

Case Studies

- Walk audience through case studies using s. 26 handout

Let audience know that there isn't a formula that will work all the time. The formula is to assess each element each time.

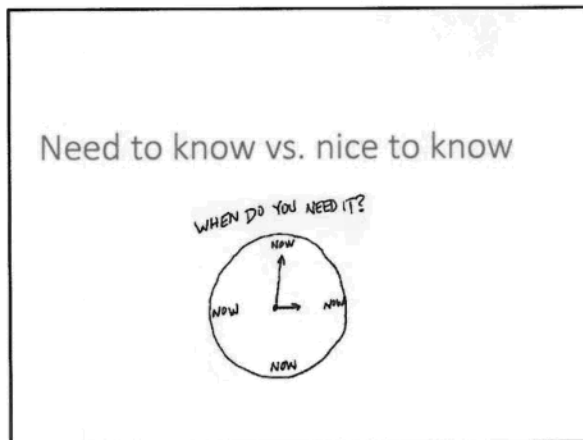
Remember that any privacy question is answered with "it depends."

Use personal information for the same purpose for which it was obtained.

- Notice how much we just talked about collection
- FOIPPA also covers use and disclosure of PI
- But 70% of what we talk about when introducing FOIPPA is collection
 - Collection is your gateway to privacy
- Use covered under s. 32
- A public body may only use personal information:
 - For the purpose for which it was obtained or compiled (so purpose you collected under s. 26), or for a consistent purpose:
 - a reasonable connection to the original purpose, and
 - necessary to perform the duties of, or for operating a legally authorized program, of the public body
 - If the individual has consented to the use
 - For a purpose for which the personal information has been disclosed to it under the Act
- Surprises are bad with use
 - E.g. if you have someone's DOB and address because they've applied for a seniors bus pass, they would likely be surprised to receive a birthday card (inconsistent use)
 - E.g. think about if it was a Cannabis company who sent you a birthday card
 - Or drug rehab clinic sends you birthday card and people you don't want to know about your rehab see the return address
 - **Note to presenter:** need to use example here that you can defend if someone pushes back if they think it's ridiculous (may be grey in real life, but law is cut and dried)

Consistent purpose =
reasonable connection
+
necessary for duties

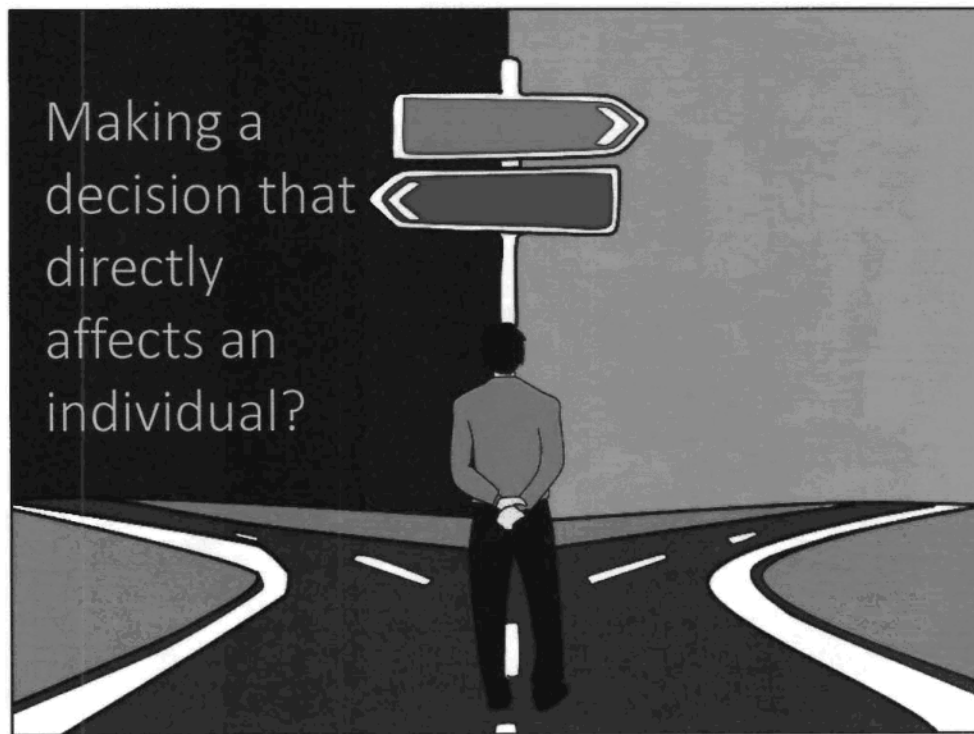
- **Note for presenter:** could adjust this for time
- Main uses of PI:
 - For the purpose for which it was obtained or compiled, or for a consistent purpose
 - FOIPPA defines consistent purpose (s. 34):
 - Has a reasonable connection to the original purpose, and
 - Is necessary to perform the duties of, or for operating a legally authorized program, of the public body
 - If for another purpose, individual can consent to the use:
 - Note that consent has to be a specific way as per Regulations ("prescribed"):
 - a) be in writing, and
 - b) be done in a manner that specifies
 - i. the personal information for which the individual is providing consent, and
 - ii. the date on which the consent is effective and, if applicable, the date on which the consent expires
- E.g. FIN has tax info so you can pay your taxes; they couldn't then use that contact info to advertise training



- **Notes for presenter:** hard to talk about all the disclosure provisions broadly
 - Better to tailor it to the audience
 - Connect audience to provisions they're more likely to use
 - **Could get case examples from the audience**
 - Or deal with on a principled basis and ask audience to be aware of their disclosure
- Disclosure provisions in FOIPPA:
 - s. 33.1 – disclosure inside OR outside Canada
 - s. 33.2 – disclosure inside Canada only
- Limit disclosure (sharing) of info:
 - Can't disclose for future purposes – needs to be in current context (NOW)
 - Limit distribution – to staff who needs to know it to do their job
 - Limit content – how much information do they need to do their job?
- Consider if your business area regularly discloses info
 - What's the act you use?
 - You should know the acts that apply to your area
- If someone asks you to disclose whether or not someone on your staff has been at work for the past week
 - Answer: don't tell them – unless they have a law that allows them to get that info (e.g. CFCSA)
- If there's an aggressive client – 1) what authority do you have to disclose; and 2) who would you share this info with
 - 1) s. 33.2(e)
 - to an officer or employee of a public body or to a minister, if the information is necessary for the protection of the health or safety of the officer, employee or minister
 - 2) Front counter staff? HR staff? Executive?
 - Who needs to know?
- Consider if someone from CRA asks for info
 - You're allowed to ask for their legal authority to do so
 - Then do you trust them?
 - If they're asking for SIN, push back based on your comfort
- Disclosure only in authorized circumstances (to other entities)
 - There are so many disclosure provisions (people often think that FOIPPA is a barrier to info sharing)
 - 33.2(c) to an employee of the public body...if the information is necessary for the performance of the duties of the employee
 - Example: A payroll clerk must see some of the personnel information of a local public body's employees to administer their pay, service and attendance records.
 - 33.1(1)(c) In accordance with an act or enactment
 - Example: Section 29 of Insurance Vehicle Act allows ICBC contacts a public body to get details about an employees attendance at work to assist in its investigation of a claim.
 - Other disclosure authorities:
 - Health and safety of employees
 - Member of bargaining agents (union)
 - Law enforcement agencies
 - Etc.

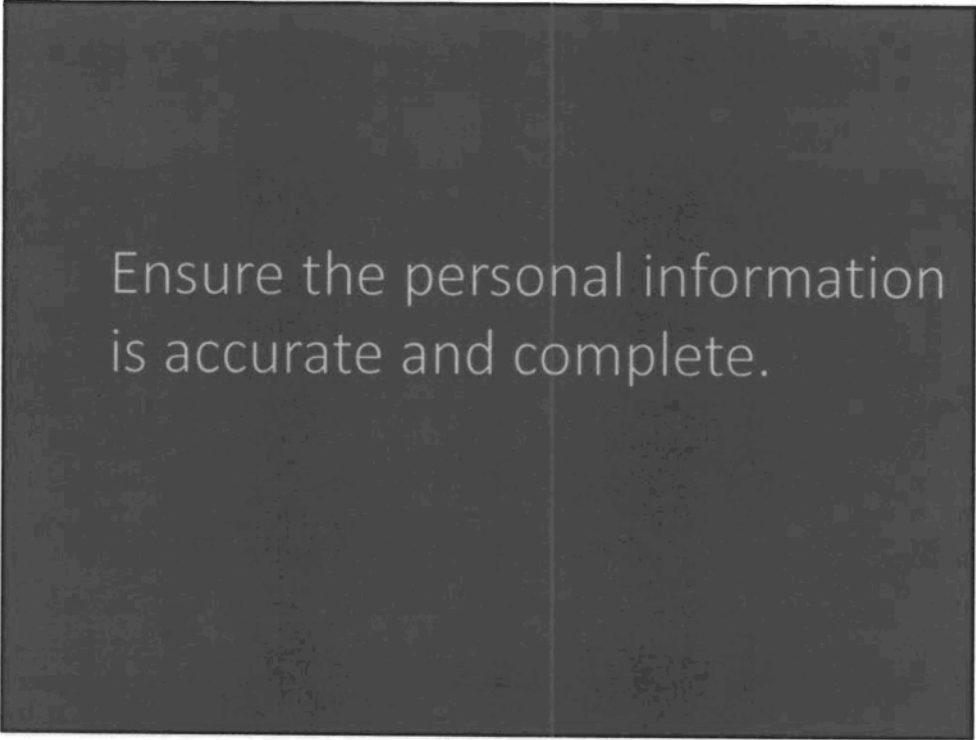
Image source: https://c1.staticflickr.com/3/2276/2312622098_b65e8f397a.jpg

- Introduce cartoon – need to know principle (limiting disclosure)



- **Note for presenter:** everyone thinks their work is important, so they'll think the product directly affects individuals
 - So handle this point with sensitivity
- If a public body is using personal information to make a decision that directly affects the individual, must keep info for at least 1 year
 - Minimum under FOIPPA
 - Other acts could require longer periods (e.g. tax records)
 - Or you may need to keep it for longer to meet operational needs
 - Note that there are risks to retaining records indefinitely: become out of date, incomplete, pose a security risk
- E.g. cutting benefits or revoking access – you'll need to keep records on this decision for at least one year
 - This allows individual to request access to those records (part of transparency)

Image source: <https://pixabay.com/en/decision-choice-path-road-1697537/>



Ensure the personal information
is accurate and complete.

- Need to ensure personal info is accurate and complete
- Also likely want to do this for business reasons
- Examples:
 - Date of birth used to determine eligibility for a benefit – want to make sure date is accurate
- Consider letting people correct their own info
- Ways to verify personal info is accurate and complete:
 - Periodic checks of the info with the individual
 - Thorough reviews of applications to make sure complete
 - Documenting when personal information is collected or received
 - Have processes in place to correct personal info

An individual has the right to request correction of their personal information.

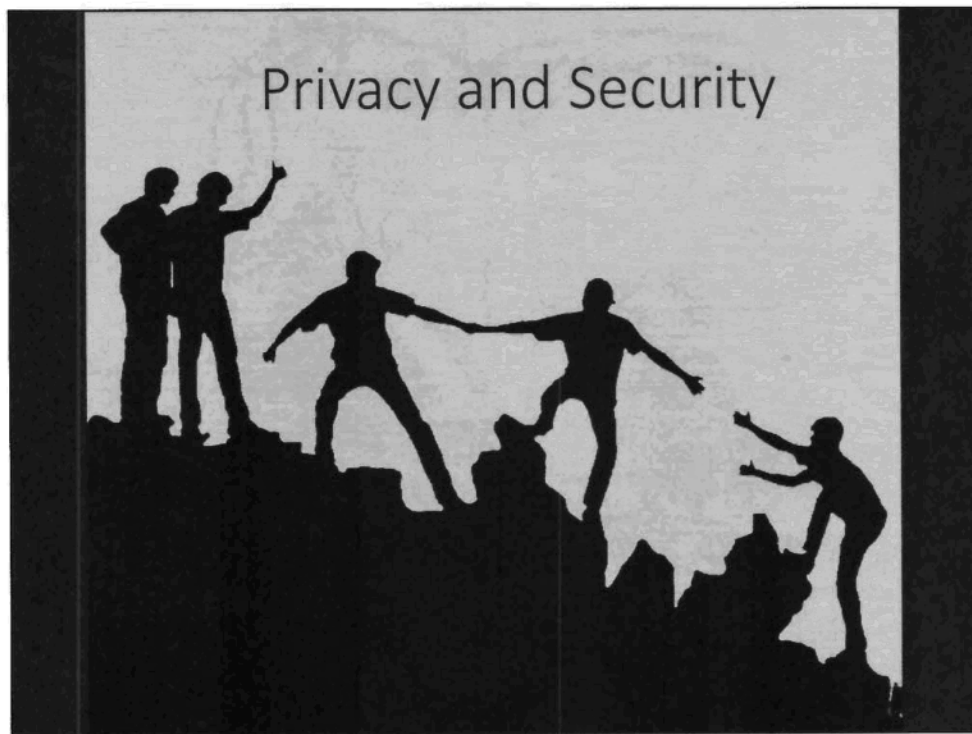
- Individuals have right to request correction of their personal info
- The right to request correction is distinct from the public body's duty to annotate
- This isn't an avenue for appeal – just because someone is complaining doesn't mean you have to correct it
 - Isn't about decision making – it's about info
- Right to correction under s. 29
 - Applies to factual errors or omissions in personal information, not to expressions of judgement
 - E.g. wouldn't apply to doctor's medical opinion
- As normal practice, a record should be kept of disclosures of personal info to other public bodies or third parties
 - Enables subsequent notification of a correction or annotation to the record

DISCUSSION IF QUESTION IS RAISED ABOUT GENDER IDENTITY:

- E.g. individuals being able to identify their gender
 - Business reasons may rely on documenting your sex at birth (e.g. Vital Stats BC)
 - But personal demands need to be taken into consideration – for you to live your life, you want to be identified as female (e.g. would need Driver's License to show gender identity)
 - Born with this sex but identify with this gender
 - This would be when annotation is crucial (rather than correction and deletion) (e.g. Vital Stats annotates record of live birth so ICBC can issue DL that lists gender appropriately).

Copyright

- Introduce cartoon: little Timmy wants to make a correction to Santa's naughty list



- Now we'll introduce the security requirements under FOIPPA
- Note that privacy and security work together
 - Work in conjunction with records management as part of a broader information management program

Image source: <https://pixabay.com/en/together-helping%E2%80%8Beach-other-winning-2643652/>



- **Note for presenter:** go with the audience for this – they will raise questions
- For example:
 - Collecting money owing: if you go outside Canada, we'll go outside Canada with info if needed (33.1(1)(i))

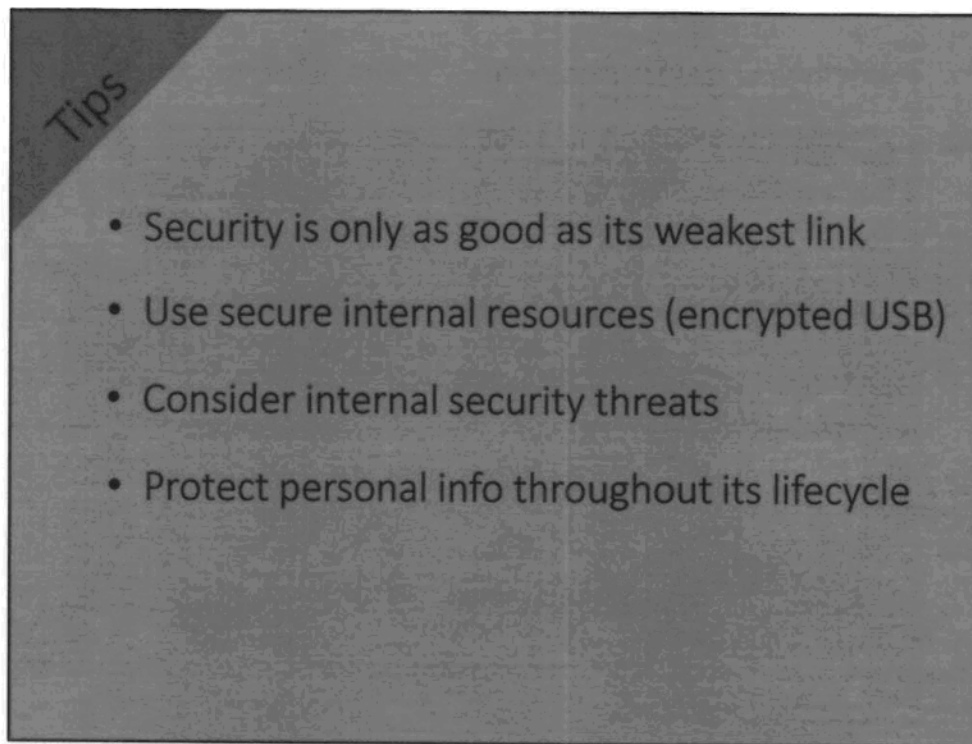
s. 30.1

- Inside versus outside Canada – important distinction in FOIPPA whether storing, accessing, or disclosing PI (s.30.1 and also 33.1)
- The default is to keep data inside Canada unless within certain scenarios as laid out in FOIPPA:
 - Typically need consent if disclosing outside Canada (on internet) (33.1(1)(b))
 - Public, voluntarily attended event (e.g. photos of ribbon cutting) (33.1(1)(q))
 - Engagement on social media (e.g. via Facebook) (33.1(1)(r))
 - Under an enactment (33.1(1)(c))

Image source: https://cdn.pixabay.com/photo/2016/02/02/01/43/canadian-flag-1174657_960_720.jpg

Reasonable security = appropriate and proportional

- s. 30 calls for reasonable security arrangements
- “Reasonable” means appropriate and proportional to the sensitivity of the info
 - Lunch order vs health records: sensitivity will determine where you store the info and who has access to it
- Appropriate and proportional will help you prioritize your focus
 - With all the personal info your org has, you’ll want to put your energy into securing the very sensitive info (e.g. health records) vs. the employee basketball roster
- Note that human error is a big contributor to breaches, so you’ll want to prevent breaches as much as possible
 - One way to do that is with robust security – security that is appropriate and proportional to the info’s sensitivity
- Safeguards should include:
 - Physical measures
 - E.g. key card access to buildings; security guard at front desk
 - Technological measures
 - E.g. encryption, firewall
 - Policies/procedures
 - E.g. don’t put password under keyboard or keep keys dangling from your locked cabinet; clean desk policy



- **Note for presenter:** use whatever examples resonate with you (can use examples from OCIO newsletter)
- Security is only as good as its weakest link
 - Train staff, conduct periodic reviews
- Use secure internal resources
 - e.g. encrypted email and flash drives
- Consider internal security 'threats' – including those from privacy-unaware staff
 - Limit access to "need to know"; consider audit trails
- Protect personal information throughout its lifecycle
 - E.g. "clean desk" policy for current records; properly storing inactive records; properly disposing of records

Incidents happen



- Information Incident:
 - An unwanted or unexpected event that threatens the privacy or security of information
- Privacy breach is a type of information incident
 - Privacy breach is a collection, use, disclosure, access, disposal, or storage of personal information, whether accidental or deliberate, that is not authorized by the Freedom of Information and Protection of Privacy Act

Image source: https://cdn.pixabay.com/photo/2017/01/09/12/49/mistake-1966448_960_720.jpg

The majority of breaches are due to human error.

- **Note to presenter:** use good examples
- Majority of breaches are because of human error
 - Which means they are typically administrative in nature:
 - Misdirected fax
 - Wrong email address (because of autofill)
 - Double-stuffed envelope
- E.g. X-files show: service provider tasked with getting rid of records; sold them to props company who then sold those records to X-files; and the records were part of the show!
- Other types of privacy breaches:
 - Inappropriate Access
 - E.g. a person accessing the health records of their family members (not authorized under FOIPPA)
 - Inappropriate disclosure:
 - E.g. telling people about foster children
 - Loss or theft:
 - E.g. lost hard drive; unsecured USBs; lost file folders; hacking or phishing attempts
- E.g. janitor was tasked with destroying records
 - Instead of shredding, took files to beach for a bonfire
 - Wind picked up and records spread down the beach
- Introduce video – breach reporting for gov, but gets message across that breaches have to be reported
 - Video: <https://gwww.gov.bc.ca/news/2018/0206/fear-not>

- 1) Report
- 2) Recover
- 3) Remediate
- 4) Prevent

- **Note for presenter:** encourage people to use this process if they're outside gov

When it comes to information incident management, employees have the following responsibilities:

Report: most important

- Report both confirmed and suspected incidents
- Work with your internal privacy office
- Useful to make notes on details of the incident – you may be asked for these during the investigation
 - Who, what, where, when, how
 - What could be the cause of the incident?
 - What and whose personal info is involved?
 - Is there any unauthorized use or disclosure and to whom?
 - What was the order of events?
- Don't delay!

Recover:

- Investigator will walk you through steps to recover confidential or personal information if possible
 - E.g. if an email is sent to the wrong person, can you contact that person and have them double delete the email and confirm they've done so?
- Note: recovery of methods could mean dumpster diving
- If can't recover it, you have to contain it
- Instances where recovery is not likely:
 - E.g. guy who wasn't adhering to clean desk policy – really messy surfaces
 - His office was locked but bird was coming in through the open window, stealing his mess and building a nest
 - E.g. doctor who faxed in patient records to health authority
 - Doctor was opinionated – sent lots of letters to local media
 - He accidentally auto dialled his faxes to media when sending patient records
 - Imagine his terror as the fax with sensitive medical info goes through the fax to the media

Remediate:

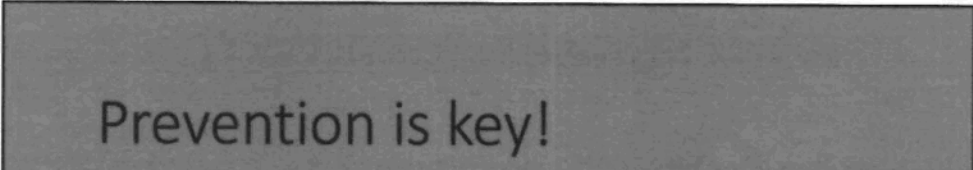
- Investigator will walk you through steps to remediate and resolve the incident:
 - E.g. may need to notify individuals or parties affected by the incident

Prevent:

- No wasted mistakes – learn from the incident
- Investigator will lay out steps to prevent similar incidents from happening

Summary of Responsibilities:

- Report it (actual and suspected info incidents)
- Be familiar with the Information Incident Management Process (3RP)



Prevention is key!

Copyright

- It's better to prevent a privacy breach than to have to respond to one
- Working in a public body, you are responsible for:
 - Promoting a culture of privacy
 - Preventing incidents from happening
- Prevent breaches through compliance with the general FOIPPA requirements, for example:
 - Awareness of the disclosure authorities and other provisions of FOIPPA
 - Reasonable policy and procedures for disposing personal info (not selling old hard-drives; shredding; etc.)
 - Reasonable security arrangements, including physical, technical and policy measures (discussed previously)

Image sources:

https://commons.wikimedia.org/wiki/File:%22Prevent_Forest_Fires%5E_Crush_Out_Yu_r_Cigarette%22_-_NARA_-_514097.jpg

https://commons.wikimedia.org/wiki/File:SMOKEY_SAYS_-_PREVENT_FOREST_FIRES_-_NARA_-_515433.jpg

https://commons.wikimedia.org/wiki/File:%22Don%27t_Let_Him_Come_Home_to_This_Prevent_Forest_Fires%22_-_NARA_-_514152.jpg


- Introduce cartoon: shows lifecycle of a record and the need to protect it through the lifecycle

Privacy Tools



- Let's look at some privacy tools that will help your organization assess privacy risks

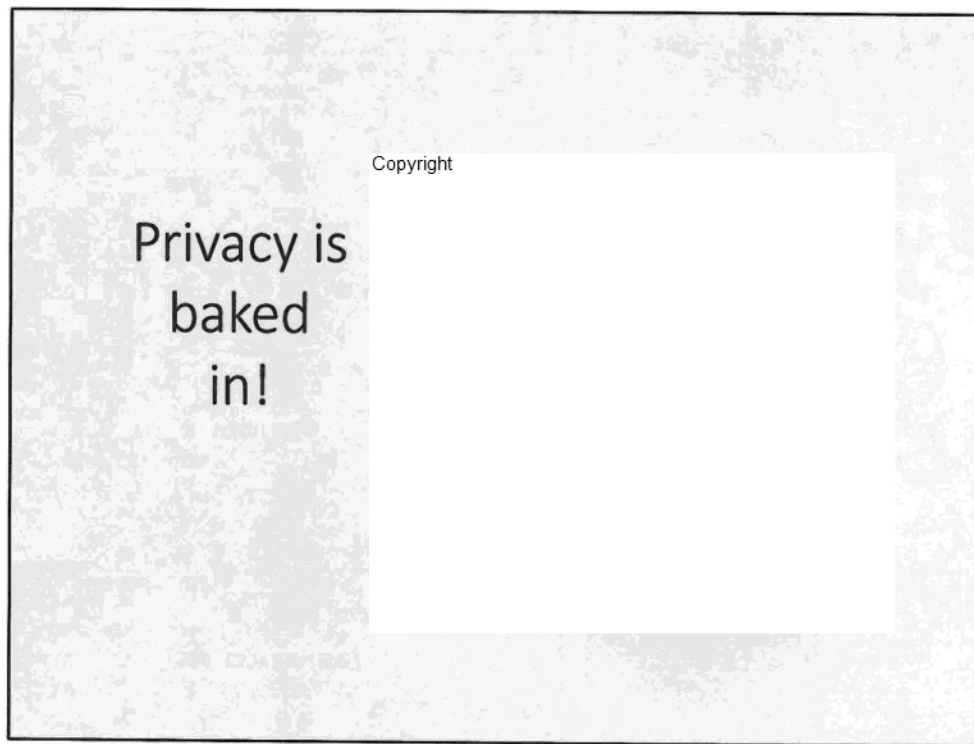
Image source: https://cdn.pixabay.com/photo/2016/07/29/08/49/tools-1551457_960_720.jpg



A Privacy Impact Assessment will
benefit your project.

