

Severing Guidelines - Calendar Entries

ENTRY OR DESCRIPTION OF ENTRY	SEVERED OR NOT SEVERED
Blackberry/cellphone numbers for government employees	Severed under section 17 – Blackberry/cellphone numbers that constitute “business contact numbers” (i.e. they are part of a signature block) will be disclosed but “confidential, unlisted” Blackberry/cellphone numbers will be withheld under section 17. The financial harm to the public body is the high cost of constantly changing these phone numbers after every FOI request.
“Cabinet” or “Cabinet Retreat”	Not Severed – there is not enough information in this entry to reveal the substance of deliberations of the Executive Council or its committees.
“Chambers” as a subject	Not Severed
“Chambers” as a location	Severed under Section 15
Constituency related / Entries in a <u>Minister’s</u> calendar that relate to his/her duties as a Member of the Legislative Assembly	If the request is worded for the calendar of “the Minister” it is appropriate to consider these entries Not Responsive to “the Minister’s” calendar.
Confirmation numbers, Reservation numbers, frequent flyer numbers, etc	Severed under sections 17, 22– Most external to government organizations will readily provide additional information regarding a reservation/booking/account provided that you are able to provide these numbers. There is a financial harm to the public body if its credit information is divulged and there is an unreasonable invasion of privacy given that there is a personal credit verification required in order to obtain a corporate travel card.
Accommodation details	Severed under section 15
Meeting location details	Severed under section 15
Working from “Home”	Severed under section 15 “Home” (only)
“WFH” (acronym for working from home)	Severed under section 15 in its entirety
“Caucus” “House” “House Business Update” “Duty House Leader” “House Duty”	Severed as Not Responsive in a Minister’s calendar only; Not severed in any other calendar
Meetings with Officers of the Legislature (see schedule 1 definition), that relate to their duties/functions under an Act	Severed under section 3 (in any calendar)
Unpublished direct telephone numbers for Minister, DM, ADM, etc.	Severed under section 17 - see comments for severing Blackberry/cellphone numbers
“Private Appointment” (as a stand-alone term)	Not severed
<i>Details</i> of a personal appointment	Severed under section 22, as appropriate
“Issue Prep with Staff”	Not Severed
“QP, “QP Prep”, “QP Briefing”	Not Severed

Severing Guidelines - Calendar Entries

ENTRY OR DESCRIPTION OF ENTRY	SEVERED OR NOT SEVERED
Teleconference information: <ul style="list-style-type: none"> - Dial- in Number - Conference Reference - Participant Conference Access Code - PIN or moderator's code 	Severed under sections 15, 17 Severed under sections 15, 17 Severed under sections 15, 17 Severed under sections 15, 17
Telephone numbers (including cell numbers)/ email addresses for people representing an organization (union, association, etc) * Personal cell numbers for people representing an organization, where they are clearly identified as such	Not Severed –business contact information is not personal information; Severed under section 22
"Throne Speech"	Not Severed –the Throne Speech is considered an event that a Minister attends in both capacities (MLA and Minister).
"Treasury Board"	Not Severed – there is not enough information in this entry to reveal the substance of deliberations of the Executive Council or its committees.
"John Smith – vacation, Jane Doe Acting"	Severed under section 22 - "vacation" Not Severed - "Jane Doe Acting."
EDO days of staffers (i.e. "John Smith – EDO")	Severed under section 22 in its entirety
File paths printed on bottom of attachments	Not Severed - If a harms assessment determines that the security of a system would be harmed by releasing information included in a file path, the information will be withheld under section 15. This would not generally be the case, as a file path alone doesn't reveal certain specifics that would be required to identify the server which a mapped drive resides on.
360's (performance review), mentoring, EPDP	Severed under section 22
Staff/Christmas parties during business hours	Not Severed – the assumption here is that these parties are paid for using public funds and attended by staff within their paid hours of work.
Staff/Christmas parties outside of business hours	Severed under section 22 – the assumption here is that these parties are paid for using personal funds and attended by staff outside of their paid hours of work.

Severing Guidelines - Calendar Entries

Request Dependent Section

In some circumstances, the approach for severing calendar entries will be dependent on the wording of the applicant's request. If a Minister's calendar is requested and there are entries that relate to that individual's duties/functions as a Member of the Legislative Assembly, they would not be responsive to the request. If an applicant agrees to exclude phone numbers and email addresses from their request for a calendar, they would not be responsive to the request. The above are only intended to be examples of circumstances where it would be appropriate to use "not responsive" to remove information in response to an FOI request for calendars (i.e. they do not constitute an exhaustive list).