Benefits of completing a PIA:

- Can ensure privacy requirements are identified and satisfied in a timely and cost efficient manner
- PIA process is also designed as an educational tool – participating in PIAs promotes privacy awareness
- The PIA can make the difference between a privacy invasive and a privacy enhancing initiative, without compromising business objectives or adding significant costs
- Meet your legislated requirements
- For those filling out a PIA: focus your attention on the first question – what are you doing?



- PIA supports privacy by design – bake privacy into your project/process
 - Concept from Ann Cavoukian, former Canadian Information and Privacy Commissioner



Complete a PIA during the development phase.

--check Governance for more info

When do you do a PIA?

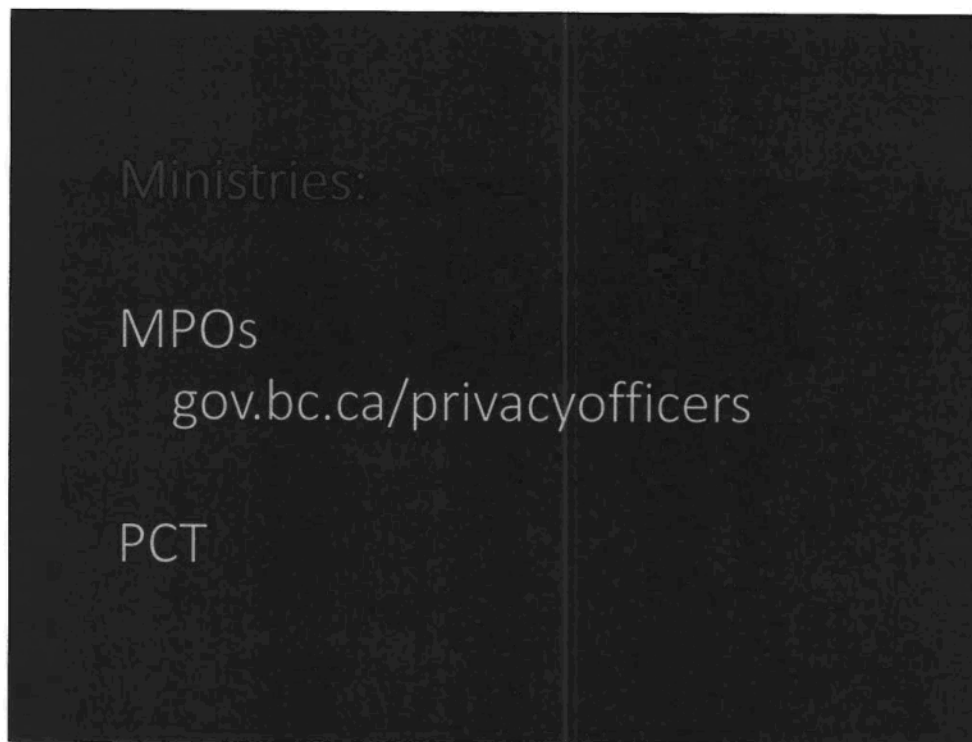
- During the development phase of a new program, project, system, legislation, technology, or other initiative
- Before the implementation of a significant change to an existing program, project, system, technology or information system, or legislation takes place
- For all significant existing programs/initiatives

Complete a PIA whether personal information is or is not collected, used or disclosed

- FOIPPA doesn't distinguish
- Sometimes personal information is identified during the process

Reason for development phase piece:

- Builds an environment of proactive privacy – of dealing with privacy before it becomes a problem
 - If every time a PIA is submitted it is done on the day before the program launches, then people will view privacy as a problem (because Privacy Officer has to take time to do a proper assessment, which could conflict with the project deadlines)
 - Helps you to think of privacy throughout the project
 - Can help you figure out what you're doing along the way



- Where do you go for help with your PIA?
- Ministries:
 - Ministry Privacy Officers (gov.bc.ca/privacyofficers)
 - Privacy, Compliance and Training
- Don't struggle with the PIA on your own
- Start it and when you start slowing as things get harder, turn to your Privacy Officer

Other public bodies:



OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for British Columbia

250-387-5629
info@oipc.bc.ca

- Non-ministry public bodies can go to OIPC for help:
 - OIPC
 - Phone: 250 387-5629
 - Email: info@oipc.bc.ca
 - Website: <http://www.oipc.bc.ca/>

Information Sharing Agreements are the terms and conditions in the exchange of personal information.

=> Used when there is a regular and systematic disclosure of PI between public bodies.

- During the privacy assessment of a project, program or activity, it may be determined that an Information Sharing Agreement is needed
- ISA is like an MOU – it is used to document the terms and conditions of the exchange of personal information
 - Be aware that people may call an ISA an MOU
- Used when there is a **regular and systematic disclosure of PI between public bodies** (not within a public body)

Components:

- Description of the PI being exchanged
- Description of the exchanged (flow)
- Efforts that will be made to ensure the PI is
 - Accurate, complete, up-to-date
 - Secure (stationary and in transit)
- Compliance monitoring and investigations with regard to the above

Benefits are:

- A clear articulation of expectations, roles and responsibilities of the parties
- Accountability for the personal information in your care and being exchanged.
- **Note:** ISA documents your authorities, but does not provide the authority
- ISA Best Practices / Guidelines:
http://www.cio.gov.bc.ca/local/cio/priv_leg/documents/foipppa/guidelines_isa.pdf
- If you don't do ISAs, consider if you should and speak with your Privacy Officer

Privacy Protection Schedule

- Attach as a schedule to the contract
- Contractor is an employee
- Can't contract out of FOIPPA

- Build privacy into contracts
- E.g. gov's Privacy Protection Schedule
 - Contractor subject to the same FOIPPA requirements as the public body
 - So is an employee of the public body
 - Can't contract out of FOIPPA obligations
 - Completed and attached as a schedule to any contract between a public body and a contractor where personal information is involved
- Contract has to make sense for both parties
 - So both parties should be able to read and understand it
- Schedule online: <https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/privacy/agreements-contracts/privacy-protection-schedule>

Privacy, Compliance and Training:

www.gov.bc.ca/protectprivacy

(list of MPOs on left-hand side)

PowerPoint Notes for Privacy and Access:

www.gov.bc.ca/privacytraining

Useful links

Mention that FOIPPA is online

BC Privacy and Access
Helpline

250-356-1851
(Service BC 1-800-663-7867)

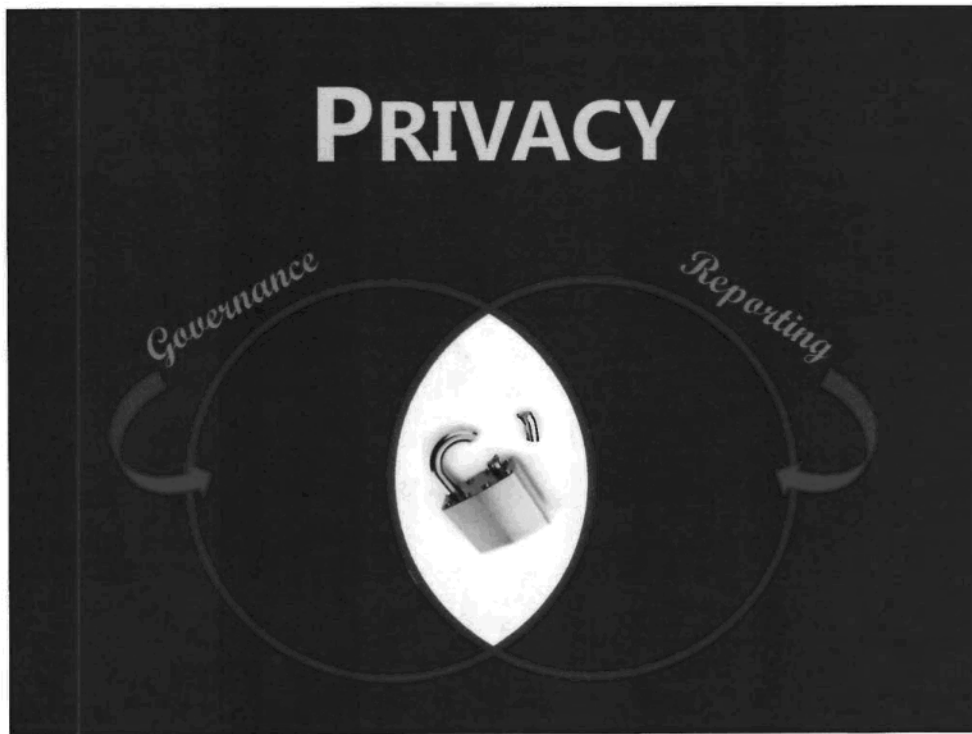
privacy.helpline@gov.bc.ca

INFORMATION INCIDENTS

Best practices and lessons learned

Policy, Compliance and Training Branch | Ministry of Education, Ontario

- Welcomes and introductions



Privacy overview/objectives:

- Audience will learn:
 - What legislation is applicable and why it matters
 - The difference between personal information and confidential information
 - Who to report to and what contacts will be important in reporting a breach
 - Fun case study exercises throughout the training session



Introduce the branch and Unit- Privacy, Compliance and Training Branch, Investigations Unit in the Ministry of Citizens' Services

PCT – Corporate privacy shop for government and manages privacy and access helpline. Broken into three groups:

- Strategic Privacy, Policy and Training
- PIA team
- Investigations and Practice Reviews
- Investigations and Practice Reviews is responsible for investigation incidents that are the responsibility of the govt of BC- how do we determine what we can investigate? Jurisdiction and Scope
 - Responsible for investigating incidents that are the responsibility of the "Government of British Columbia"
 - Mandated to investigate all real or suspected information incidents (i.e. violations of FOIPPA)
 - Which bodies are responsible for what in incidents involving dual/multiple responsibility?

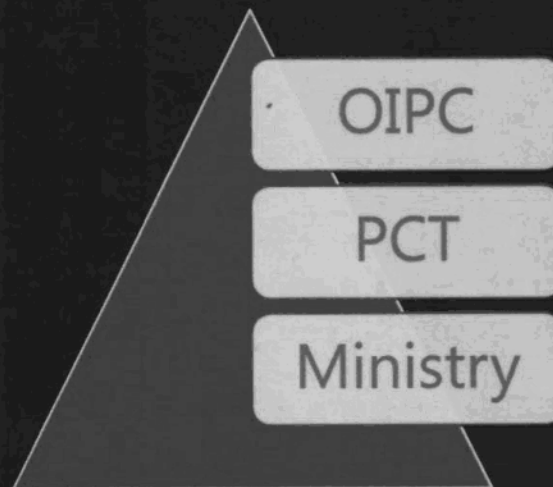
- Helpline

-Responsible for all investigations into all information incidents for all government ministries and public bodies that fall under core policy

-we provide advisory services to organizations that are outside of our jurisdiction (advice, best practices)

-if you don't know whether your organization falls under core policy you may need to consult with your legal counsel

ROLES AND RESPONSIBILITIES



OIPC – independent oversight and enforcement of BC's access and privacy laws, including: FOIPPA and PIPA. We will discuss more about the OIPC's roles and responsibilities in the next slide.

Ministry

Designated business Representatives (e.g. MCIO, MISO, MPO, specialists)

MPOs typically only have roles in privacy incidents, vs. MISOs/MCIOs have roles in info incidents generally

Partners:

- Human resources/labour relations
- IT Security and forensics
- Legal (consultation and litigation)
- Law enforcement

-we also work on incidents that involve multiple responsibilities/jurisdictions : this requires a conversation about who is responsible for what, at the outset



OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
for British Columbia

Protecting privacy. Promoting transparency.

The Office of the Information and Privacy Commissioner (OIPC):

- conducts reviews and investigations to ensure compliance with FOIPPA
- mediates FOI disputes
- comments on FOI and privacy implications of proposed legislative schemes or public body programs

It's also very important that we talk about 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. The OIPC is not government – it is an independent office of the Legislature

OIPC provides a very useful resources regarding previous decisions/orders

- by section of FOIPPA
- Basis of interpretation of FOIPPA
- We use this resource

Michael McEvoy is BC's Information and Privacy Commissioner. The Information and Privacy Commissioner is the Regulator of FOIPPA and PIPA.

The Commissioner has the power to:

- Investigate, mediate and resolve appeals concerning access to information disputes, including issuing binding orders;
- Investigate and resolve privacy complaints;
- Initiate Commissioner-led investigations and audits of public bodies or organizations, if there are reasonable grounds of non-compliance or if it is in the public interest;
- Comment on the access and privacy implications of proposed legislation, programs or policies;
- Comment on the privacy implications of new technologies;
- Conduct research into anything affecting access and privacy rights;
- Educate the public about their access and privacy rights and the relevant laws.



PIPA - Private sector equivalent, does not apply to public bodies

- PIPA includes similar regs to protect PI and failure to adhere is still a breach

- Further, the OIPC's guidelines on an organization's obligations when dealing with a breach are the same, whether they are covered by PIPA or FOIPPA

- OTHER- as noted, some other prov. Legislation has specific carve-outs that provide additional authorities for collection use and disclosure EX: CFCSA s. 79

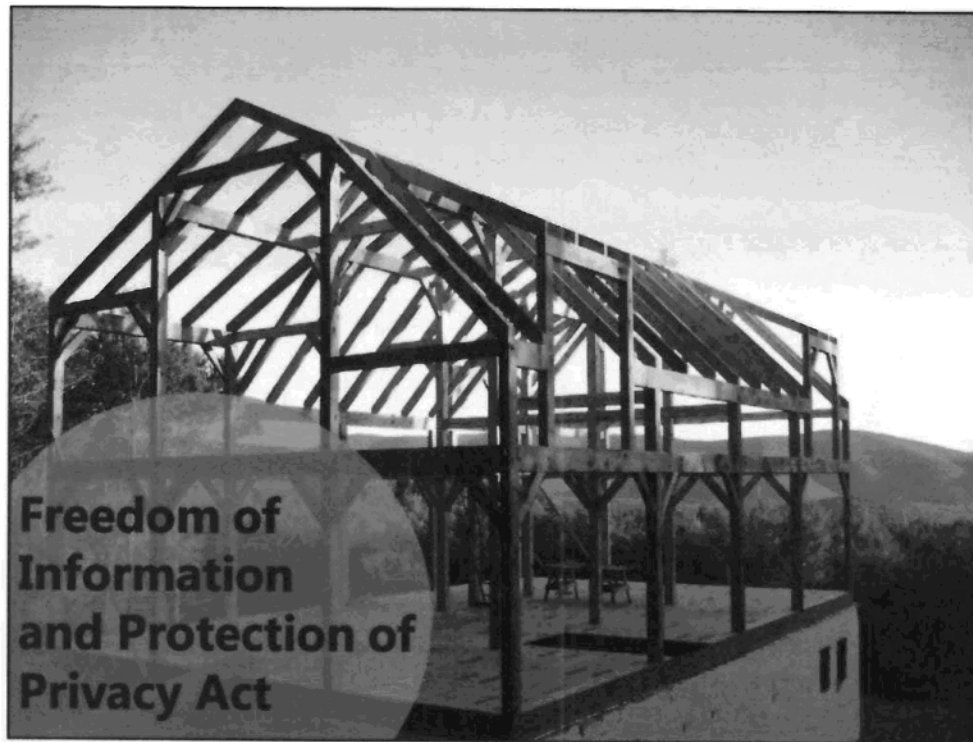
- contraventions of other legislation can also constitute breaches (i.e. could be a breach of a CFCSA info-sharing authority)

- FOIPPA honours these authorities

- the Investigations Unit is familiar with these and frequently works in the nexus of FOIPPA and other legislation

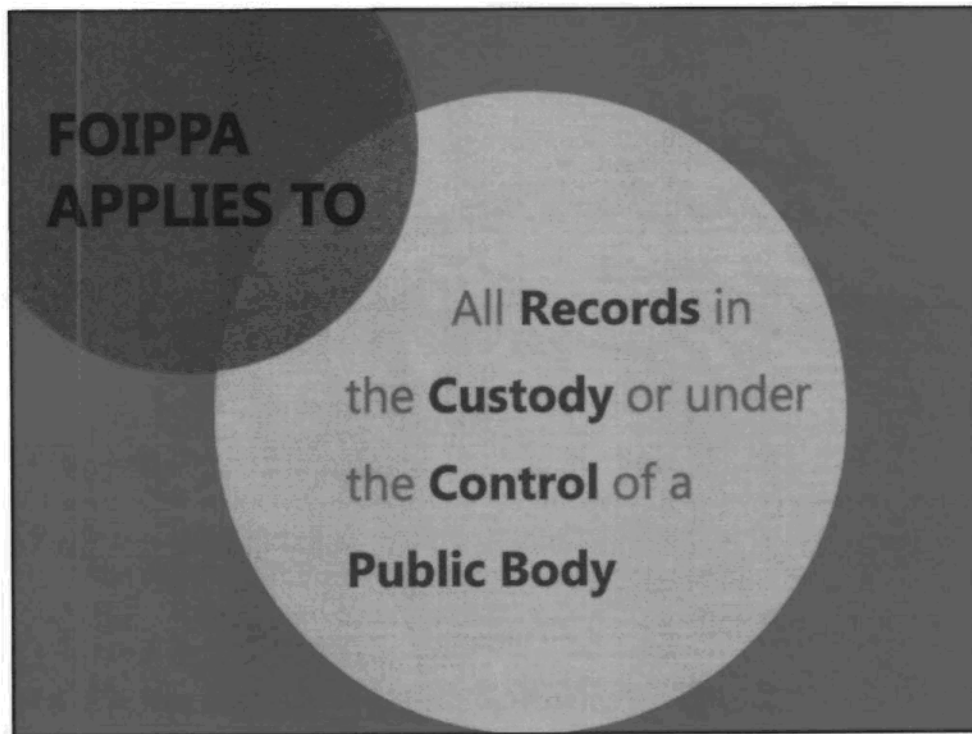
Federal - although FOIPPA is the foundation within BC some organizations within prov. Govt work with Fed govt, so have to be aware of federal legislation as well— some external orgs are governed by Fed. Leg due to nation-wide business operations— largely similar but good to know

- CHARTER- comes into play when conducting investigations due to S.8 protections against unreasonable search and seizure.



Legislative framework in British Columbia

- FOIPPA is the legislative framework that applies to all public bodies in BC
- Divided into 2 sections
 - Pt2- Freedom of Information (guides the release of info in responses to FOI requests)
 - Pt3- Protection of Privacy (authorities for collection, use disclosure and reasonable security measures)
- contravention of FOIPPA authorities constitutes a breach
- contraventions of other legislation can also constitute breaches (i.e. could be a breach of a CFCSA info-sharing authority);
- The breach management process is a key part of meeting, or re-establishing, the reasonable security measures test, as every breach constitutes a contravention of this section (s. 30)
- FOIPPA is the foundation for all actions govt can take with PI- there are certain pieces of legislation that include carve-outs/exceptions; however, no policy can be in conflict with FOIPPA



Who/What does FOIPPA apply to?

- All records in the custody or control of a public body
 - So we now know what records mean according to the legislation

~~-if you're a service provider to a PB, you must fulfill the public body's privacy obligations under FOIPPA~~

~~-there's no contracting out of FOIPPA~~

~~-this pertains specifically to records containing personal information related to your contract, not all records including PI.~~

Record: A "record" is any information recorded or stored by any means whether in hard copy or in electronic format. This includes books, documents, maps, drawings, photographs, text messages, letters, e-mails, telephone records, black books, vouchers, papers, etc...

Public body: Over 2,900 public bodies. Including government ministries, universities, health boards, governing bodies of professions, municipalities, regional districts and police boards

Keep in mind that in cases where public bodies contract out their services to non-profit organizations, these orgs take on the FOIPPA obligations of the public bodies.

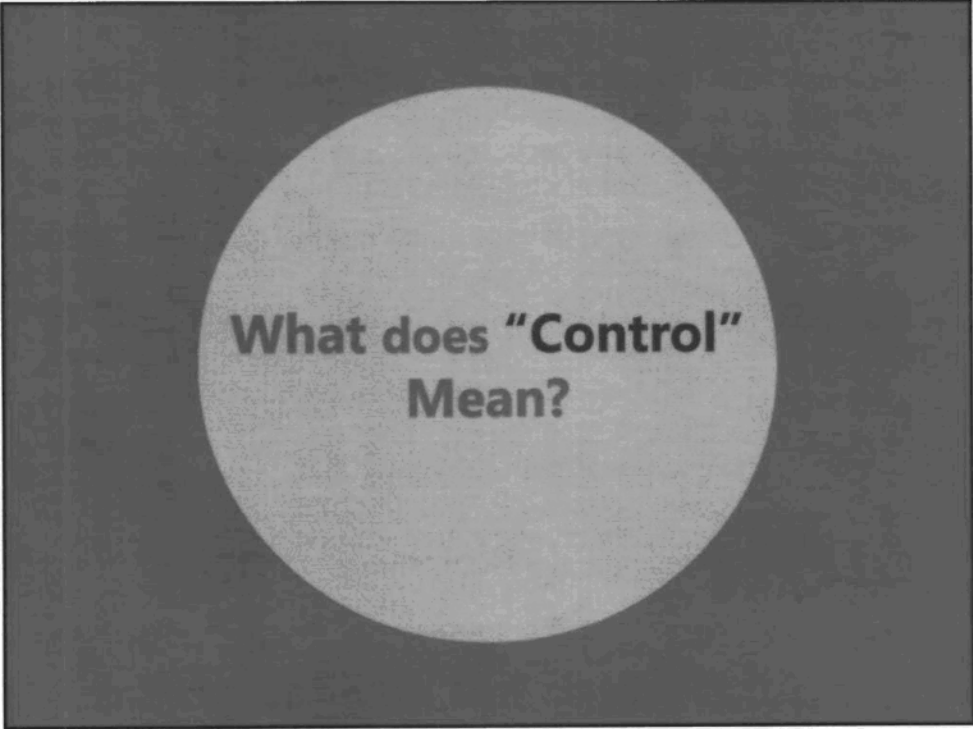
Physical possession

- paper document / in-tray / desk
- Word / Excel / desktop / LAN
- Post-it note on your computer

Not the same as **responsible for content**

BUT...responsibility for access, managing, maintaining, preserving, disposing, and providing security of that record in your physical possession.

Example, even though no “control” over content of report - whether or not you, or someone else sees that record, reads it, holds it, “accesses” it, deletes it, is up to you.



What does “Control” Mean?

And what is control?

- power or authority to **manage**, restrict, regulate or administer the use or disclosure of a record throughout its life cycle, including:
 - restricting, regulating and administering its use or disclosure.

Difference between custody and control

Indicators of control:

- Created by an employee of a public body,
- Created by a consultant for the public body,
- Specified in a contract,
- Subject to inspection, review or copying by the public body under contract.

Babysitter example.

Baby Sitter = custody:

- feeding time
- Reads books
- Puts baby to bed

Parent = control

- What food fed
- Which stories
- What time bed

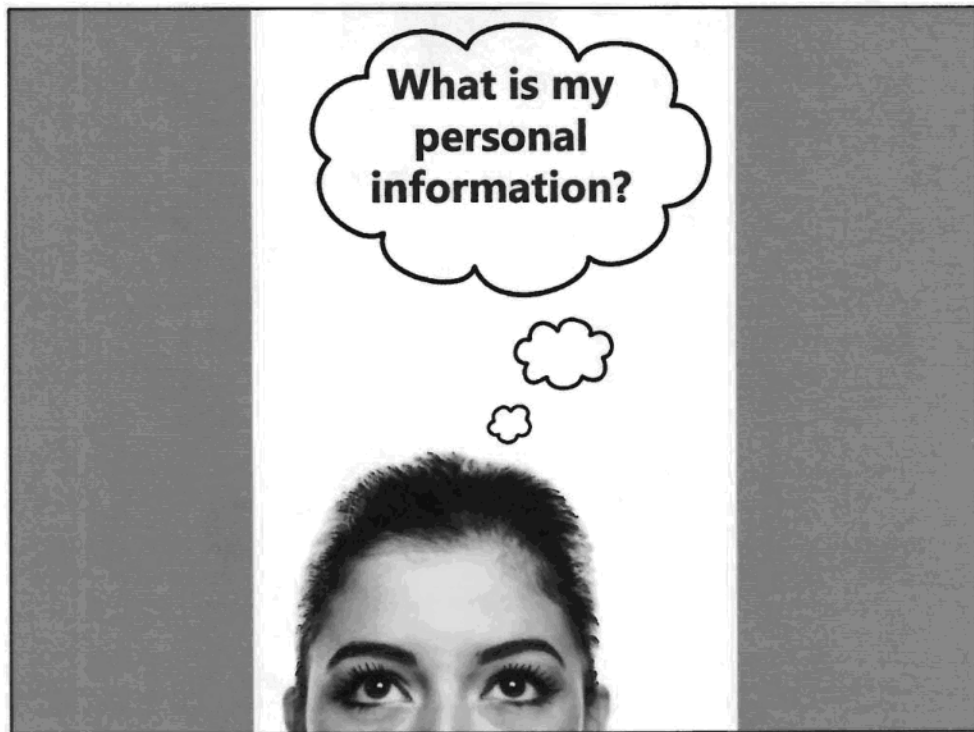
• Phone company example (corporate may be PIPEDA; services provided under contract with government FOIPPA).

PERSONAL INFORMATION...

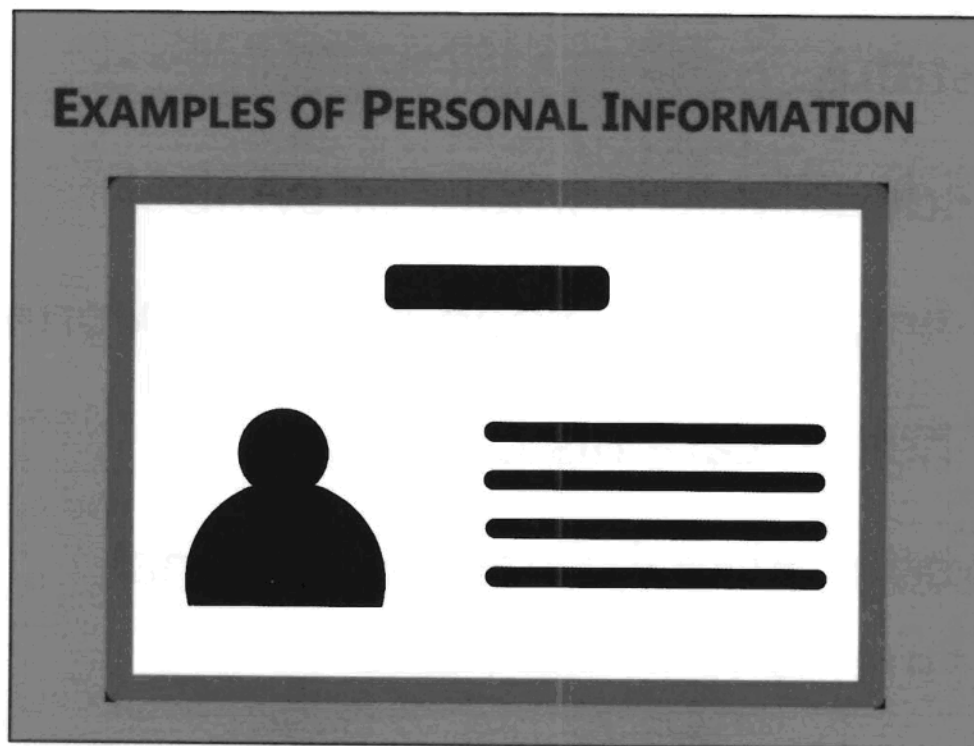
means recorded information
about an identifiable individual
other than business contact
information.



- Important to know what personal information is so that we can identify it in records.
- There use to be a list in FOIPPA but it was determined that this was not an effective approach---- any thoughts why? Answer: PI is evolutionary, privacy is evolutionary and contextual, if you ask 10 people what privacy means to them, it will be different answers, similarly privacy can be a cultural concept and can be a generational concept
- In this environment it can feel like the goal post for what we are trying to protect are also evolving- in such a context we fall back on Leg, defn, while being aware that citizens have expectations for us in handling PI



- FOIPPA definition: means recorded information about an identifiable individual other than contact information
- to break this down further- recorded- this includes written and electronic records
- business contact info- business contact exclusion- example (purpose- for collection)
- identifiable information- not just a name or record where a person is named, ex: SIN: Unique identifier that can be linked to a single individual EX: Photos- if an individual is identifiable



-go over different types of PI

-in this environment it can feel like the goal post for what we are trying to protect are also evolving- in such a context we fall back on Leg, defn, while being aware that citizens have expectations for us in handing PI

status

- identifying number or symbol
- fingerprints, blood type, DNA prints
- health care history
- educational, financial, criminal, employment history
- anyone else's opinions about an individual and the individual's personal views/opinions unless about someone else



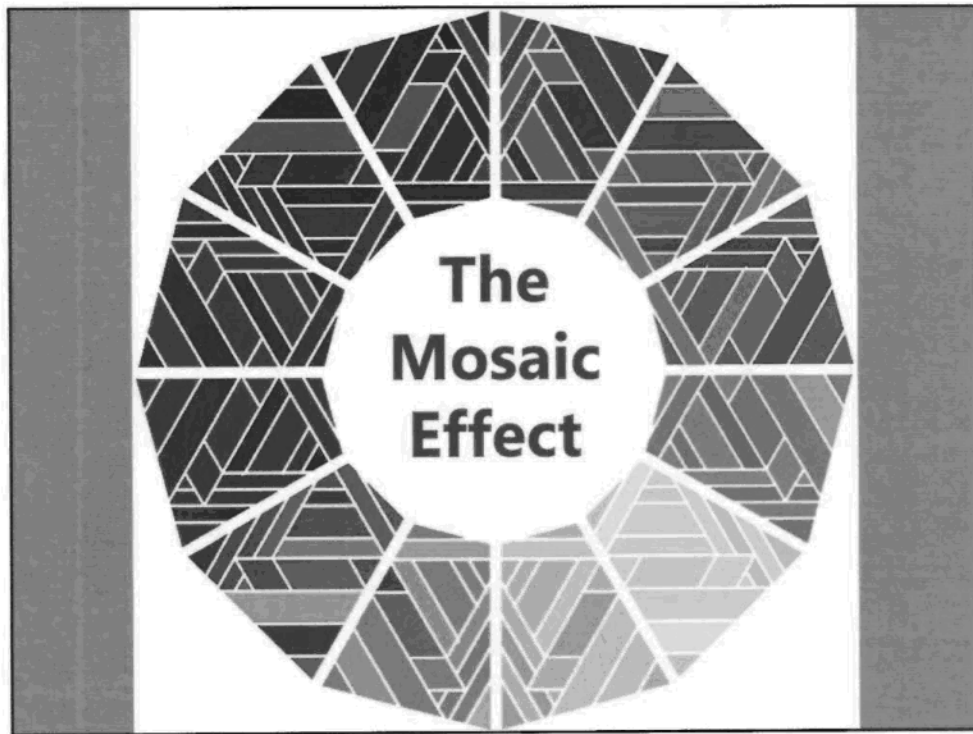
Used to be right to be left alone – is now **informational self-determination**

- You get to choose what happens to your information
- Eg. Who has cell phone? Password protected? How many digits? = individual differences
- Eg. 90 year old man (closing curtains in his living room) vs 15 yr old teenager (Facebook privacy settings) = differences by group

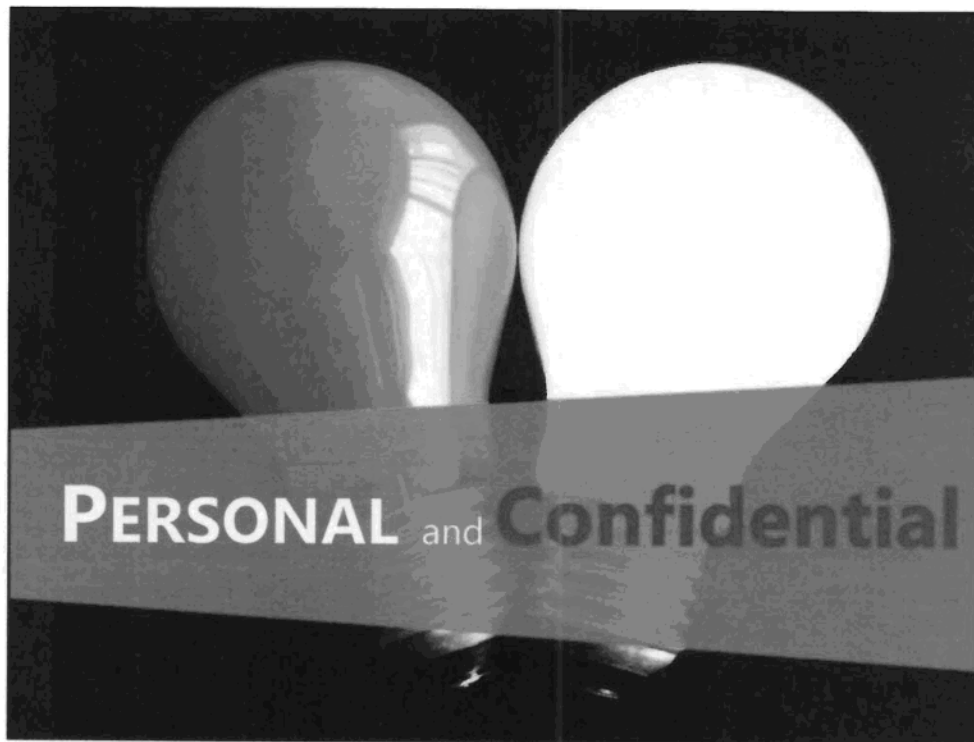
Privacy isn't just physical – it can be viewed in many ways:

- Physical – drug testing, body scan at airport- person's physical being – bodily integrity
- Spatial (territorial) – locker search, video surveillance – intruding into another persons environment
- Informational – records with personal information – health record, bank record

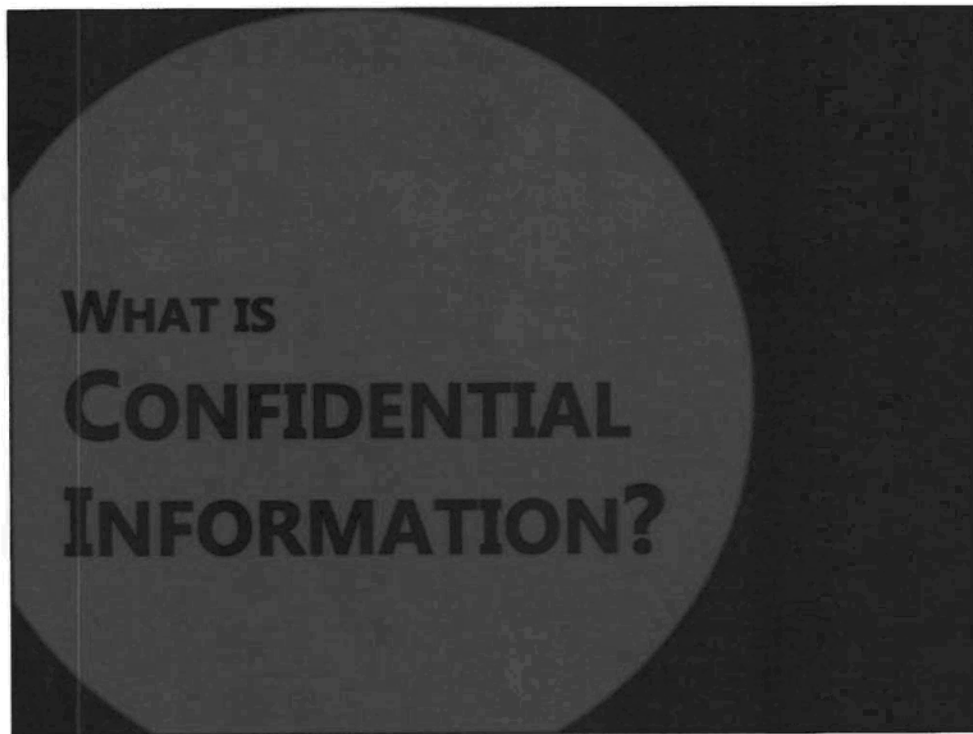
-* ask for other examples- what does your area manage*



- Additional concepts to be aware of: Mosaic effect- this occurs when pieces of info are put together to form a picture of an identifiable individual
- Example: (your last name), (age), white chevy, 4000 seymour, brown hair- each may not be identifiable alone, but together it becomes identifiable



- in addition to personal info, we also have to be aware of confidential info
- confidential info is a broader category that can include PI but also non-PI
- today when I refer to confidential info, I am meaning that which is not personal
- in most organizations there are further security requirements around confidential info, as there is also risk associated with the release of this info



Confidential information includes personal information, where its disclosure would constitute

- government economic, like cabinet confidences or financial information that has not yet been implemented or made public;
- information harmful to intergovernmental relations (e.g., information received in confidence from another government);
- third party business information, where its disclosure would harm the third party (e.g., a reference to correspondence from an identifiable individual); and,
- legal advice or law enforcement information.

Section 12 - Cabinet confidences

**Section 14 - Legal advice or law
enforcement information**

**Section 16 - Information harmful to
intergovernmental relations**

**Section 17 - Government economic or
financial information**

**Section 21 - 3rd party business info
(damage to interests of a 3rd party)**

Section 22 - Personal information

**collection, use, disclosure,
access, disposal or storage**

of personal information,
whether accidental or deliberate,
that is **not authorized** by the

**Freedom of Information and
Protection of Privacy Act.**

A collection, use, disclosure, access, disposal or storage of personal information, whether accidental or deliberate, that is not authorized by FOIPPA

-Generally, we use the trigger of whether an incident involves PI in order to determine whether a privacy breach, but the more technical and specific def'n is noted here

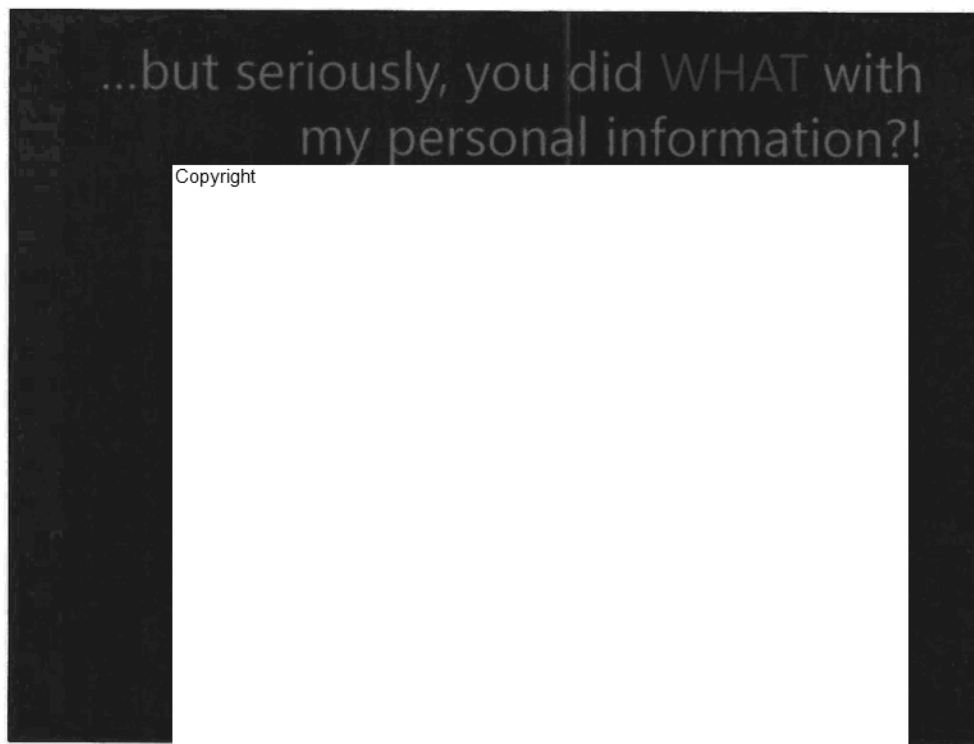
-An information incident is any unwanted or unexpected events that threaten the privacy or security of information

-Demonstrate responsibility of employees when dealing with an information incident Chapter 12 of policy manual. Core Policy applies to employees and business owners (including supervisors and contract service providers) or any person handling information managed (e.g., collected, accessed, used, shared, stored, disclosed, disposed of, or archived) by the government of British Columbia

-Various types of incidents:

- Privacy breaches
- Privacy complaints
- Security breaches
- Breaches of confidential information

Includes privacy complaints...



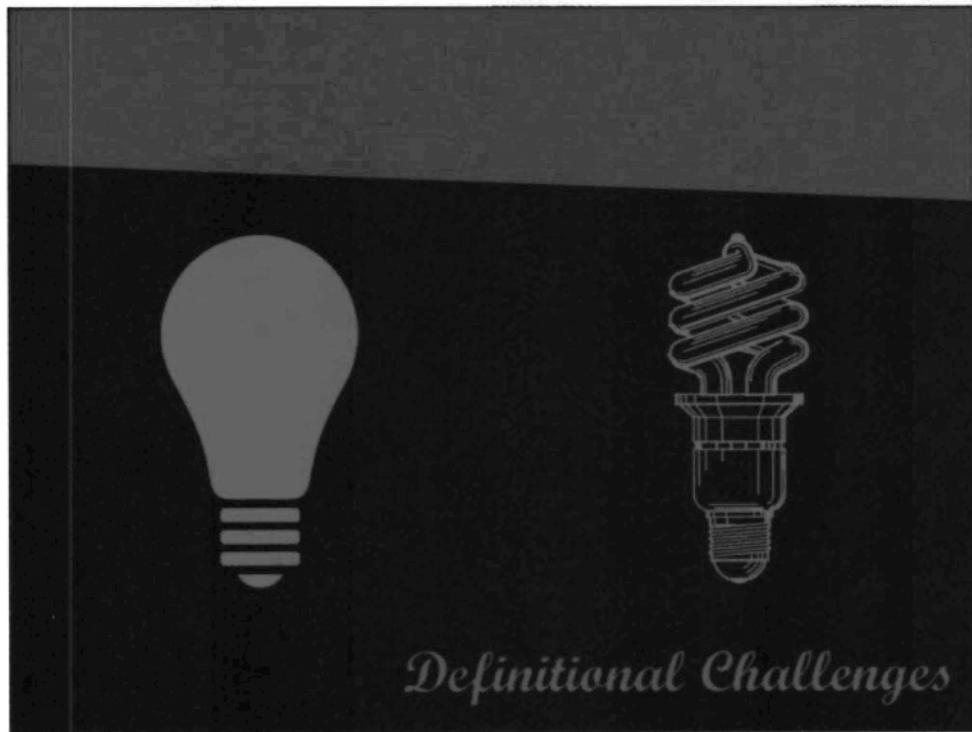
-Privacy breaches can also be **privacy complaints**

-Complaints are distinguished from breaches by who reports it (complaints are reported by the impacted individual)

-Complaints can be submitted to govt verbally, or in writing and can be submitted to any govt employee— however, they should always be brought to the PCT Investigations Unit

-Complaints are treated as possible breaches, until we can confirm whether anything inappropriate or unauthorized has happened

-Complaints are only substantiated in about **40% of cases-60%** are unfounded which could mean something didn't happen or that the person had authority to do what they did



Break after this slide

Other definitional considerations:

- Other situations involving inappropriate retention, storage, or failure to protect personal information?
- Violations of other legislation or records that are not in scope of FOIPPA – i.e. YCJA records, court records?

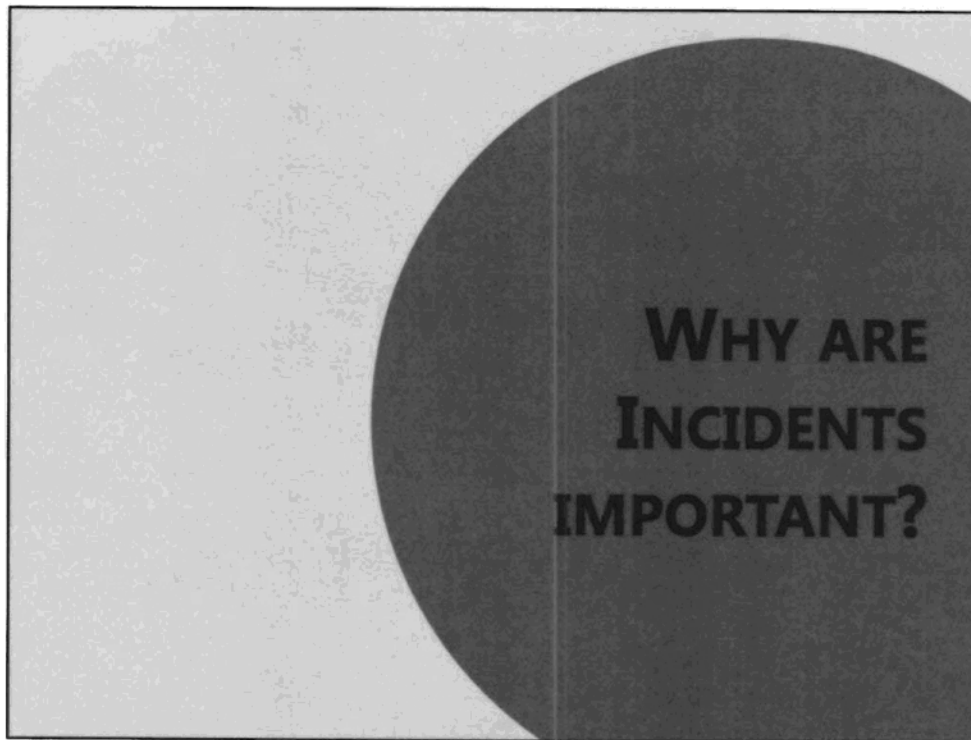
-Although we've talked about the definition our unit uses, it is not the only one. Listed is the definition used by the OIPC, other organizations may have their own definition

-What about violations of FOIPPA not related to aspects described? Retention, storage, or failure to protect
-not expected to know all the relevant exceptions or authorities of other leg but the IU will work with you to help determine if the disclosure was authorized.

-What about violations of other Leg. That includes info protection provisions?

-What about exposure of info that is excluded from FOIPPA? Court Records?

- When in doubt, report



Resume from Break

- As public bodies, our primary obligation is to consider the harm to our clients
- We will discuss harm later on, but what kinds of harm do you think could result from a breach? What would you be worried about if it were you?
- Each incident could also cause **harm to your organization or harm to an individual including an individual's reputation**
- When something is disclosed there is an impact to the individual. It's not just harm to a person's physical, spatial or informational privacy but also to their reputation
- With public awareness of privacy, there is a media appetite to report on privacy incidents
- Impacted parties may take their stories to the media
- Breaches can also be harmful if there is a loss of public trust/confidence in government operations



-Speaking of reputational damage factor...