Severing Guidelines - Calendar Entries

ENTRY OR DESCRIPTION OF ENTRY	SEVERED OR NOT SEVERED
Blackberry/cellphone numbers for government employees	Severed under section 17 – Blackberry/cellphone numbers that constitute “business contact numbers” (i.e. they are part of a signature block) will be disclosed but “confidential, unlisted” Blackberry/cellphone numbers will be withheld under section 17. The financial harm to the public body is the high cost of constantly changing these phone numbers after every FOI request.
“Cabinet” or “Cabinet Retreat”	Not Severed – there is not enough information in this entry to reveal the substance of deliberations of the Executive Council or its committees.
“Chambers” as a subject	Not Severed
“Chambers” as a location	Severed under Section 15
Constituency related / Entries in a <u>Minister’s</u> calendar that relate to his/her duties as a Member of the Legislative Assembly	If the request is worded for the calendar of “the Minister” it is appropriate to consider these entries Not Responsive to “the Minister’s” calendar.
Confirmation numbers, Reservation numbers, frequent flyer numbers, etc	Severed under sections 17, 22– Most external to government organizations will readily provide additional information regarding a reservation/booking/account provided that you are able to provide these numbers. There is a financial harm to the public body if its credit information is divulged and there is an unreasonable invasion of privacy given that there is a personal credit verification required in order to obtain a corporate travel card.
Accommodation details	Severed under section 15
Meeting location details	Severed under section 15
Working from “Home”	Severed under section 15 “Home” (only)
“WFH” (acronym for working from home)	Severed under section 15 in its entirety
“Caucus” “House” “House Business Update” “Duty House Leader” “House Duty”	Severed as Not Responsive in a Minister’s calendar only; Not severed in any other calendar
Entries that relate to the exercise of the duties/functions of an Officer of the Legislature (see Schedule 1 definition) under an Act	Severed under section 3 (in any calendar)
Unpublished direct telephone numbers for Minister, DM, ADM, etc.	Severed under section 17 - see comments for severing Blackberry/cellphone numbers
“Private Appointment” (as a stand-alone term)	Not severed
<i>Details</i> of a personal appointment	Severed under section 22, as appropriate
“Issue Prep with Staff”	Not Severed
“QP, “QP Prep”, “QP Briefing”	Not Severed

Severing Guidelines - Calendar Entries

ENTRY OR DESCRIPTION OF ENTRY	SEVERED OR NOT SEVERED
Teleconference information: <ul style="list-style-type: none"> - Dial- in Number - Conference Reference - Participant Conference Access Code - PIN or moderator's code 	Severed under sections 15, 17 Severed under sections 15, 17 Severed under sections 15, 17 Severed under sections 15, 17
Telephone numbers (including cell numbers)/ email addresses for people representing an organization (union, association, etc) * Personal cell numbers for people representing an organization, where they are clearly identified as such	Not Severed –business contact information is not personal information; Severed under section 22
"Throne Speech"	Not Severed –the Throne Speech is considered an event that a Minister attends in both capacities (MLA and Minister).
"Treasury Board"	Not Severed – there is not enough information in this entry to reveal the substance of deliberations of the Executive Council or its committees.
"John Smith – vacation, Jane Doe Acting"	Severed under section 22 - "vacation" Not Severed - "Jane Doe Acting."
EDO days of staffers (i.e. "John Smith – EDO")	Severed under section 22 in its entirety
File paths printed on bottom of attachments	Not Severed - If a harms assessment determines that the security of a system would be harmed by releasing information included in a file path, the information will be withheld under section 15. This would not generally be the case, as a file path alone doesn't reveal certain specifics that would be required to identify the server which a mapped drive resides on.
360's (performance review), mentoring, EPDP	Severed under section 22
Staff/Christmas parties during business hours	Not Severed – the assumption here is that these parties are paid for using public funds and attended by staff within their paid hours of work.
Staff/Christmas parties outside of business hours	Severed under section 22 – the assumption here is that these parties are paid for using personal funds and attended by staff outside of their paid hours of work.

Severing Guidelines - Calendar Entries

Request Dependent Section

In some circumstances, the approach for severing calendar entries will be dependent on the wording of the applicant's request. If a Minister's calendar is requested and there are entries that relate to that individual's duties/functions as a Member of the Legislative Assembly, they would not be responsive to the request. If an applicant agrees to exclude phone numbers and email addresses from their request for a calendar, they would not be responsive to the request. The above are only intended to be examples of circumstances where it would be appropriate to use "not responsive" to remove information in response to an FOI request for calendars (i.e. they do not constitute an exhaustive list).

FREEDOM OF INFORMATION BEST PRACTICES FOR MINISTRIES

FOI Roles and Responsibilities and General Best Practices

Ministries and IAO – a Partnership

The processing of Freedom of Information (FOI) requests is a partnership between BC Government ministries whose records are requested and Government's FOI service provider - Information Access Operations (IAO). The respective roles and responsibilities are assigned to the parties that are best-positioned to undertake them; i.e.:

- Ministries have custody and control of their records, and are the “knowledgeable owners” of those records. They are best-positioned to determine whether their records are responsive to applicants’ requests, and whether release of information in those records will result in harms.
- IAO holds the expert knowledge of the *Freedom of Information and Protection of Privacy Act* (FOIPPA) and how it can be applied in various situations, and provides advice and guidance to client ministries regarding the application of FOIPPA.