-Hardly a day goes by when we don't hear about a breach in the media

-No organization is immune to privacy breaches.....for example

-Govt has faced recent high profile incidents as well----education

-These, and their high profile nature, show that the public is becoming aware of privacy, which makes the stakes even higher for organizations to have ways to prevent breaches from happening and how to respond when they do

Examples:

Nova Scotia – FOI one

US Postal Office of Personnel Management- Cyberattack , 2014 Employee and customer personal information

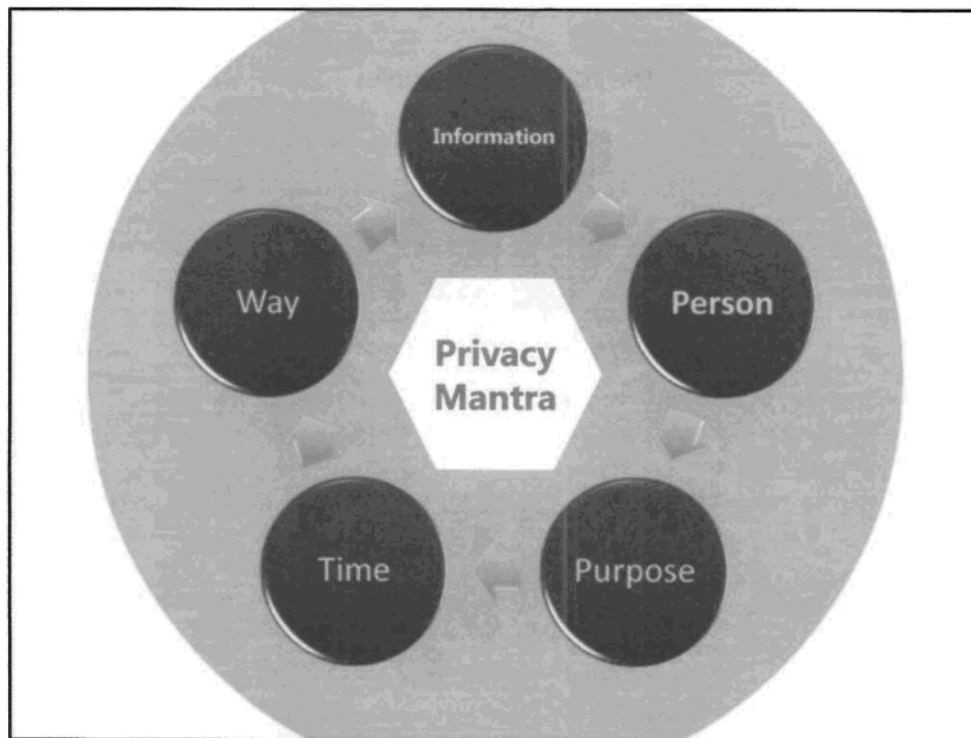
- 800,000 employees and 2.9 million customers (names, addresses, date of birth, SIN, email address)
- Information could be used for fraud/identity theft

Sony Hack- Fall 2014, cyberattack involving 40 gigs of sensitive company data stolen (emails, employee personal information)

Ashley Madison- Summer 2015- Hacker group stole user data and shared online. 32 million accounts

BC Ministry of Education- Fall 2015- Lost hard drive containing personal information- 3.4 million people in

BC/Yukon impacted

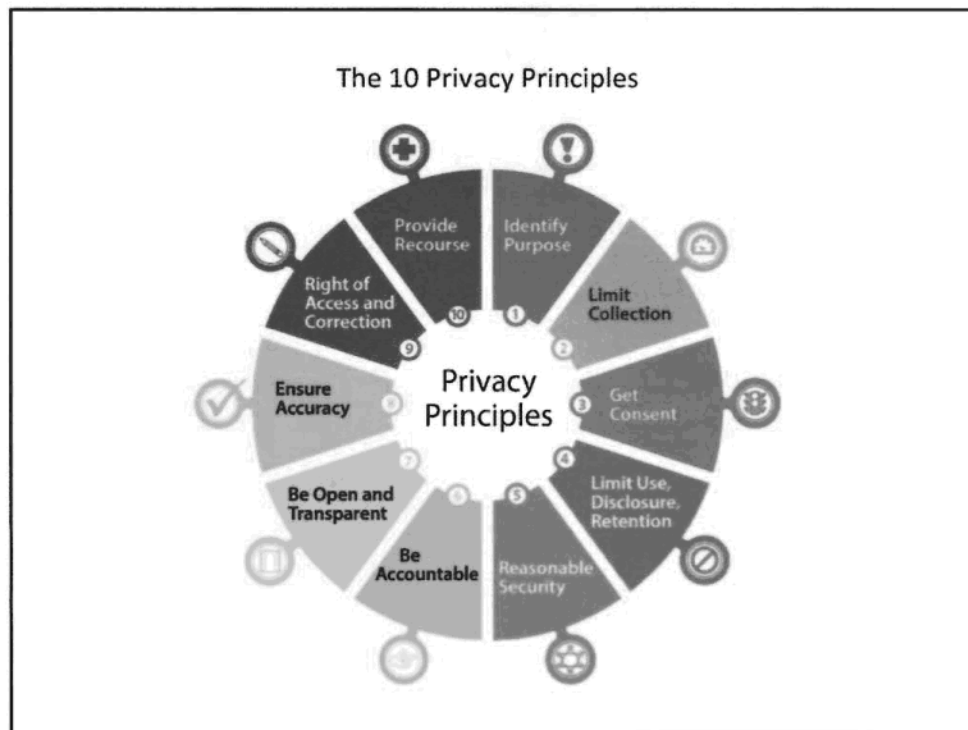


-Govt's breach management process is predicated on 5 key principles

-Border guard example positive way—negative way

-A breach of even one of these could create a breach

- Right Info- the appropriate information in the context
- Right Person- the person with authority- a business reason to have the info
- Right Purpose- a business person, a reason authorized by legislation
- Right Time- the time that is appropriate as per process policy
- Right Way- The right modality- ex: encrypted transmission



These are 10 internationally recognized privacy principles. This can be used as a tool to guide you in your work – paper handouts are in your package.

-As employees of the BC government we deal with a lot of information- be aware of your roles and responsibilities when it comes to Privacy.

-Think ahead about privacy and security to **mitigate potential risks**

-Be aware of potential privacy and security risks- keep safe the information you deal with!

-Not here to punish but here to improve and become better- we are all human we all make mistakes

-Accidental incidents can be just as harmful as deliberate incidents – focus on **training and awareness** for staff

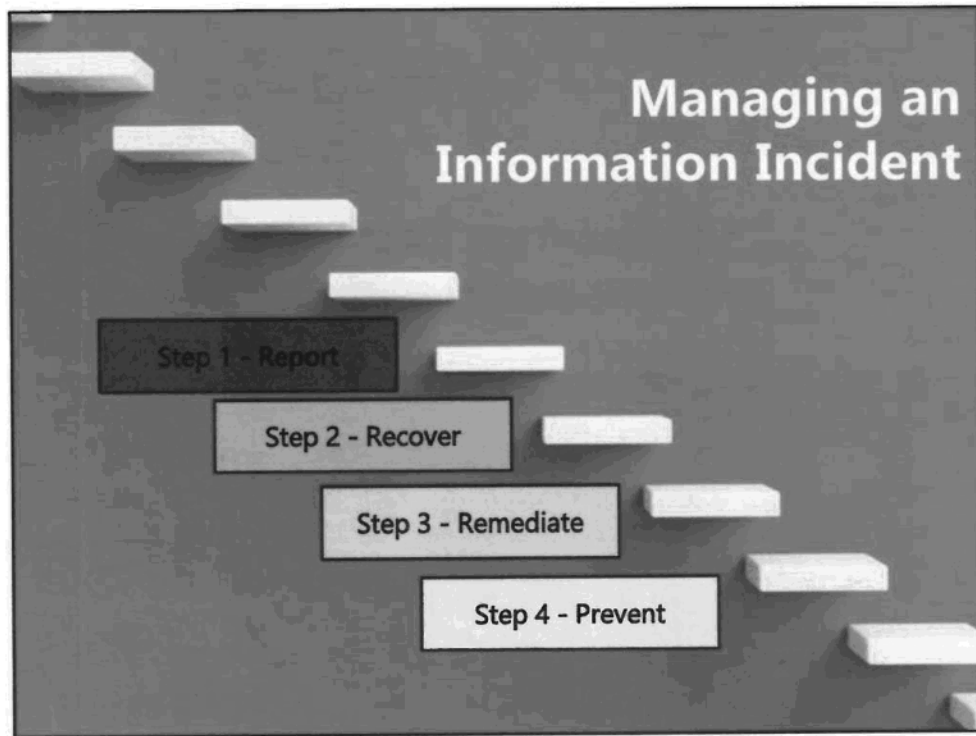
-in doubt talk to your supervisor or manager....you are a supervisor or manager....give us a call!

Play Incident Video: <https://gwww.gov.bc.ca/news/2018/0206/fear-not>

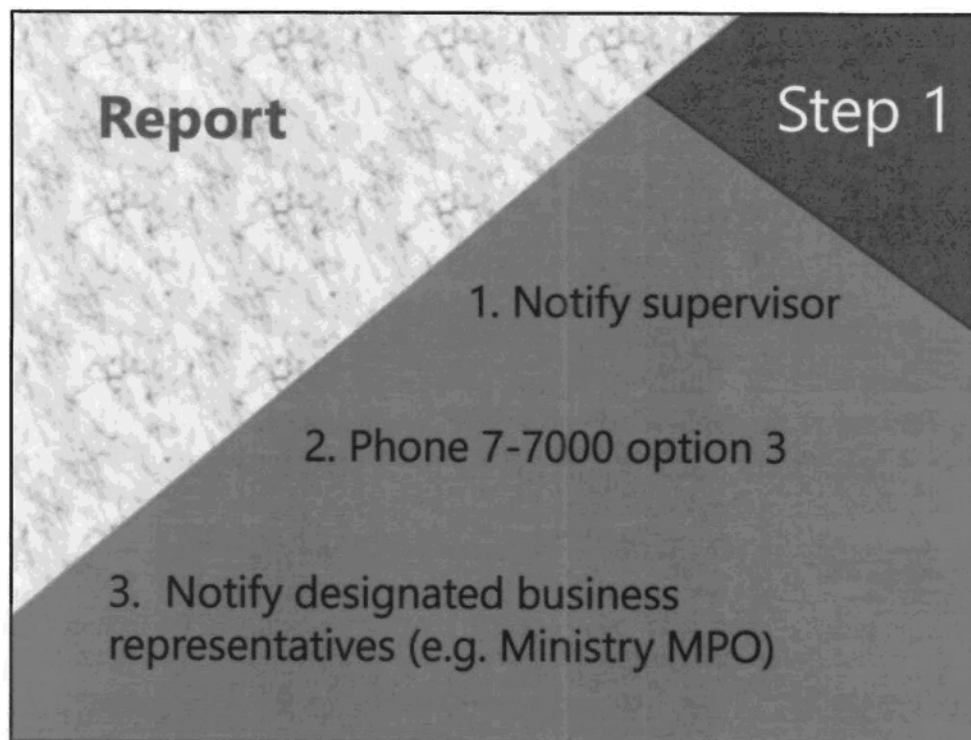
-Now, here we have the approach for all of government! There were multiple (sometimes conflicting) processes across government.

-Amount of incidents that the IU deals with- Roughly 1500 incidents last year where there was a suspected or confirmed privacy breach

-Government employee? fall under core policy? Then you are responsible for following the Information Incident Management Process



-Our four pillars of our office and the information management process



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

-7-7000 Option 3- this is for all government Ministries and public bodies that fall under core policy----everyone else (health authorities, educational bodies, Crown Corps---you should have your own process, Privacy Officers)

- Once the incident has been reported to 7-7000 the investigations unit has a 2 hour window to respond so please make sure that you an alternate contact are available. The IU will make every attempt to contact you or your supervisor (even at home)

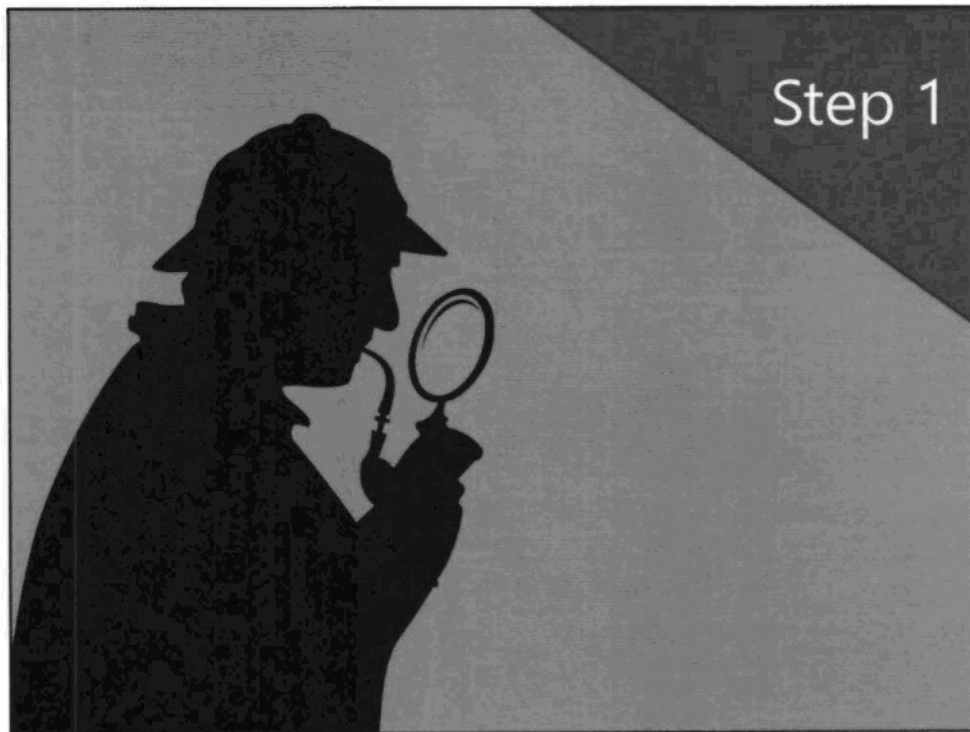
However, some ministries have their own internal processes which are in addition to the core policy and do not conflict so these will always need to be followed

– make sure you know these and follow them (SDSI process)

Sometimes even a 24 hour delay can be too much

Example of small amount of information but large consequences:

- An individual made an FOI request for their own records after going through a court case. One name was not severed out the FOI records which was the name of a witness reporter. Recipient had gang ties and the name of the individual who reported was not severed. The witness reporter had to move to a new city because they received death threats. Even after the witness reporter had moved out of town they were still harassed and followed.



-Discuss how a call will usually go: Call 7-7000 option 3, inform them you are reporting an information incident or a privacy incident. You don't need to go into detail at this stage unless 7-7000 asks you specific questions

→directed to the Investigations Unit

-Investigator contacts reporter for triage and assessment

-Don't worry if you don't have all the information, don't worry if you are not sure if it is an incident, we are here to assess the incident for you (we are the experts)

-Open a file on the investigation either suspected or confirmed: we send out an email that will inform the MPO, MCIO's and MISO's of the incident, start an investigation

-Regularly refer IT security incidents, occasionally HR incidents and threats to employees to appropriate bodies

-We will reject or refer an incident where appropriate!

-PCT Investigations Unit is responsible for investigation incidents that are the responsibility of the govt of BC- how do we determine what we can investigate?
Jurisdiction and Scope.

Jurisdiction refers to the body involved, scope refers to the information involved

Jurisdiction: Deals with what organizations we can investigate

Govt Ministries

broader public sector? No- they should have their own privacy team,
although we will provide advisory services on request

arm's length- sometimes- if they are under core policy

****contractors- YES- under contractual agreements

SCOPE: deals with what types of incidents we can investigate

cases that involve personal info i.e. privacy breaches

cases involving a violation of FOIPPA authorities

but info involved must be within scope of FOIPPA- not everything is (S. 3
defines limits EX: court records)

-we also work on incidents that involve multiple responsibilities/jurisdictions : this
requires a conversation about who is responsible for what, at the outset

A team approach to resolving incidents; PCT Investigator leads conversations related to information management. There may be parts of the conversation that are led by others (Security, PSA) where they are the experts

Collaborative approach – NOT punitive (Not here to punish, but to resolve issues)

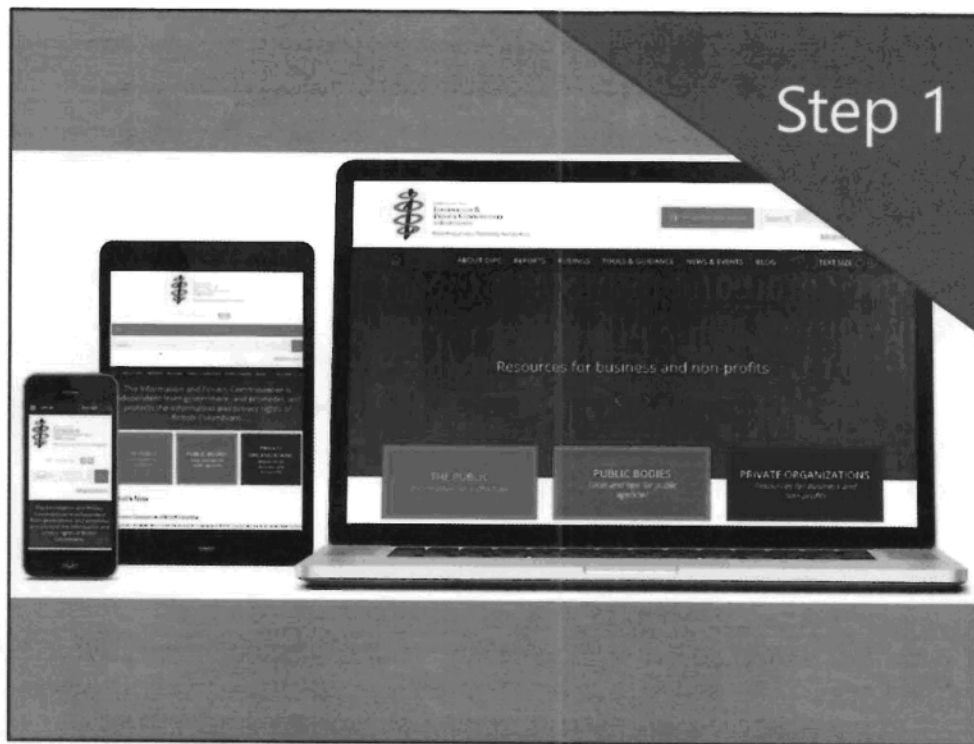
We want to help fix it and prevent it from happening again.

Don't be afraid - this is not a punitive process. Majority of incidents are accidental – staff need to feel supported / free to report these incidents.

Some MCIOs delegate to other ministry staff. (MPOs or MISO-Ministry Information Security Officer)

Partners:

- Human resources/labour relations
- IT Security and forensics
- Legal
- Law enforcement



-IU will advise a program area on what should or shouldn't be reported based on the incident and IU will liaise with the OIPC as necessary

-Oversight Body of government with regards to Privacy (FOIPPA)

-Considerations:

The sensitivity of the personal information breached

Whether the incident could result in serious harm to (an) individual(s)

Whether the incident involves a large number of impacted individuals

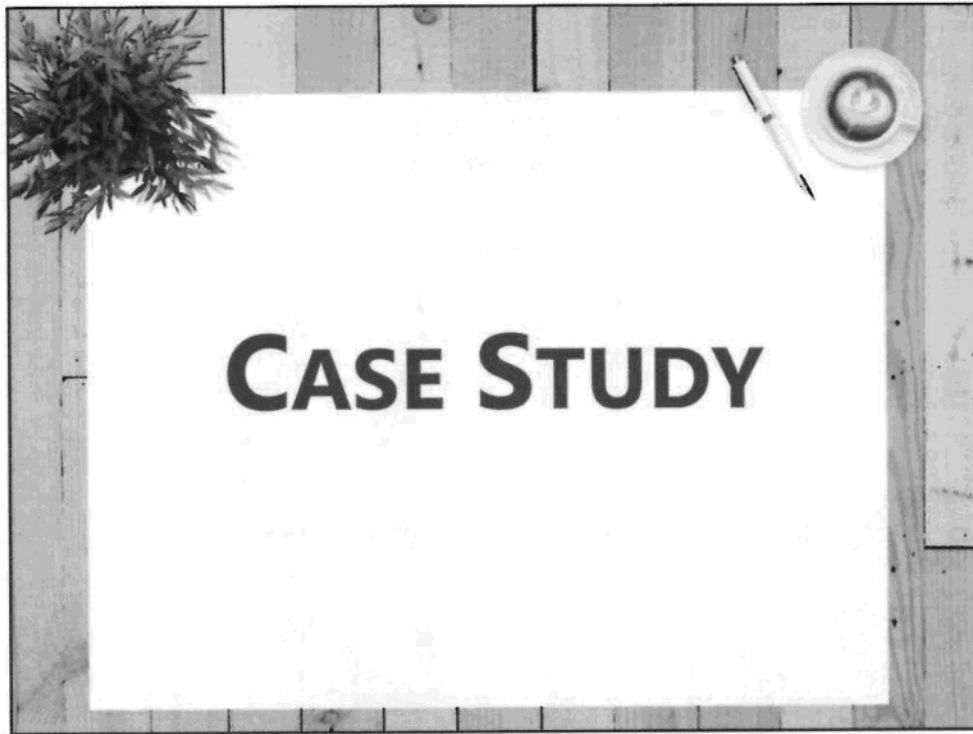
Whether the incident is, or could become publicized

Systemic issues

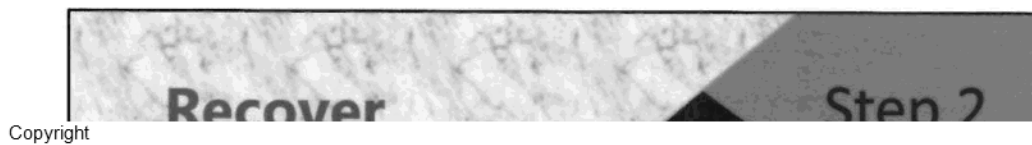
-IU sends a report monthly about all breaches investigated by our office to enhance transparency and allow the OIPC an opportunity to assess whether they want to open files on matters that don't meet the proactive reporting criteria – sometimes OIPC will request additional info, or may open a file to review, depending on the circumstances

-IU will proactively report serious breaches to OIPC

-after IU reports to OIPC, the OIPC investigator will investigate and IU will liaise with OIPC and provide updates. Doesn't change the process at all and no additional work for the Ministry. IU keeps the OIPC informed as the investigation continues.



Scenario 1A – Reporting



Copyright

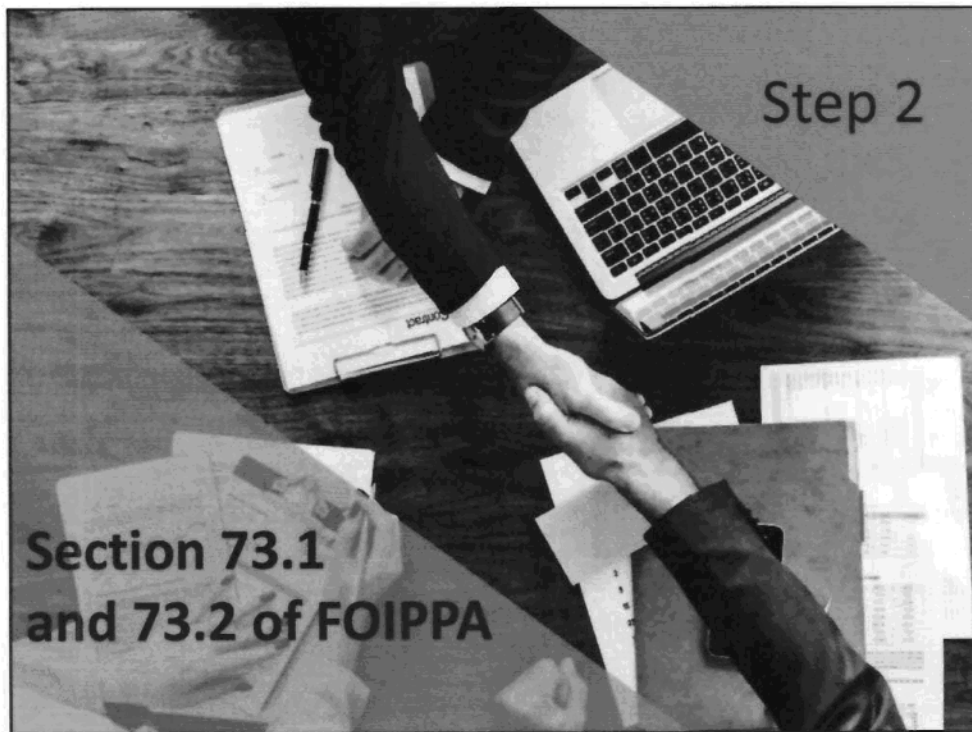
-bread and butter of the investigation: Recover exposed personal or confidential information/contain the incident

-Various tools to get containment/recovery:

- verbal confirmation of destruction/verbal confirmation that information will not be shared
- written confirmation of destruction
- Declarations/attestations
- Legal demand notices (s73.1, 73.2 FOIPPA) further below

-Sometimes it is as easy as getting confirmation of a double deletion, fax shredding, or returning of letter (written confirmation)

-Declarations are one tool that can be used as a containment or prevention measure- this is a written statement that the government employee or even individual can be given to state that they have not kept any copy of the personal or confidential information or that they will use or disclose any information for any purpose



-This is our legal authority to demand that personal information is returned/destroyed

-In most cases the Reporter would respond and state that they have destroyed the information. But what happens if they don't?

Authority derived from s.73.1 (demand notices) and s.73.2 (seeking court order) of FOIPPA

Can issue when we have reasonable grounds to believe an individual has unauthorized possession of personal information in the custody or under the control of the public body

Subject has 20 calendar days to respond in writing, and either:

- provide written confirmation that they have securely destroyed the records (on what date);
- Object to our request based on:
 - Evidence that the records were not in the custody/control of the body, or
 - That they were authorized to receive/possess the documents.

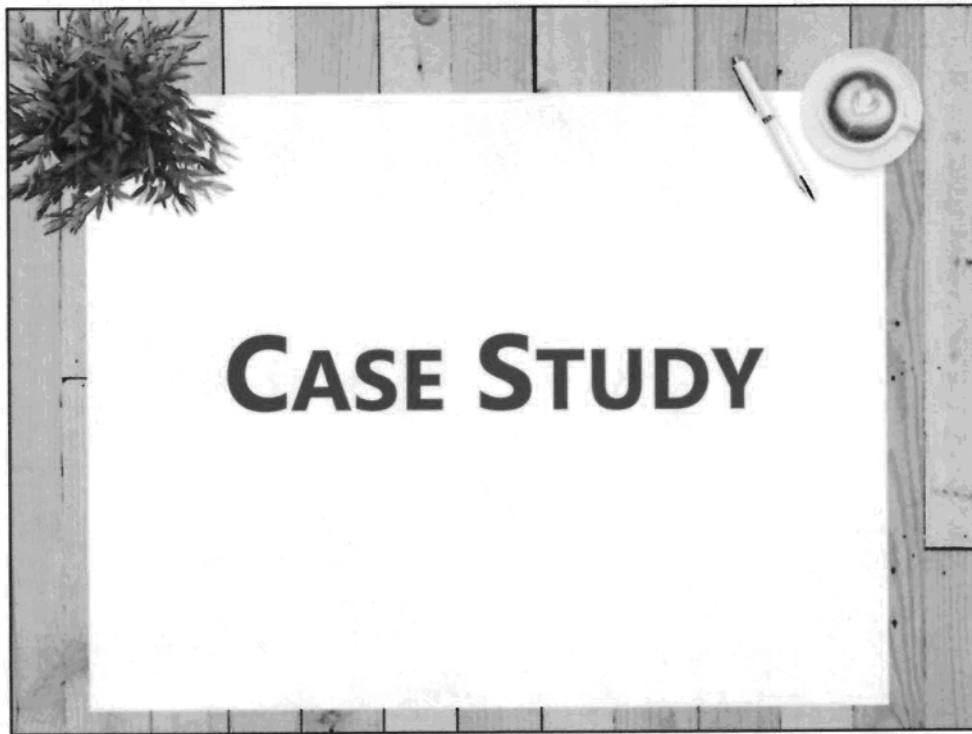
Example: a government employee has leaked 100 emails that contain information on an incident that the government was involved in, but on those 100 emails there is personal information. The employee shares this with a reporter who runs a story but also posts the 100 emails with the personal information. We send a Demand notice asking that the personal information be taken down and destroyed. Note: Only the personal information would be asked to be destroyed, we are not here to censor the Media



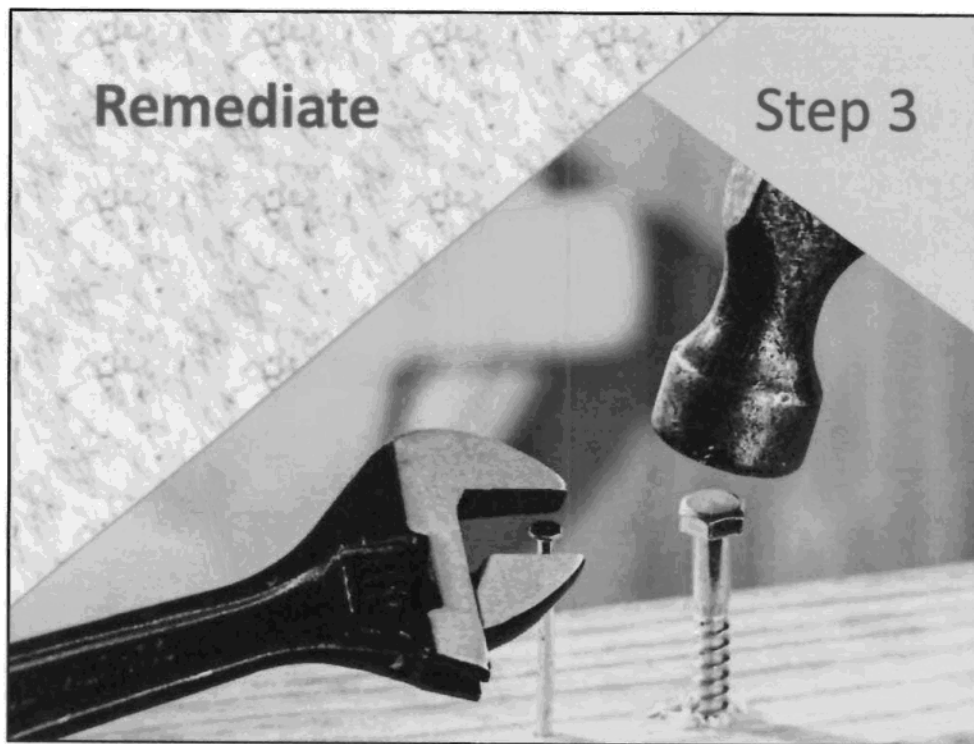
- Petition to Court (Superior Court)
- At this moment no one has ever gone to court over this
- Demand notices are the final, last resort option (~~Nuclear option~~), we look at a staged approach, don't go from 0-100 with demand notices. One step at a time, we work our way up

Considerations:

- Demand notices must come from person authorized to act as a delegate of the head of the public body (e.g. executive, legal)
- If person does not comply there are few remaining options outside of the court process
- If person fails to provide an adequate response the next step is to engage in a "petition to court" process
- Seek a staged approach to containment with an uncooperative individual



Scenario 2 – Recovery and Containment



-Assessment of the incident thus far?

-How was containment or Recovery achieved?

- Establish investigation team and incident action plan
- Find out the specifics of the incident – Who, What, When, Where, Why and How?

-This is a discussion that will occur as a team

-Looking at the bigger picture of an incident

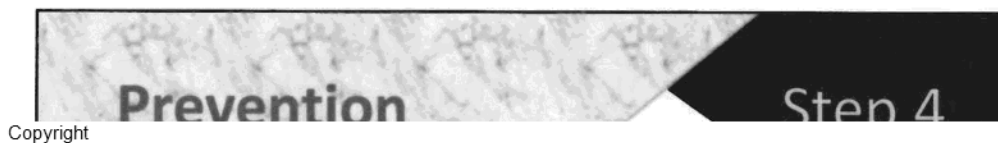
- Gather information to assess the potential for harm from the incident
 - File reviews and use of notification assessment templates
 - Need to decipher what personal or confidential information was exposed for each individual



- Notification should occur with support of Investigations Unit, try to avoid notifying before contacting the IU
- IU help assess each situation with you on if notification is recommended or not.
- Evaluate for harm
 - Sometimes notifying can cause more harm, certain wording has to be included (understanding of privacy rights)

Consider:

- Identity theft or identity fraud
 - Physical harm
 - Hurt, humiliation or damage to reputation
 - Loss of business or employment opportunities
 - Also consider potential legal or contractual obligations
-
- In the end, it is the recommendation of the IU, but the Ministry's responsibility to notify and their final decision
 - We will help you draft the wording that will be used in the notification process as there are certain requirements----we are here to assist with the process



-Favorite part of the investigation- Prevention– Learning time!

IU will discuss recommendations with ministries before making them, especially if there is any complexity and/or financial/resourcing implications

Some recommendations may be:

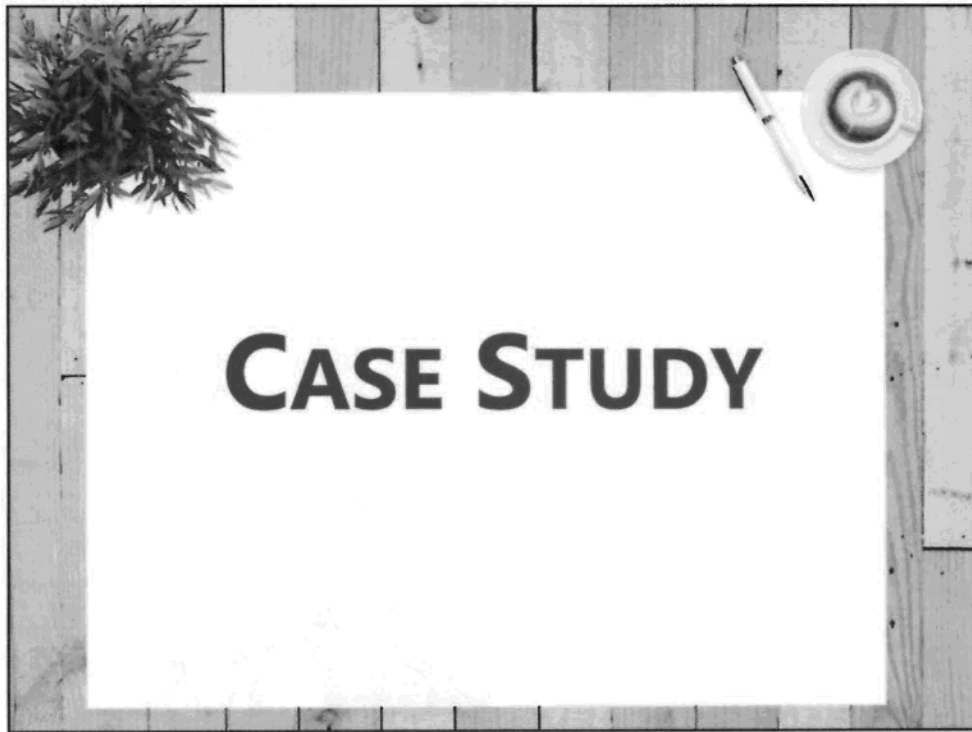
- staff coaching
- discussions with staff member
- improvement of a policy

Look for a reasonable prevention, not here to break the bank or break your office, what works to avoid future incidents

Consider for each incident

For reasonable prevention measures consider:

- Training, education, and awareness
- Policy and business practices
- Improvements to IT systems



Scenario 3 - Notification and Prevention

Copyright

250-356-1851 PRIVACY.HELPLINE@GOV.BC.CA
250-356-1851 PRIVACY.HELPLINE@GOV.BC.CA
250-356-1851 PRIVACY.HELPLINE@GOV.BC.CA
250-356-1851 PRIVACY.HELPLINE@GOV.BC.CA
250-356-1851 PRIVACY.HELPLINE@GOV.BC.CA
250-356-1851 PRIVACY.HELPLINE@GOV.BC.CA
250-356-1851 PRIVACY.HELPLINE@GOV.BC.CA
250-356-1851 PRIVACY.HELPLINE@GOV.BC.CA
250-356-1851 PRIVACY.HELPLINE@GOV.BC.CA
250-356-1851 PRIVACY.HELPLINE@GOV.BC.CA
250-356-1851 PRIVACY.HELPLINE@GOV.BC.CA

Privacy Governance

Privacy, Compliance and Training
Ministry of Citizens' Services

Copyright

Welcome!

Intro

Names and titles

Where we're from (not too detailed – have slide later on)

For reference only

Privacy governance is more than legislation – it encompasses all the processes and tools in place that help build a culture of privacy. This course introduces those elements that make up a privacy management program.

This in person, 3-hour course provides an introduction to privacy governance within any organization, including the BC public service. The course includes the following:

An overview of privacy and its importance;

Introduction to the concept of privacy governance and how the privacy management program fits into it;

Details on the elements of a privacy management program; and

Tips on how to build a positive privacy culture.

Upon completion of this course, participants will have a better understanding of the breadth of privacy within the BC public service and the requirements for a privacy management program.

Image source: Graphic Design Unit photo database

A world without privacy.



Ask everyone to turn to the people beside them

What happens in a world without privacy?

Prompts:

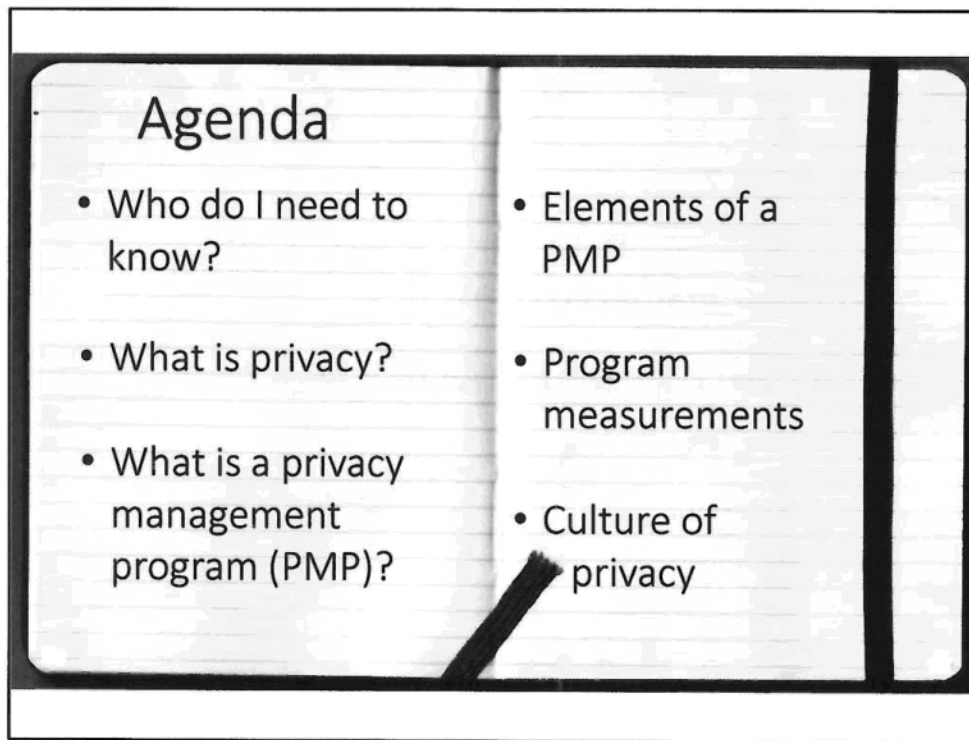
- Perspective
 - Individual, business, public body
- What would be different?
- What would be positive, what would be negative?
- What assumptions do we have about privacy?

Give them 3 mins and ask them to come back with their thoughts

Encourage people to think of the benefits as well as the negatives

-e.g. convenience; marketing would be easier (could track preferences and target the marketing)

Image source: https://c1.staticflickr.com/6/5228/5679642883_24a2e905e0_b.jpg



In a world where the benefits of technology increasingly override our privacy, how do we manage privacy?

- We'll walk you through the privacy landscape within the public sector
- Provide tips on what a privacy management program should include

Introduce agenda:

- Who you need to know
- Brief overview of privacy
- Introduce the concept of privacy governance and how the privacy management program fits into it
- Detail elements of a privacy management program
- Discuss program measurements
- And throughout, we'll provide tips to build a positive privacy environment

-encourage questions throughout

-encourage participation – this is a venue for like-minded professionals to learn from each other (your successes and challenges)



PCT is government's
corporate privacy office.

PCT

Corporate Information and Records Management Office

Essentially, our branch = government's "corporate privacy branch"

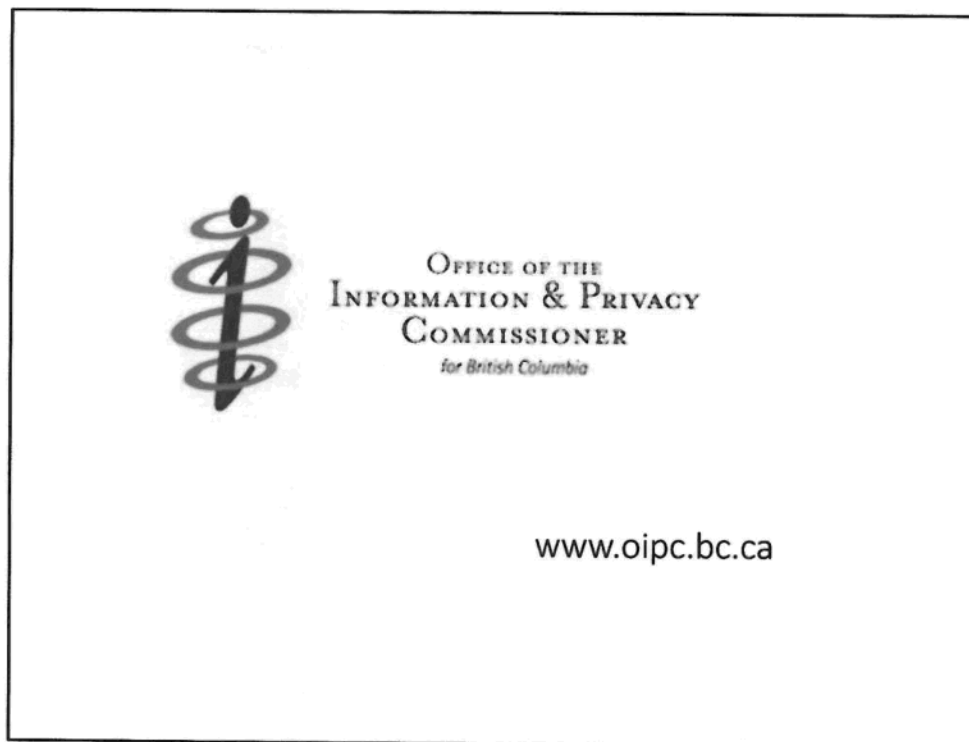
- Experts on FOIPPA
- Lead strategic privacy initiatives across government
- Establish government policy, standards and guidelines on access and privacy issues
- Provide services, support and leadership to assist ministries and other public bodies in complying with FOIPPA
- Provide input and advice on legislative proposals and reviews
- Provide privacy training across the province

The importance of knowing who we are is knowing how we fit into a privacy management program.

Are we a support for you? Should we be? If you are within a ministry – do you understand our overall role within government?

-ask audience where they are from

-Public? Private?



OIPC

- established in 1993
- Commissioner (OIPC) provides independent oversight and enforcement of BC's access and privacy laws

Michael McAvoy is the Acting Information and Privacy Commissioner

What OIPC does:

- Conducts reviews and investigations to ensure compliance with FOIPPA
- Mediates FOI disputes
- Comments on FOI and privacy implications of proposed legislative schemes or public body programs
- Provides useful resources regarding previous decisions/orders
- Where organizations outside the BC gov can go for help with PIAs
 - Ministries are required to come to PCT

-explain that OIPC can only be reactive if they aren't kept informed

-e.g. should consult with them on surveillance projects, projects dealing with vulnerable populations

Similar to our branch – how does the OIPC fit into a privacy management program?

They are obviously a regulator or watchdog for all of us (in BC), but for organizations not bound by FOIPPA, they also review PIAs, or answer routine questions from you.

Note for presenter: typically this will silence the room – point is that people don't walk around with a definition of privacy

-so we can address why we're here

Potential activity:

Throw this one out to the audience.

Use the flip board again to write out responses.

-this and next slide could be a 10-15 min conversation depending on audience

-ask audience to define privacy

-think of how we feel it in our day-to-day

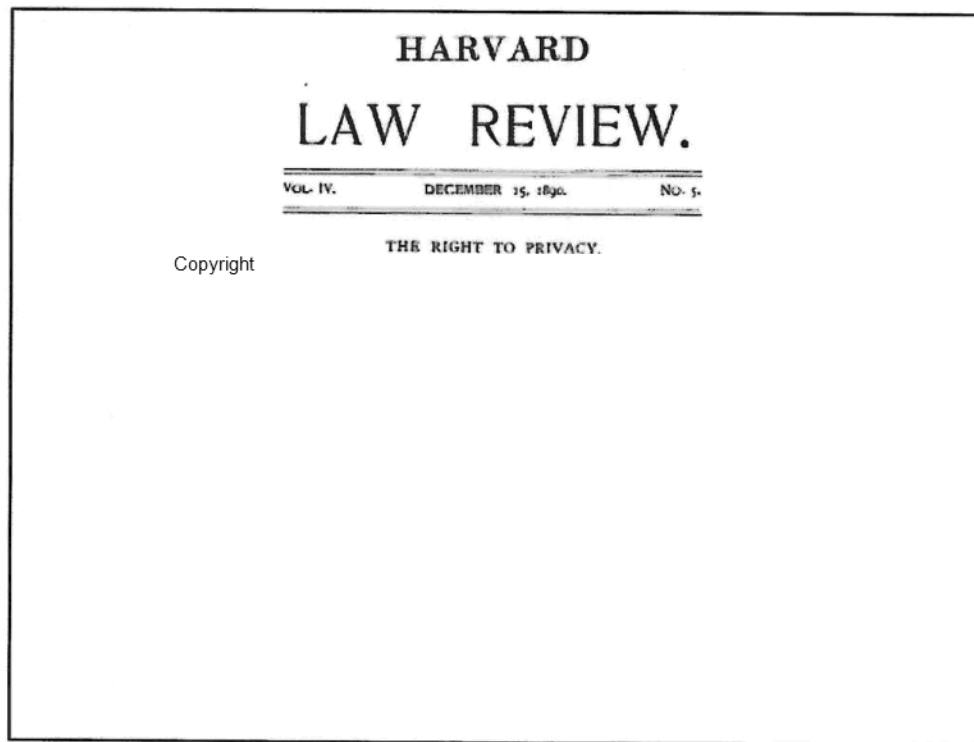
-e.g. when it's infringed upon

-privacy is about choice, but how do you manage choice?

Privacy:

- None of the statutes define "privacy" but aim to achieve it with rules for how personal info is to be collected, used and disclosed

Image source: <https://pixabay.com/en/boy-child-confused-person-61171/>



-1890, law review article written by Samuel Warren and Louis Brandeis and published in the *Harvard Law Review*
-considered to be influential and the first publication in the US to advocate a right to privacy

-defined privacy as the right to be let alone
-especially in relation to appearing in newspaper stories – cameras a new technology at the time
-technology can often trigger a privacy discussion

Today privacy is more about **informational self-determination**
(you get to choose what happens to your information)

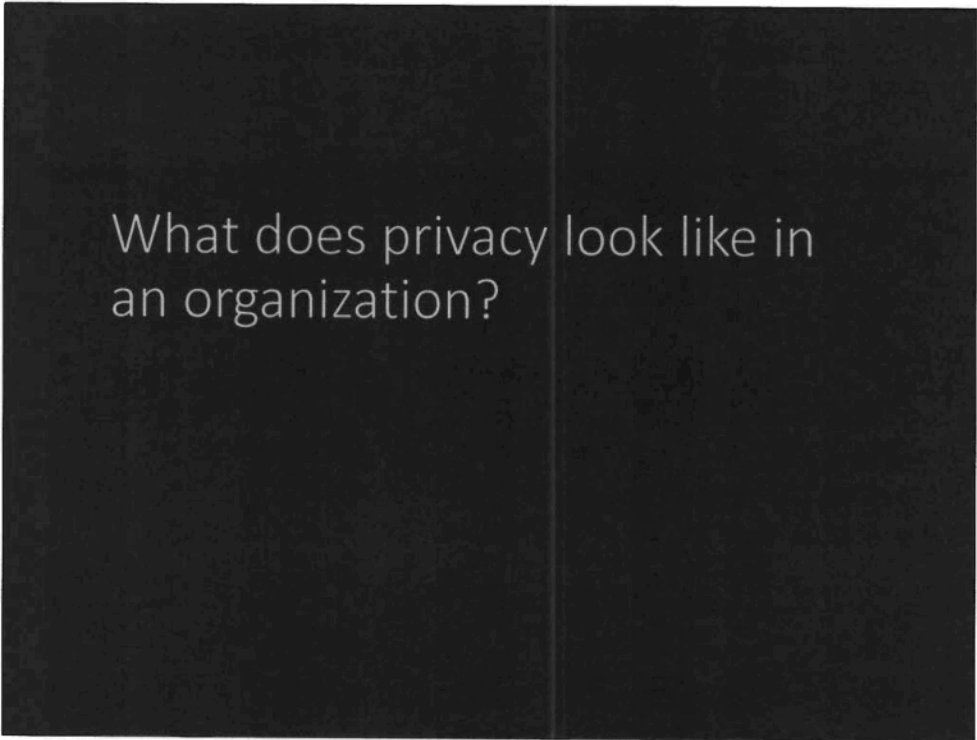
- Informational self-determination is not the law, but is the underlying principle
 - e.g. if you robbed a bank, your physical description (personal info) is now handed over by witnesses to the police – even though that individual doesn't want their personal info out
- Privacy is about having a choice

With choice comes the need to weigh options

- Think of how much of our privacy we'll give up for convenience, fame, etc.

Pictures demonstrate this:

- Top left: performance artist had attendees at an Brooklyn arts festival trade their private info (image, fingerprints or social security number) for a cookie; people even proudly tweeted about it
- Top right: celebrity culture and the attempt to get back lost privacy
 - think of how privacy was previously defined as the right to be let alone
- Bottom left: person using their sweater as a privacy screen
- Bottom right: tourists on Hollywood Blvd gave away their passwords on live TV for a split-second of fame on Jimmy Kimmel Live
 - <https://www.youtube.com/watch?v=opRMrEfAlil> (start video at 0:42)

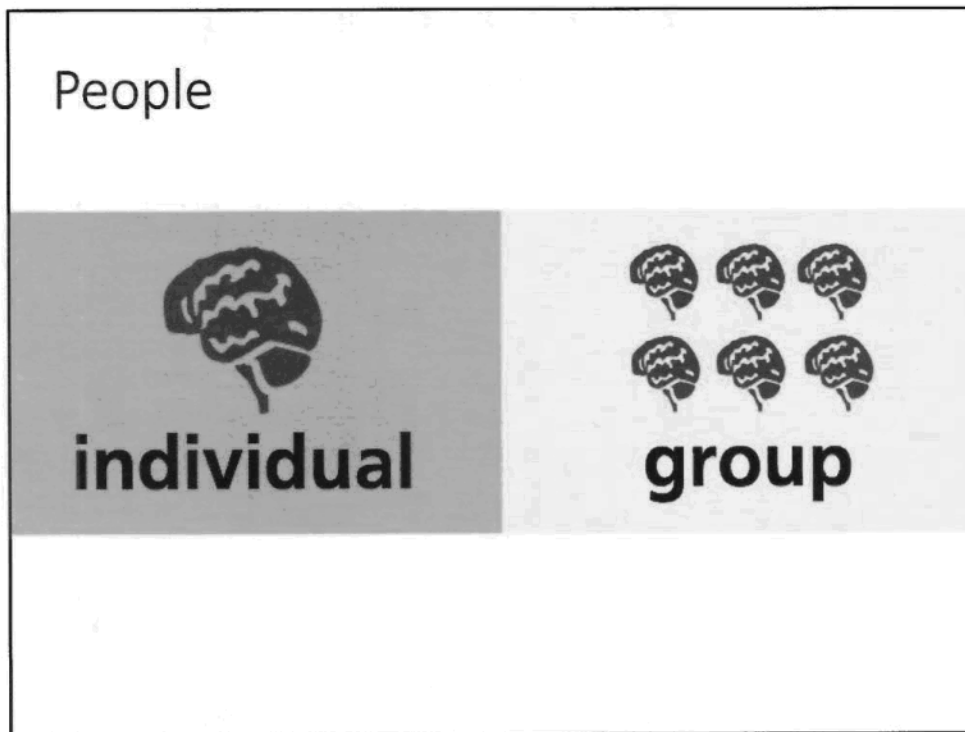


What does privacy look like in an organization?

What does privacy look like in an organization?

Just to help you think through this a little bit, we'll use 3 buckets for where you'll encounter privacy within an organization:

- people – getting everyone on board and on message
- programs – consultations, new systems, etc.
- technology – phones, etc.



People:

- With privacy, it's important to have everyone on board and on message
- This speaks to practices. Privacy Officers – those designated to manage privacy for an organization – should be concerned about what people are doing, and how they do it. Are there secure shredding bins for people to use; do they know how to not become victim to auto-fill in Outlook; etc.
- This is privacy on an everyday level. It is probably one of the hardest to speak to because it is impossible to keep people from making mistakes
- In sum, people create privacy problems – so orgs have to think about how to manage the people side of privacy.

Image source:

https://www.google.ca/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=0ahUKEwj53J-BqMHYA hVB42MKHf_3AiAQjRwIBw&url=https%3A%2F%2Fwww.flickr.com%2Fphotos%2Fsmemon%2F5162224869&psig=AOvVaw145FM6pXN99pwrX8G1vQcT&ust=1515258478462147



Programs

Programs:

- Programs are a little bit like groups of people but also a little bit different. For programs, rather than thinking of what people work on the programs, think of the nature of the work itself.
 - Is there a marketing or citizen engagement aspect?
 - Is the nature of the work more technical?
- Think of the programs that are important to manage from a privacy perspective. This is where proactive measures can be put in place to ensure privacy is managed at the right time and in the right way.
- I will give an example – we have the BC Services Card program in the BC Government. This is a program that contains a lot of people, doing a lot of varied work. Some technical people, some policy people, some program people. But we have established a really positive relationship with this program whereby we have regular check ins, we have a clear process on how to engage, etc. We have worked to ensure really positive privacy outcomes, but building a relationship with not just the people (because some have turned over), but with the program as a whole.
- Take a moment to think about or identify if there are programs within your organization that as discrete entities would benefit from having a more formalized approach to privacy.

Image source: Graphic Design Unit photo database



Technology:

- You can work really well with the people, and that is positive in the now. You can work well with a program, and that sets up for the medium term, but if you really want to establish a longer term privacy enhanced program, you also need to think about the third and final bucket. You need to think about the technology. You can have the same people, working in the same places for 10 years, but the privacy problems that they will produce in those static places are fundamentally different year over year. Because of their technology.
- Let's take as an example social workers – or perhaps even just front line staff in any of your organizations – counter staff, ferry staff, practitioners, etc. How different is their relationship with the public given the use of a high tech device? For the social worker, there is this added opportunity or desire to engage not by phone call into an office phone, but via text message. Or via social media. Or via some other means. And this absolutely changes the privacy problem. Phone calls are more public because people can overhear things, but text messages are more permanent so are more able to be read by others. This changes how you need to train the PEOPLE to work, because it becomes a practice thing.
- So an organization needs to manage changing technology
- Think of what a phone looked like and it's functionality before it became a portable technology
 - Now it's a mini computer and must be managed differently
- These changing technologies will have an impact on privacy within your org

Image sources:

Left – <https://commons.wikimedia.org/wiki/File:DynaTAC8000X.jpg>

Right – https://commons.wikimedia.org/wiki/File:Samsung_SPH-M300_Cell_Phone.jpg

Middle –

https://www.google.ca/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=0ahUKEwiYkuirrcHYAhVM32MKHbWyCysQjRwIBw&url=https%3A%2F%2Fwww.pexels.com%2Fsearch%2Fsmartphone%2F&psig=AOvVa_w3YFxrRkhMCQ-v4Zyz0kfHB1&ust=1515259831890541

Privacy is:

- Subjective
- Contextual
- “Negative”

Privacy is:

- Subjective
 - Different to me than to someone else
 - How I feel about privacy, working in the field, is very different to my 11-year old who just wants to play his online game already (doesn't care if game is tracking his location)
- Contextual
 - Different across cultures, time, generations, etc.
 - E.g. privacy for a 70 year old will differ from a teenager's view of privacy
 - 70 year old may focus more on right to be left alone (closes curtains)
 - Teenager will think about the settings on their phone and social media
 - Can flux depending on personal vs work life
- Negative form of privacy
 - You're often not aware of your privacy until it gets infringed uponExamples: airport body scan, bag search

How can an org manage something as subjective, contextual and fluid as privacy?

- Through privacy governance



Ok, what is privacy governance?

- Not just a public sector buzz word
- Refers to the structures and processes that ensure an organization's accountability
- Governance tells an organization's staff how to do a function
 - Provides rules to follow

From: <http://www.unesco.org/new/en/education/themes/strengthening-education-systems/quality-framework/technical-notes/concept-of-governance/>

Governance:

- refers to structures and processes designed to ensure accountability, transparency, responsiveness, rule of law, stability, equity and inclusiveness, empowerment, and broad-based participation.

Freedom of Information and Protection of
Privacy Act (FOIPPA)
Personal Information Protection Act (PIPA)

Personal Information Protection and
Electronic Documents Act (PIPEDA)
Access to Information Act
Privacy Act

For privacy governance, you'll be working within the legislative landscape

FOIPPA

- Public sector access and privacy legislation
- Applies to "public bodies" in BC

Before 1993:

- No set rules for what info a public body could collect

After 1993:

- FOIPPA passed
 - Protects personal privacy by preventing the unauthorized collection, use and disclosure of personal info by public bodies
 - Has to cover all public bodies for all things
 - So isn't going to explicitly cover technologies like cloud

PIPA

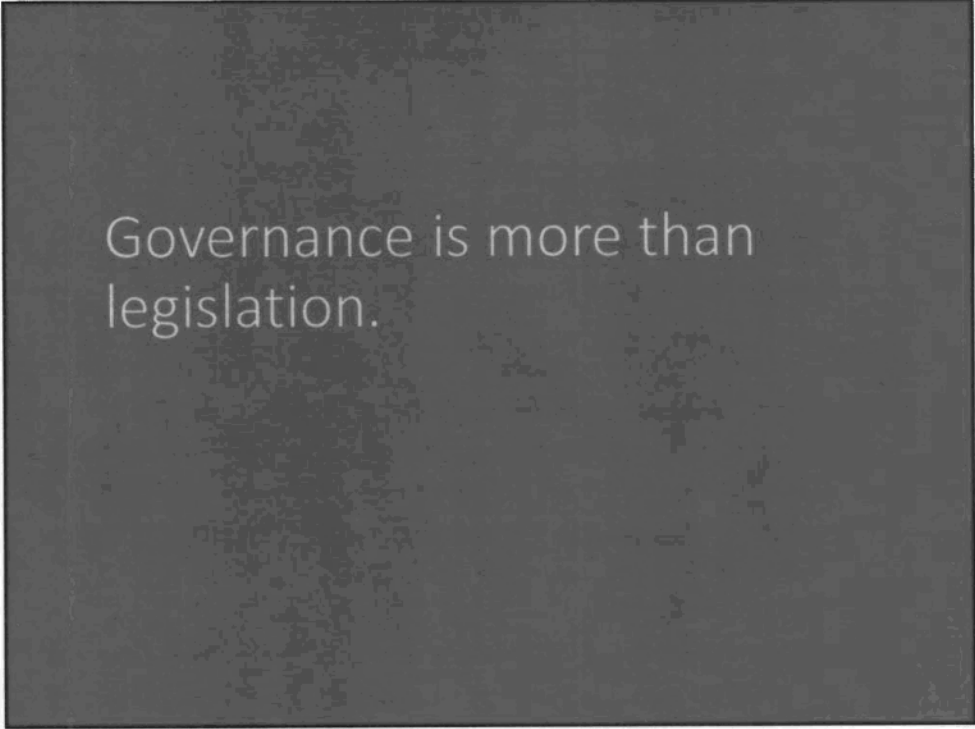
- Private sector privacy legislation
- Applies to "organizations" (more than just businesses) in BC
 - e.g. non-profit organizations, charities
- "Common sense" rules for collection, use, disclosure of PI – consent-based
 - FOIPPA = authority based

PIPEDA

- Applies to federal works, undertakings or businesses
 - banks, airlines, and telecommunications companies
- PIPA BC specific

Canada's *Access to Information Act* and *Privacy Act*

- Federal equivalents to BC's FOIPPA
- Applies to Federal Gov't institutions and federally regulated institutions



Governance is more than
legislation.

But governance is more than just legislation

Ask the audience: What makes for “good governance”?

Incorporate audience answers in discussion of the following elements of “good governance”:

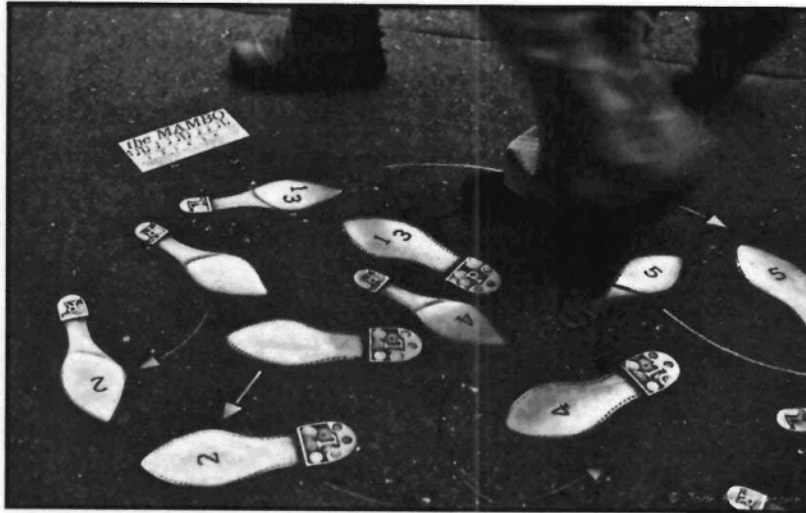
“Concrete” elements that make it up...

- Technology
- Law
- Market
- Consumer/citizen choices

“Soft” elements

- Integrity
- Accountability
- Ethics
- Stewardship (looking after privacy on behalf of British Columbians/clients)
- Transparency
- Leadership

First step: Privacy Management Program



First step is to build a privacy management program

Ask the room who has a privacy management program in their org

Get them to think of the sum total of their privacy work in their org

As we go through the elements, they may see that they already do things that are part of a larger privacy management program

A privacy management program is the sum total of how you treat privacy within your organization. By calling it out as a program, we are no longer onside of the law by chance, but we are onside the law by design.

We will use a standard privacy management program to walk through some of the nuts and bolts of exactly what this program should entail. This doesn't mean that orgs can't do other things. But these are the big ones. These are the things that orgs should be prepared to answer for if pressed by someone – say for instance the OIPC. But more importantly, these are the things that orgs should be prepared to answer when in a crisis situation. If the OIPC is demanding of your org – how to manage this or that – is this something that your org wants to have to solidify in that moment, or something that your org will have already prepared.

Image source: https://c1.staticflickr.com/8/7053/6858612077_1429297229_b.jpg

Executive support is crucial.

- Executive-level support is key for a privacy-aware culture and a successful privacy management program
 - Support will include resources and funding
- Some areas will have Executive support and some will be struggling with it
 - Can anyone think of tips to get Executive on board?
 - E.g. breach numbers

To govern privacy is a never ending process. A bit like preparing for an exam – when is enough enough?

This creates a bit of a dilemma in that executive may see privacy as a money pit, where they throw money into it and they don't see any return. And there will never really be a return, will there? Having a net result of "nothing" would be great, right? How do you show that people didn't do the terrible thing that they might have if you hadn't trained them, consulted with them, or responded to their issue in a timely way.

This is where the Privacy Officer for an org becomes crucial.



Designate a Privacy Officer.

Each org should have a Privacy Officer

Privacy Officers have organization-specific privacy knowledge.

Privacy Officers:

- Responsible for an organization's compliance and privacy practices
- They are the critical fulcrum between privacy law/privacy practices and the business operations of the organization in which they work
- POs need to know the people, programs and technologies in their org – remember what we talked about earlier in terms of what privacy looks like in an org
- PO needs to be solutions oriented and be on the side of the organization
 - Can't be in a privacy bubble

Example of work PO's do:

- Each ministry's Privacy Officer is responsible for implementing the privacy management and accountability policy in their ministry
 - Serve as ministry staff's primary contact for privacy-related questions

MPO also:

- Manages their ministry's specific privacy training and policy needs
- Reviews all privacy impact assessments, information sharing agreements and research agreements before they're completed

Empower a Privacy Officer.

- Win if org even has a PO
 - Better if that PO is empowered to do their work
- PO needs support in terms of resources
 - In order to effectively manage all potential privacy problems, a Privacy Officer would have to be hanging over the shoulder of every single employee – which is obviously not feasible.
 - So there's the question of resources and the question of "when is it enough" in terms of the privacy work put in place
 - PO will determine what can be done given their specific resources, culture, etc.

Build a culture of privacy
through training and
awareness.

- Since Privacy Officers can't be everywhere at all times:
 - Need to build a culture of privacy
 - Do that through relationship building and problem solving (not an office of no)
 - Are proactive with Executive and staff
 - Breach reporting – normalize this as part of everyday privacy
 - Awareness building and success reports – Executive and staff shouldn't only hear from a PO when something bad happens (creates a fear-based image of privacy)
- Training and awareness programs are a good way to introduce and strengthen privacy within an organization
 - Also lets an organization know who their privacy contacts are (provides a face)

Informed organization:

- Helps staff be privacy compliant
 - Takes the mystery out of privacy
- Helps staff identify privacy issues, including breaches
 - Means breach reporting may rise with the level of privacy awareness

Requirements for privacy training:

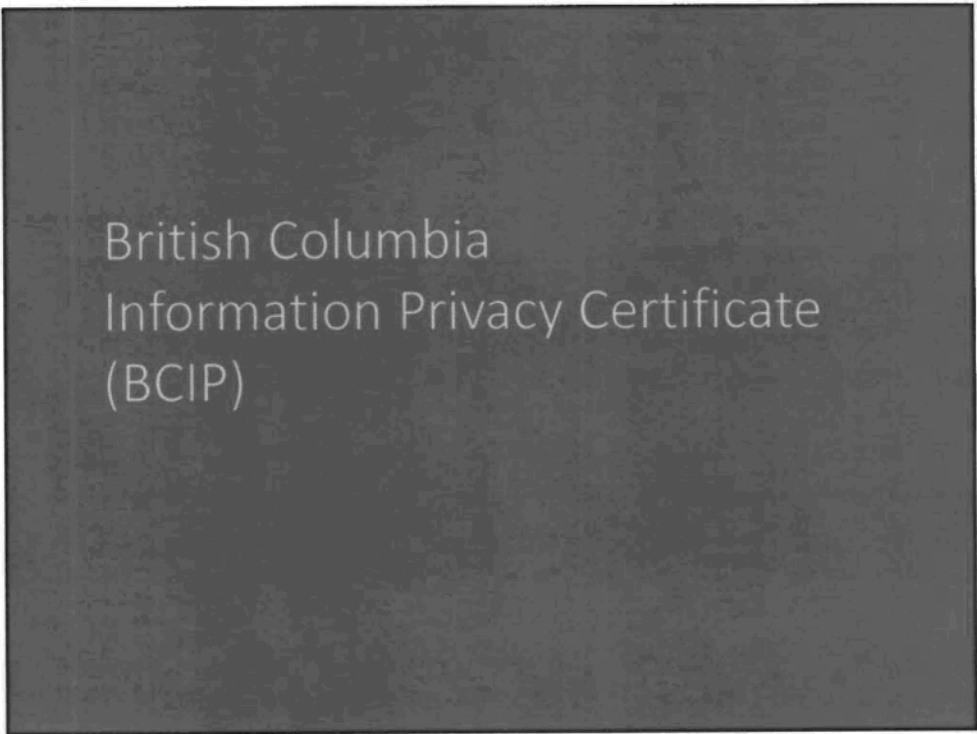
- Mandatory
- Tailored
- Ongoing
- Reviewed and updated

Privacy training should be:

- Mandatory
- Tailored to specific duties
- Ongoing
- Reviewed and updated as appropriate

Examples from gov:

- Mandatory training
 - IM117 for all staff and Executive
 - Contractor training – Privacy and Information Sharing through Open School BC (OSBC)
- Tailored training
 - Ad hoc sessions dependant on need
 - For gov, broader public sector and private sector orgs
 - Privacy and Access Helpline for requests
 - BCIP certificate program – launched in April
 - Mention attendance list and mailing list for BCIP
 - Mention attendance list for IDIM staff

The logo is a dark grey rectangle with the text "British Columbia Information Privacy Certificate (BCIP)" in a light grey, sans-serif font. The text is centered and arranged in four lines: "British Columbia", "Information Privacy Certificate", and "(BCIP)".

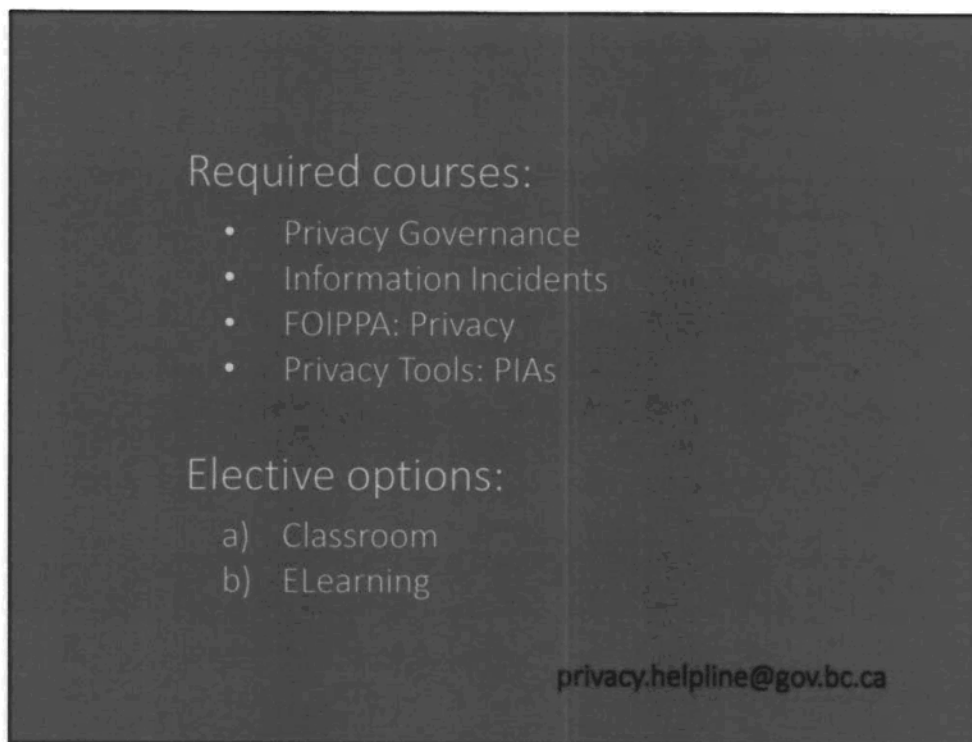
British Columbia Information Privacy Certificate (BCIP)

Description

The new British Columbia Information Privacy Certificate Program (BCIP) offers comprehensive privacy training designed specifically for the provincial public sector.

For:

- Employees committed to protecting privacy and those preparing for a career in information privacy
- Or those who want a better understanding of how privacy and FOIPPA impacts their work



(no need to say all of this – summarize; these notes are for reference)

Courses

To complete the certificate, participants must finish four interactive classroom courses and an elective option.

The four classroom courses are each three hours in length, are scheduled approximately every two months over the coming year:

- Privacy Governance
- Information Incidents
- FOIPPA: Privacy
- Privacy Tools: Privacy Impact Assessments

In addition, participants must select one of the following elective options:

- a) Classroom
 - FOIPPA: Access
- b) ELearning (Note: All three courses must be completed)
 - IM 112: Managing Government Records
 - IM 114: A Day in the Life – Information Security and You
 - IM 118: Information Security and Awareness: Supporting Employees in the Workplace

Enrol

To enrol, email the Privacy and Access Helpline.

Note: The classroom courses are only available in Victoria for the time being. They can also be taken independent of the certificate program and in any order.

*No cost to take the program except if you need to travel to Victoria (that cost will be the responsibility of the participant).

PCT delivers the program.



So how do you create impact with your training and awareness endeavors?

Engagement opportunity:

- Have the audience think of how to make training an impactful tool
 - E.g. training 5 executives for 15 mins. compared to 40 staff for 1 hr

Image source: https://commons.wikimedia.org/wiki/File:Impact_font.svg



- promote privacy in creative ways
- privacy can be a hard sell

Use different formats:

- Group training
- One-on-one training
- Webinars
- Fun, informative videos
- Gamification (e.g. game show host)
- Contests
- Newsletters
- Info booths
- Take advantage of privacy week (in May???)
- Community of practice
 - e.g. gov's Privacy Smart Community of Practice (PriSm)
 - Celebrate successes
- For training, think of what you need them to do or be able to do

Image source: <https://www.flickr.com/photos/ben124/14695359673>

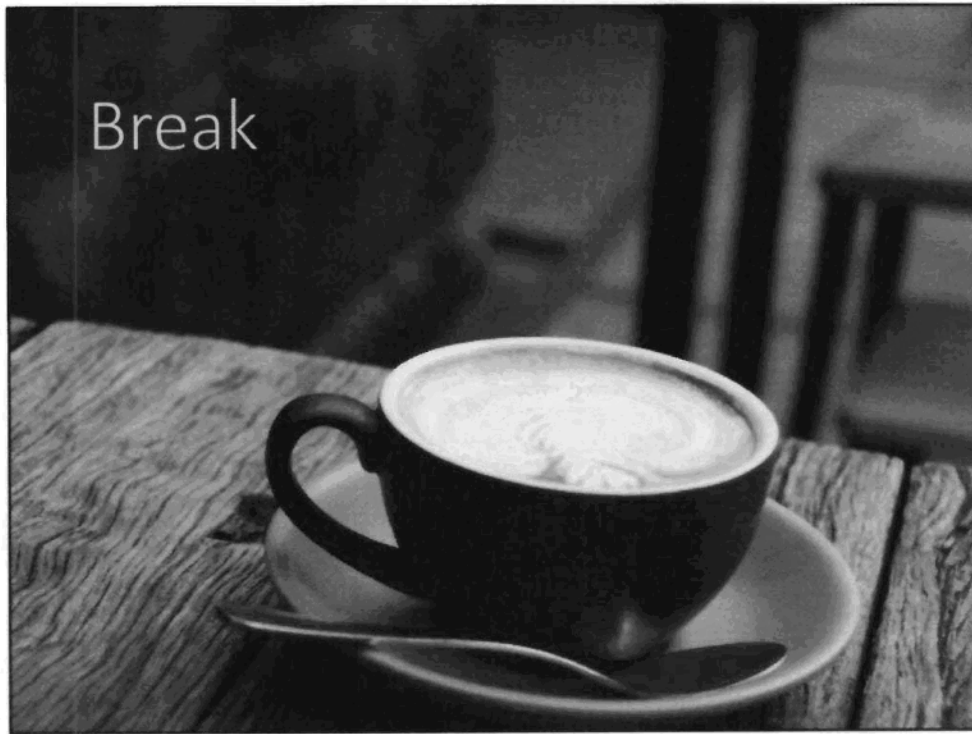
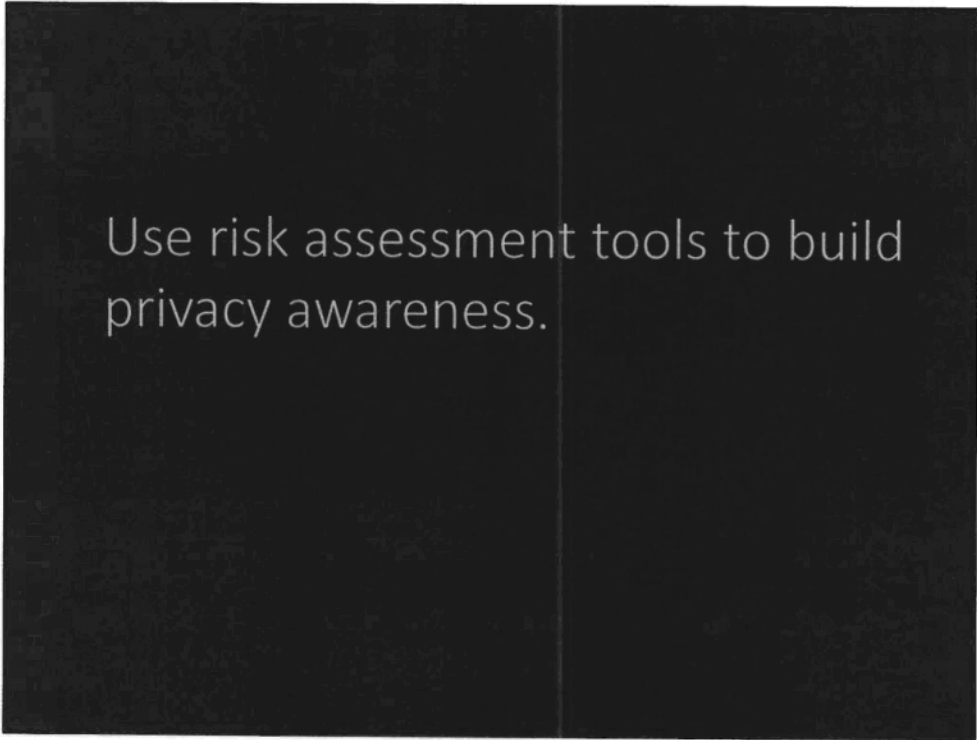


Image source: <http://maxpixel.freegreatpicture.com/Table-Drink-Coffee-Cup-Coffee-Coffee-Break-Break-2725265>



Use risk assessment tools to build privacy awareness.

Moving on to risk assessment tools, which help build privacy awareness in an organization

PIA is one type of risk assessment tool

PIA process itself can be an educational tool

- Participating in PIAs promotes privacy awareness
- Helps those involved to think of their project from a principle perspective

What's in the
tool box?



Let's look at some privacy tools that will help your organization assess privacy risks

Image source: https://cdn.pixabay.com/photo/2016/07/29/08/49/tools-1551457_960_720.jpg

A Privacy Impact Assessment has multiple benefits.

Benefits of completing a PIA:

- Can ensure privacy requirements are identified and satisfied in a timely and cost efficient manner
- PIA process is also designed as an educational tool – participating in PIAs promotes privacy awareness
- The PIA can make the difference between a privacy invasive and a privacy enhancing initiative, without compromising business objectives or adding significant costs
- Meet your legislated requirements

-PIA is usually first point of contact people have with Privacy Officer

-will change how people feel about Privacy Officer role

-for those filling out a PIA: focus your attention on the first question – what are you doing?

-set the assessment up in a way that fits with your org

Contents of a PIA

Part 1 – General Information

Part 2 – Protection of Personal Information

Part 3 – Security of Personal Information

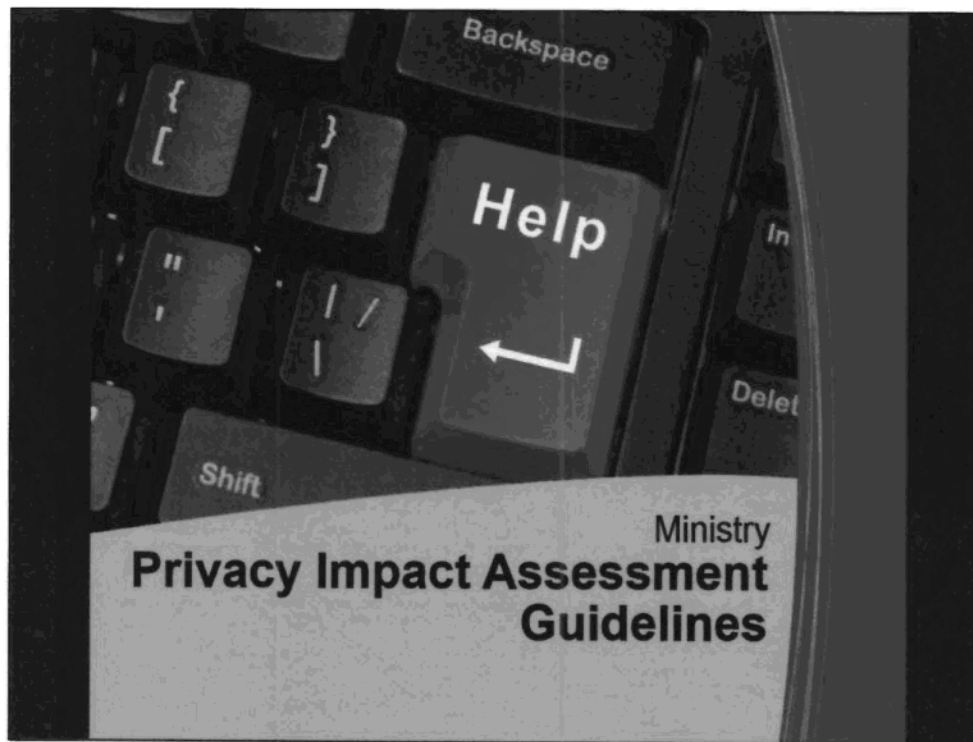
Part 4 – Accuracy, Correction and
Retention of Personal Information

Part 5 – Further Information

Part 6 – Comments/Signature

- PIA templates are on our site
 - For public and private sector bodies

-template designed to walk you through privacy considerations rather than being a checkmark exercise



- PIA guideline is online
 - Will help non-ministry public bodies and private organizations as well

https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/information-privacy/privacy-impact-assessments/pia_guidelines.pdf

Complete a PIA during the development phase.

When do you do a PIA?

- During the development phase of a new program, project, system, legislation, technology, or other initiative; OR
- Before the implementation of a significant change to an existing program, project, system, technology or information system, or legislation takes place; OR
- For all significant existing programs/initiatives

Complete a PIA whether personal information is or is not collected, used or disclosed

- FOIPPA doesn't distinguish
- Sometimes personal information is identified during the process

There are reasons for these rules:

- Pushes assessment of whether PI is involved to privacy experts
- Supports the culture of privacy
 - Helps normalize privacy into the everyday dealings of orgs – if we can streamline the process for PIAs in easy situations, then people will be more likely to do them

Reason for development phase piece:

- Builds an environment of proactive privacy – of dealing with privacy before it becomes a problem
 - If every time a PIA is submitted it is done on the day before the program launches, then people will view privacy as a problem (because Privacy Officer has to take time to do a proper assessment, which could conflict with the project deadlines)
 - Helps you to think of privacy throughout the project
 - Can help you figure out what you're doing along the way

Where do you go for help?

Ministries:

- MPOs

www.gov.bc.ca/privacyofficers

- PCT

Where do you go for help with your PIA?

Ministries:

- Ministry Privacy Officers (gov.bc.ca/privacyofficers)
- Privacy, Compliance and Training

- Don't struggle with the PIA on your own
- Start it and when you start slowing as things get harder, turn to your Privacy Officer

Other organizations:



OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for British Columbia

250-387-5629
info@oipc.bc.ca

Where do you go for help with your PIA?

Non-ministry Public Bodies:

- OIPC
Phone: 250 387-5629
Email: info@oipc.bc.ca
Website: <http://www.oipc.bc.ca/>

How to demonstrate value:

- Insert PIAs into other processes
- Grouping strategies
- Program vs technology

- Insert PIAs into other processes
 - E.g. contract process
 - Financial approval processes
 - Business planning exercises
- PIA grouping strategies
 - Business areas don't want to do a million PIAs and the Privacy Officer doesn't want to review them
 - Use grouping
 - Corporate PIAs vs one-offs each time a program area uses a particular technology
- Program not technology
 - When technologies are used in a similar way (for example, a program changes the software it uses because of cost – so the technology piece is used in the same way each time)
 - It's the program that's different and can be assessed rather than the technology the program uses

Speak with your MPO about ways to meet your PIA and program area needs.

PIAs should not be:

- Administratively burdensome
- A waste of time
- Get in the way of a program going forward

An Information Sharing Agreement is like an MOU.

During the privacy assessment of a project, program or activity, it may be determined that an Information Sharing Agreement is needed

-ISA for regular and systematic exchanges of info

- ISA is like an MOU – it is used to document the terms and conditions of the exchange of personal information
 - Be aware that people may call an ISA an MOU
- Used when there is a regular and systematic disclosure of PI between public bodies (not within a public body)

Components:

- Description of the PI being exchanged
- Description of the exchanged (flow)
- Efforts that will be made to ensure the PI is
 - Accurate, complete, up-to-date
 - Secure (stationary and in transit)
- Compliance monitoring and investigations with regard to the above

Benefits are:

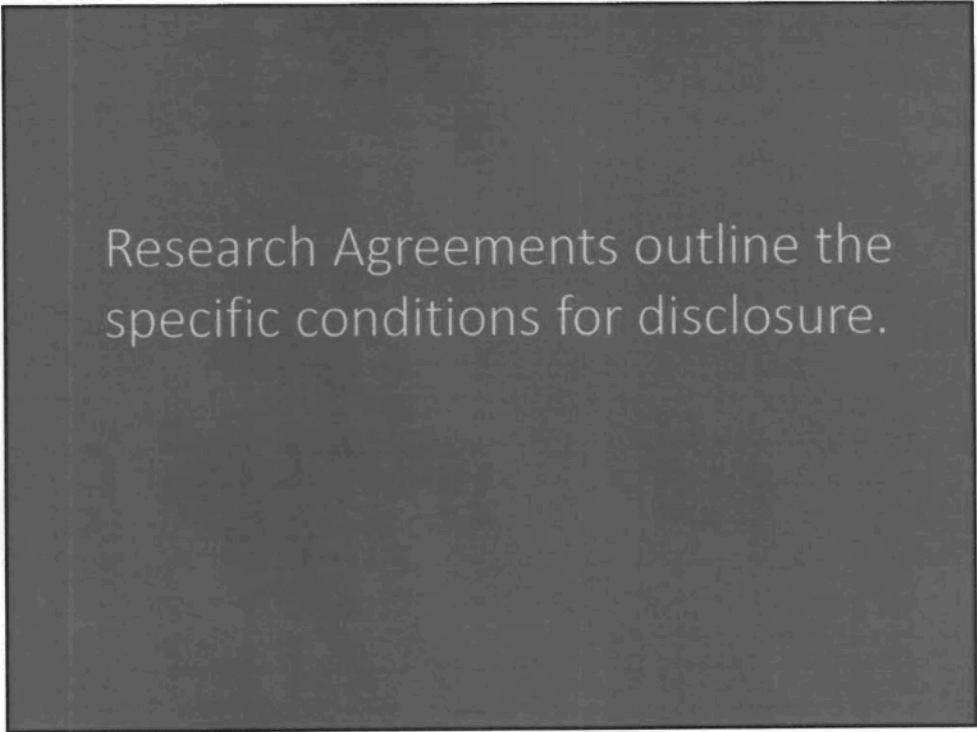
- A clear articulation of expectations, roles and responsibilities of the parties
- Accountability for the personal information in your care and being exchanged.

NOTE: ISA documents your authorities, but does not provide the authority

ISA Best Practices / Guidelines:

http://www.cio.gov.bc.ca/local/cio/priv_leg/documents/foippa/guidelines_isa.pdf

If you don't do ISAs, consider if you should and speak with your Privacy Officer



Research Agreements outline the specific conditions for disclosure.

Similarly, the assessment process may identify the need for a Research Agreement

- FOIPPA allows public sector organizations in B.C. to disclose personal information in their custody or under their control for research or statistical purposes
- Researchers can gain access to this information by entering into a legal research agreement that outlines the specific conditions for disclosure

Common or integrated program or activity examples:

- BC Services Card program
- Service BC

Or the program/activity may be identified as a Common or Integrated Program or Activity

- FOIPPA defines common or integrated program or activity as: "a program or activity that:
 - (a) provides one or more services through
 - (i) a public body and one or more other public bodies or agencies working collaboratively, or
 - (ii) one public body working on behalf of one or more other public bodies or agencies, and
 - (b) is confirmed by regulation as being a common or integrated program or activity."
- What is needed in a COIPA (in FOIPPA Reg s. 12):
 - (A) a description of the services provided by the program or activity;
 - (B) a description of the types of personal information collected, used and disclosed in the course of providing the program or activity;
 - (C) a description of the purposes, key objectives and expected benefits or outcomes of the program or activity;
 - (D) a description of the respective roles and responsibilities of each public body and agency through which, or on whose behalf, the services are provided;
 - (E) the date on which the program or activity will start and, if applicable, the date on which the program or activity will end, or
- Section 69(5.5) of FOIPPA requires ministries to notify the OIPC of a common or integrated program or activity in the early stages of developing the program or activity

Perceived barriers:

- Legal
- Complexity
- Timing

- Barriers to agreements are often perceived barriers:
 - Legal
 - FOIPPA and PIPA don't require that legal get involved in these types of agreements (ISAs, RAs, COIPAs)
 - Don't assume you must go to legal – unless your org's policy tells you to
 - Complexity of agreements
 - Agreements can be simple
 - Important to get the relevant parties in a room
 - Think of what you actually want to say (in human terms vs legal terms)
 - Lawyers may want to lawyer it up
 - Need a common understanding of parties involved rather than just the lawyer
 - Timing
 - Important to be clear on when agreements are needed
 - ISAs: when there is a regular and systematic disclosure of PI between public bodies (not within a public body)
 - RAs: when public bodies need to disclose personal information in their custody or under their control for research or statistical purposes
 - COIPAs: this one is a bit trickier – but good place to start is "Is one public body acting as a service provider for another public body?"
 - Then ask "Is there an authority in another act that allows this disclosure?"
- Templates on our site
 - May not be exactly what you need but a good start

Build privacy protection
into contracts.



A contract is an agreement that should be in place when using service providers

- Remember that agreements don't give authority for the collection, use or disclosure of personal information
 - Privacy leg gives authority

Image source: <https://commons.wikimedia.org/wiki/File:ContractLaw.jpg>

Privacy Protection Schedule

- Attach as a schedule to the contract
- Contractor is an employee
- Can't contract out of FOIPPA

Example: gov's Privacy Protection Schedule

- Contractor subject to the same FOIPPA requirements as the public body
 - So is an employee of the public body
- Can't contract out of FOIPPA obligations
- Completed and attached as a schedule to any contract between a public body and a contractor where personal information is involved
- Contract has to make sense for both parties
 - So both parties should be able to read and understand it

Schedule online:

<https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/privacy/agreements-contracts/privacy-protection-schedule>

Purpose of compliance policies:

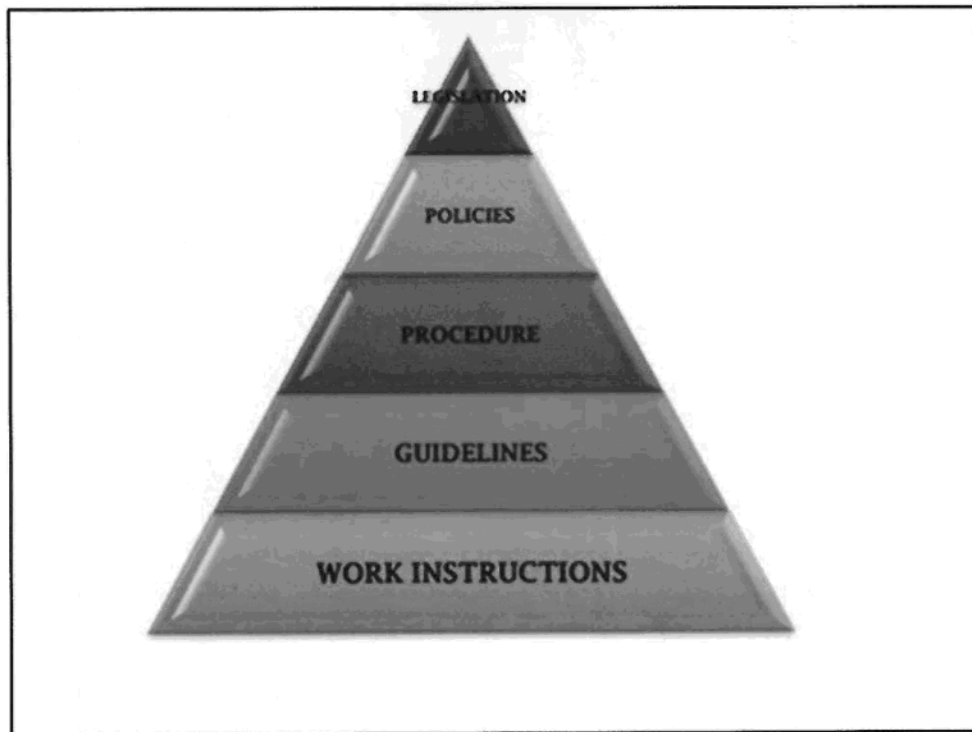
- Bakes privacy right in
- Maintains client trust
- Prevents breaches

Another element of a privacy management program is compliance policies

- e.g. for reasonable security (in FOIPPA, very vague – so compliance policies can provide that clarity for your org)

Purpose:

- Ensure privacy built into all projects, programs and services
- Helps maintain client trust
- Helps prevent breaches



DO WE NEED THIS????

This is the hierarchy of governance, or policy:

- Top is legislation – FOIPPA in this instance
- Then policies, procedures, guidelines and work instructions

From previous slide, compliance policies:

- Provide direction (e.g. don't put confidential materials in the blue boxes)
 - Good until you change custodial staff and they recycle your confidential docs
 - Give people the why so they can make an informed decision
- Things to direct people on what to do
 - E.g. form that builds out to process when pulling data for reports

As we get further down the pyramid, the rules or guidance become more and more granular to the roles of employees, and less and less rigid.

Everything in the triangle gets you to the same place in terms of business purpose

???Interactive activity:

- Take a moment to think of the work you do in each of these spaces – each one plays a different role than the others

Question to audience – areas of concern/risk?

Privacy issues to address:

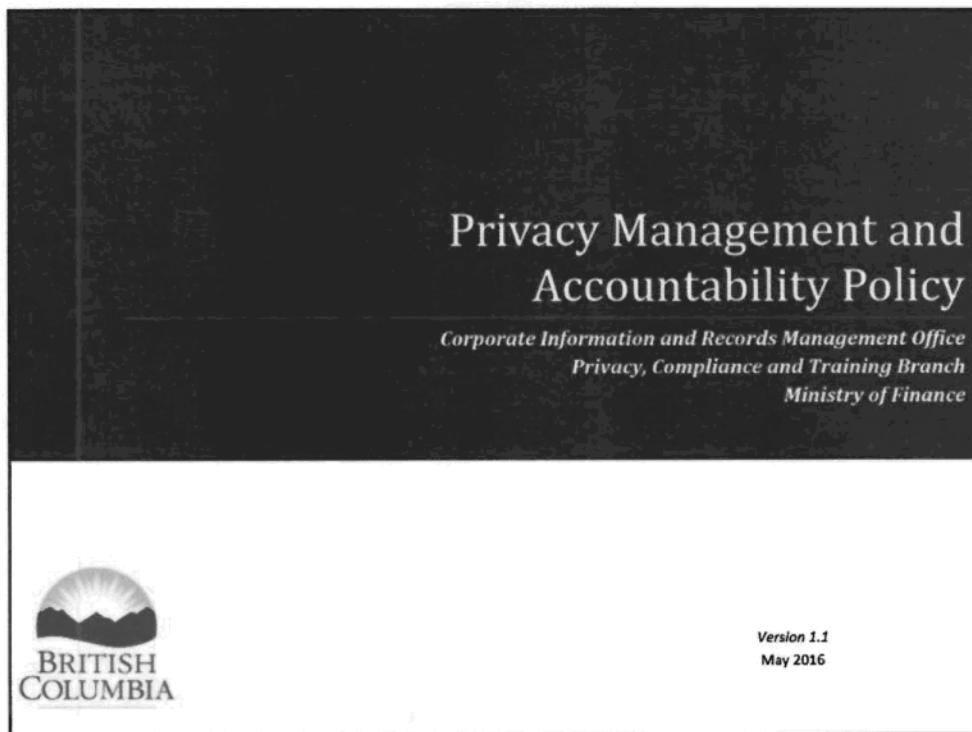
- Retention and disposal of PI
- Process for privacy complaints
- Appropriate use for technology
- Access to and correction of PI

Privacy issues to address through policies:

- Retention and disposal of personal info
- Process for handling complaints related to privacy
- Appropriate use policies for technology
- Access to and correction of personal information
 - Individual's right to request access to and correction of their own personal information

These are examples of places where you could develop policy

- Though these may not be issues or concerns for you or your organization – which means you may not need a policy
- Also think about the level of the issue and the product that is appropriate for it
 - E.g. disposal of PI: is this the kind of problem area that needs a policy?
 - Likely work instructions would suffice. Employees need guidance or instructions on things like not putting sensitive documents into blue bins or using secure shredders, etc.



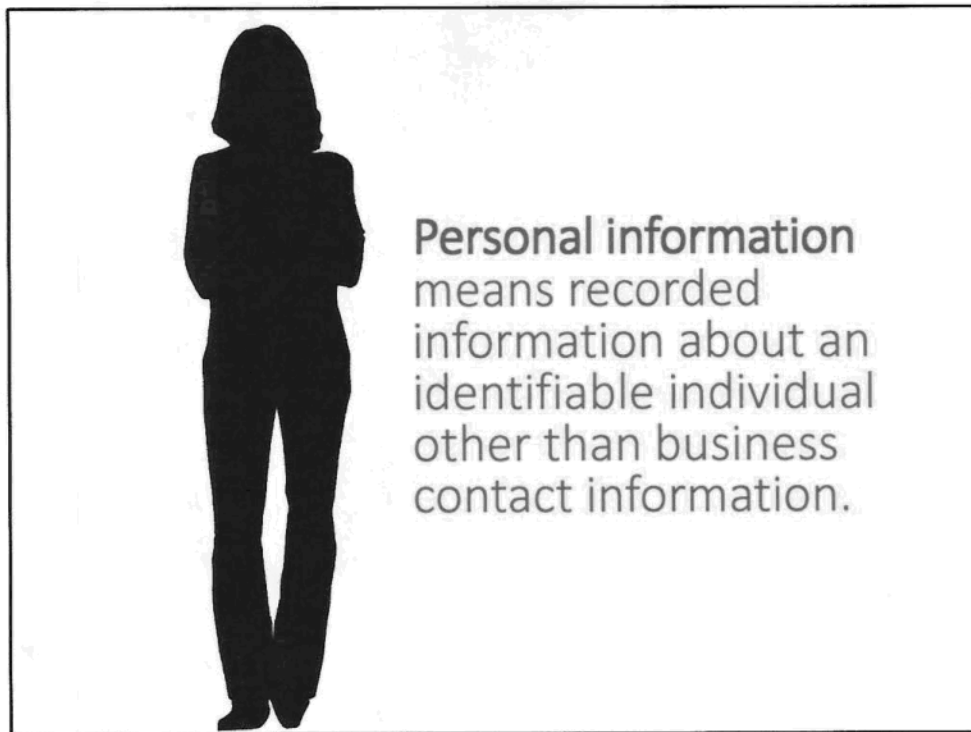
Example: Privacy Management and Accountability Policy (PMAP) for gov

- government's corporate approach to privacy management
- clarifies the privacy management roles and responsibilities of Government's ministries, the Corporate Information and Records Management Office (CIRMO) and Employees

I mention this policy as an example for one reason, and that is that it is a consolidation of government's privacy management program. Many of the requirements contained in here are not new – the requirements exist somewhere else, but it brings them all together into a single place.

Create a personal information inventory.

- If an org doesn't know what data they have:
 - How will the org protect it?
 - How will the org know they're in compliance with leg?
- Org should know type and amount of personal info it's collecting, using, disclosing and retaining
- Should also know the purposes behind the collection, use, disclosure and retention
- Should know location where personal information is held, including where service providers are holding personal information
- Inventory ensures accountability, which underlies FOIPPA



As a reminder, personal info is:

- Recorded information about an identifiable individual other than business contact information
- (Schedule 1 definition in FOIPPA)
- Used to be examples written into the definition
 - Was seen as an exhaustive list
- Intention is to have a broad definition that will be applicable in multiple situations

Examples

- Race, national/ethnic origin, skin colour
- Religious or political beliefs or associations
- Age, sex, sexual orientation, marital status
- Fingerprints, blood type, DNA information, biometrics
- Health records, educational, financial, criminal, employment history
- Your opinions

➤ If your opinion is about someone else, then that is the other person's personal info

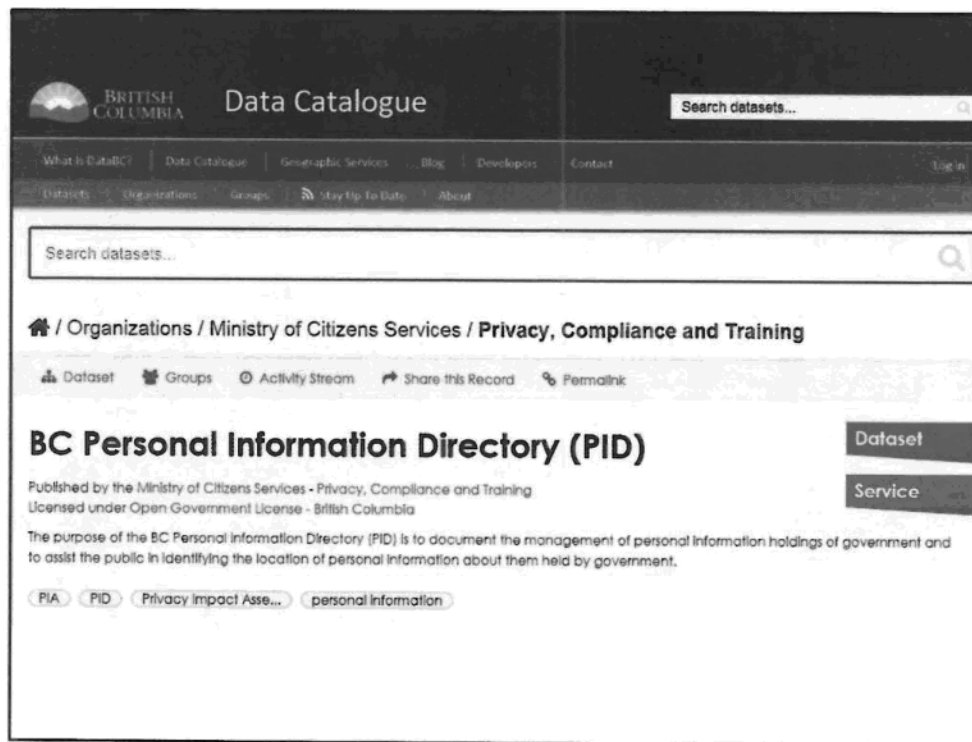
"contact information"

-information to enable an individual at a place of business to be contacted

-name, title, business telephone number, business address, business email or business fax number

- Contextual personal info – when is it business contact info and when is it personal?

Image source: clipart



Example: gov's Personal Information Directory

- Lists PIAs



Build practice reviews into your
privacy management program.

Part of privacy management program is ongoing review and revision

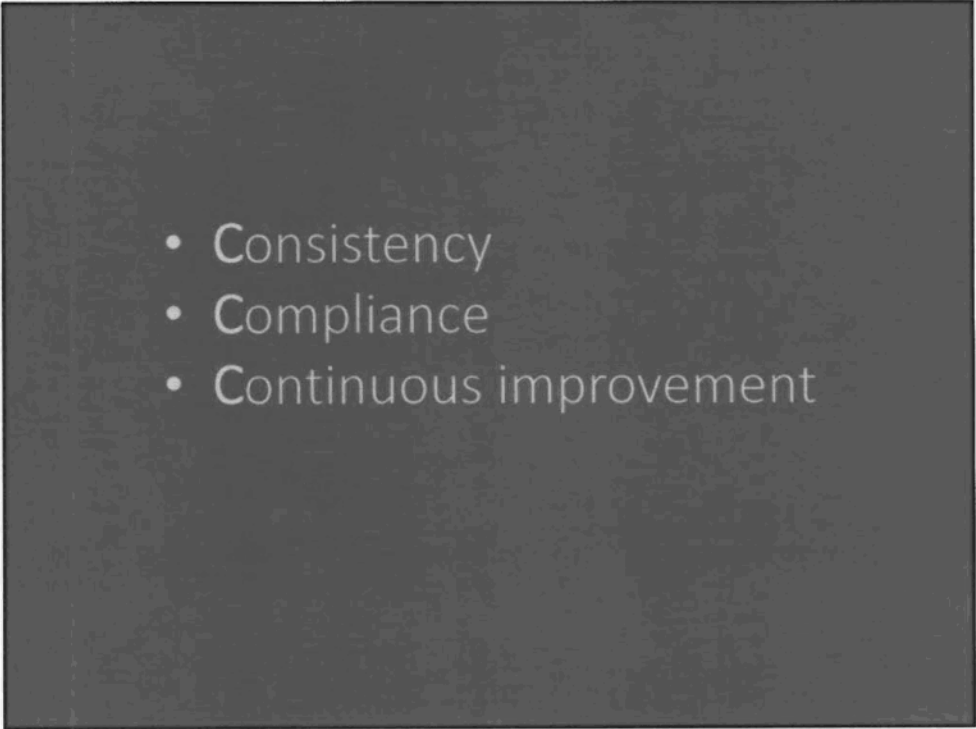
- Helps program remain effective

Review information management practices in four areas/domains:

- Privacy
- Records management
- Information access
- Information security

Gov's Practice Review Program as an example of steps to take

- Goal is to assess how well ministries are doing with their Information Management processes

- 
- Consistency
 - Compliance
 - Continuous improvement

- Consistency in the IM practices across government by reviewing those practices
- Compliance with relevant legislation and policies
- Continuous improvement (maturity) in information practices

REVIEW



Scheduled

- Baseline/Routine
- Self review

Ad hoc

- Issues based

- Scheduled practice reviews:
 - Could do a fulsome review to get a baseline
 - Then move to routine schedule
 - Privacy Officer can do baseline and push self reviews to business areas
 - For baseline reviews, think of how you will measure your baseline
 - Self reviews
 - Point here is to be completely honest (self review isn't worth much if the org hides problems from itself)
- Ad-hoc reviews
 - Issues Based
 - When issues come up, such as a privacy breach, a review can be conducted once the incident is contained

Engagement

Ask audience to think of benefits and drawbacks of each

Issue source: <http://creative-commons-images.com/handwriting/a/assessment.html>

Governance gone wrong.



When privacy governance goes wrong, breaches happen

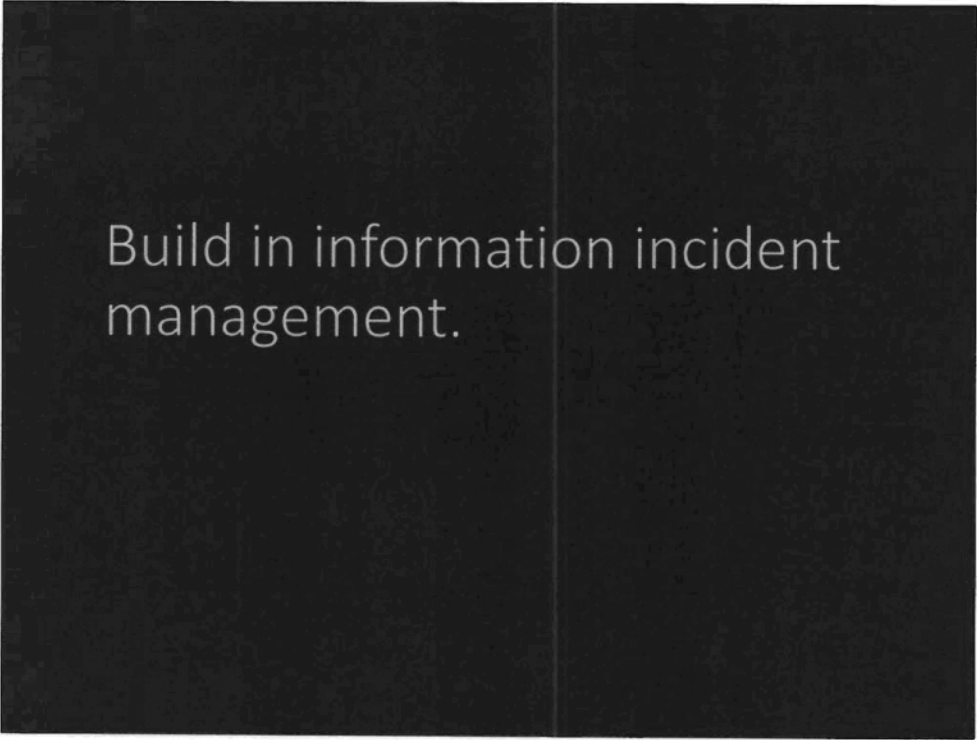
Facebook????

Examples:

- Equifax
 - 19,000+ Canadians affected
 - Source: <https://toronto.ctvnews.ca/total-number-of-canadians-impacted-by-equifax-data-breach-passes-19-000-1.3698900>
- Uber
 - Data from 57 million users was compromised a year ago, but Uber didn't disclose
 - Uber hackers paid a "bug bounty" of \$100,000 (bug bounties reward people for reporting software vulnerabilities – this one was large)

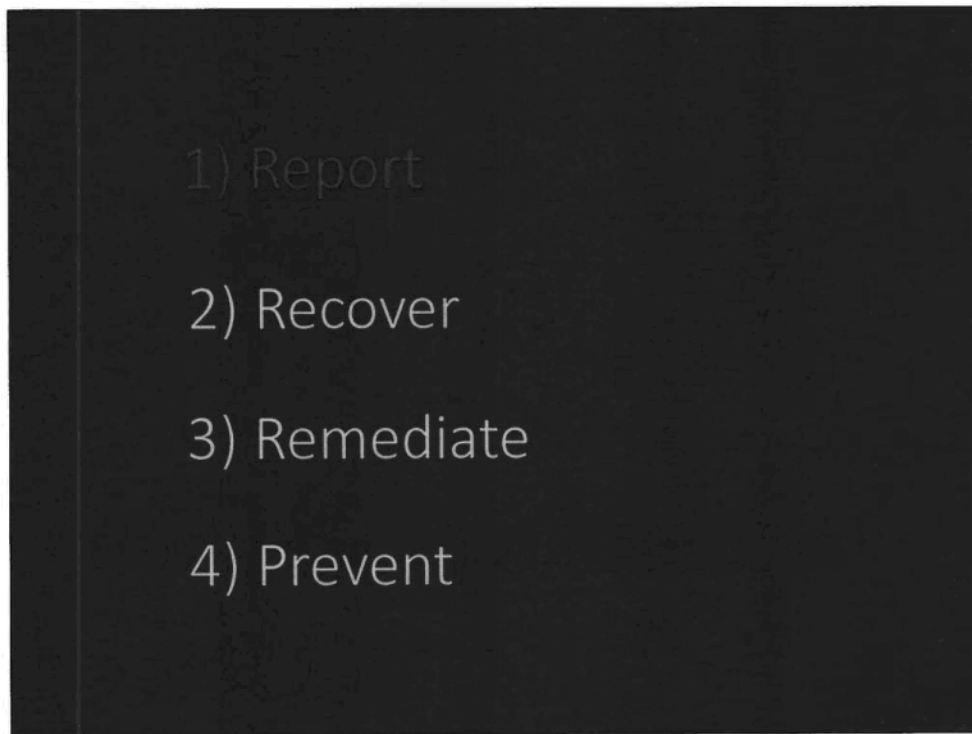
Ask audience to name other large breaches of the year

- We now focus on response time rather than thinking we can 100% prevent breaches
- Recognize that people feel terrible when they do something wrong
 - Story: janitor responsible for shredding records took them to beach for a bonfire; wind picked up and blew the records down the beach
 - Think of that person having to report to the Privacy Officer



Build in information incident
management.

This is why a privacy management program needs to have an info incident management process built in



When it comes to information incident management, gov has the following process:

Report: most important

- Report both confirmed and suspected incidents
- Reporter works with their internal privacy office
- Useful to make notes on details of the incident – investigators may ask for these during the investigation
 - Who, what, where, when, how
 - What could be the cause of the incident?
 - What and whose personal info is involved?
 - Is there any unauthorized use or disclosure and to whom?
 - What was the order of events?
- Don't delay!

Recover:

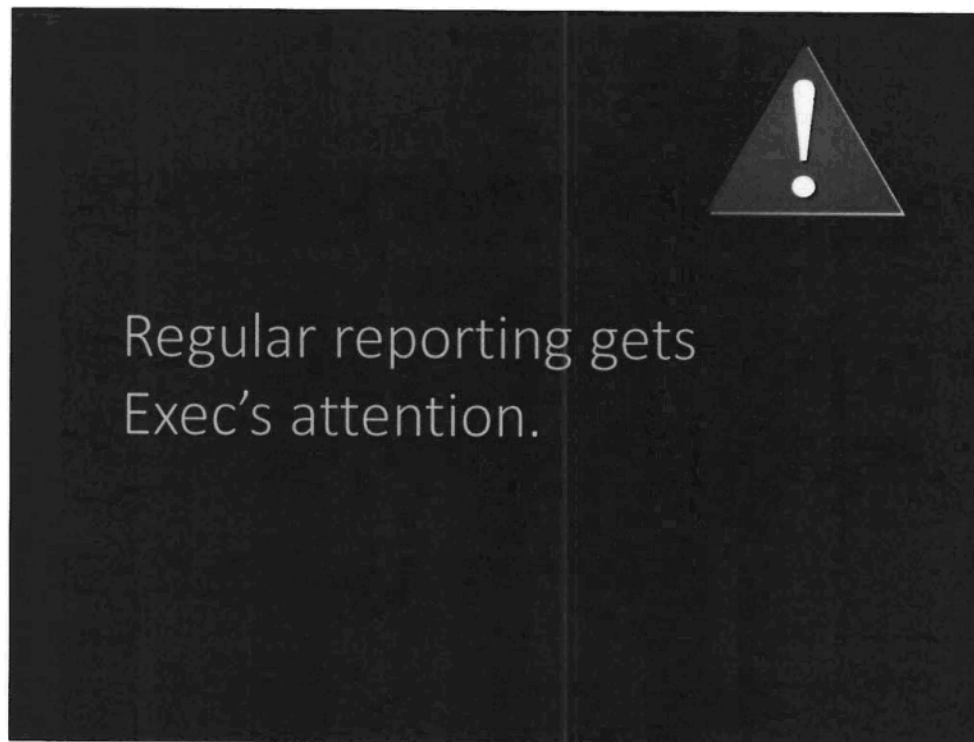
- Investigator walks reporter through steps to recover confidential or personal information if possible
 - e.g. if an email is sent to the wrong person, can that person be contacted to double delete the email and confirm they've done so?

Remediate:

- Investigator walks reporter through steps to remediate and resolve the incident:
 - e.g. may need to notify individuals or parties affected by the incident

Prevent:

- No wasted mistakes – learn from the incident
- Investigator lays out steps to prevent similar incidents from happening



Important for orgs to regularly report to Exec

Itemized list of breaches to ADMs

- Gets exec buy in – when their attention is not required
- Never underestimate the power of regular reporting
- Normalize that mistakes happen
- Plus shows that Privacy Officer is on top of it
 - Useful and effective process in place

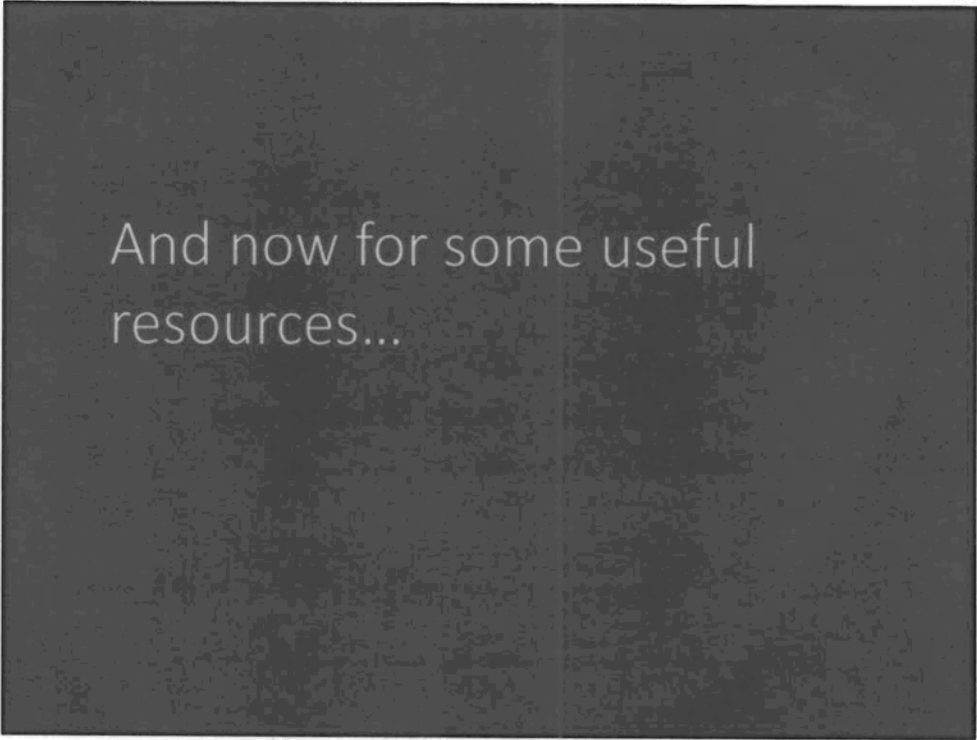
Image source: https://commons.wikimedia.org/wiki/File:Icon_attention.svg

How do you measure prevention?

- Program measurements are important to determine the success of a privacy management program
 - But how do you measure prevention?
- How do you prove you've done something when you're in the prevention space

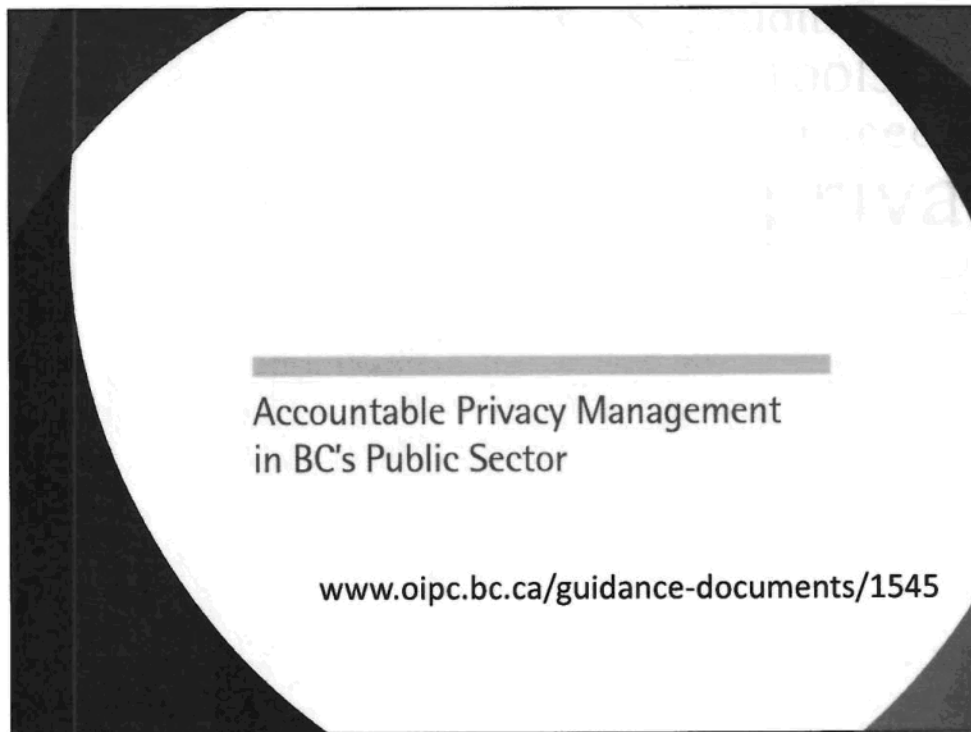
Options:

- PIA stats – how long it takes for Privacy Officer to review; how long for Exec to sign off
- Training uptake
- Reductions in types of breaches
- Sign off times for PIAs



And now for some useful
resources...

We have some useful resources for you



- OIPC released framework for privacy management program for public sectors
- Can be used for private sector as well

<https://www.oipc.bc.ca/guidance-documents/1545>

Privacy, Compliance and Training

www.gov.bc.ca/protectprivacy

Privacy Management and Accountability Policy

www.gov.bc.ca/privacypolicy

Useful links:

- protect privacy link has info on training, PIAs, the breach process, contracts, etc.
- privacy policy link provides gov's Privacy Management and Accountability Policy in full

BC Privacy and Access
Helpline

250-356-1851
(Service BC 1-800-663-7867)

privacy.helpline@gov.bc.ca