This document describes recommended best practices for ministries to employ in carrying out their FOI-related responsibilities. The attached Appendix provides a high level summary of the respective roles and responsibilities of both IAO and ministries in working together to process FOI requests.

Ministry FOI Coordinator/Central Point of Contact

A dedicated, in-house FOI Coordinator is recommended for ministries, to enable them to meet their statutory obligations to respond on time to ever-increasing FOI request volumes. The FOI Coordinator ensures that all ministry responsibilities regarding the processing of FOI requests are assigned, understood and completed; provides clear advice and direction to ministry program areas; and serves as the ministry's central point of contact with IAO. FOI Coordinator responsibilities and best practices are described further in subsequent sections of this document.

Electronic Sharing and Transmission of Records Saves Time and May Reduce Errors

FOIPPA legislates very tight timelines and strict deadlines for responding to FOI requests. The statutory obligations that must be met during these time frames are considerable, leaving little time for records to be in transit. Electronic sharing and transmission of records is recommended to minimize “downtime” while records are in transit, and to facilitate concurrent reviewing of records by ministry officials. Electronic transmission also facilitates the tracking of records’ whereabouts and control over document versions, which reduces the risk of releasing incorrect records.

FOI is a Government Priority

Giving FOI a high profile in ministries is a recommended best practice. The importance of FOI can be profiled in executive communications to ministry staff. Some ministries include FOI as a standing agenda item at executive meetings.

Record Gathering Best Practices

FOI Coordinator's Role

When IAO receives FOI requests for records of its client ministries, IAO prepares and sends a Call for Records to the appropriate ministry's FOI Coordinator with a requested response date. It is recommended that each ministry maintains a central FOI e-mailbox for this purpose. The ministry FOI Coordinator reviews the Call for Records and then forwards the Call to the ministry program area(s) that are likely to have records that are responsive to the applicant's request. The FOI Coordinator receives and organizes all responses from the program areas; reviews them for accuracy and completeness, and follows up with program areas when information provided is incomplete or unclear; removes duplicate records; and then sends the complete ministry package back to IAO. Should the program areas have differing opinions on what needs to be provided, the FOI Coordinator discusses the issue with the relevant parties and then provides IAO with clear ministry direction.

Managing Timelines

FOIPPA establishes a 30 business day time frame for responding to most FOI requests (with limited provisions to extend deadlines or put requests on hold temporarily). FOI is a complex process, and there is potential for delays at all stages. It is recommended that all steps in the FOI process be completed with appropriate due diligence as expeditiously as possible. Time saved in the Record Gathering stage may be needed in later stages of the process to keep the FOI request from going overdue. Overdue requests can cause considerable additional work for ministries, and those should be avoided to the extent possible.

Duty to Assist and Adequate Search

FOIPPA establishes a duty to assist FOI applicants. This duty involves making every reasonable effort to assist applicants and responding without delay to each applicant openly, accurately and completely. The duty to assist is shared by IAO and its client ministries, and is facilitated by good communication between the parties.

Most duty to assist complaints from FOI applicants pertain to adequacy of search. Adequate search involves making reasonable interpretations of applicants' FOI requests, requesting clarification when applicants' requests are unclear, and then performing a reasonable search for the requested records.

In limited circumstances, the duty to assist requires ministries to create a record.

Fee Estimating

FOIPPA permits the charging of limited fees for certain activities pertaining to the processing of FOI requests for general records (not personal records). As most applicants prefer to receive their records electronically, FOI fees are charged primarily for time spent locating, retrieving and producing responsive records; and for preparing records for disclosure; at a rate of \$30 per hour. (Per FOIPPA, the

first three hours spent locating and retrieving records, and any time spent reviewing responsive records for harms or severing are provided free of charge.)

When total fees on an FOI request are estimated at \$50 or more, FOI Coordinators are encouraged to send their ministry's fee estimate information to IAO as quickly as possible, to enable IAO to send the fee estimate to the applicant, which stops the FOI clock until the applicant responds. Record gathering on files with fees should begin when the required deposit or fee is paid, or when the fee is waived.

FOI applicants have the right to challenge fee estimates and to complain to the Office of the Information and Privacy Commissioner about same; therefore, fee estimates should reflect reasonable estimates of chargeable work that will be required to process individual FOI requests.

Responsive Records Only

While FOIPPA requires ministries to conduct a thorough search for records requested through FOI, it is important to provide ONLY records that respond to the applicant's request. Providing additional records that are not responsive to the applicant's request causes delays in the processing of that request, increasing the likelihood that the ministry will not meet its statutory deadline to respond.

Complete Call for Records Form

Recipients of Calls for Records are requested to complete all ministry sections of the Call for Records form and to send that completed form with the responsive records to the FOI Coordinator, for review and forwarding to IAO. The ministry sections of the Call for Records form are:

- Section 1: Initial Records Assessment - Complete this section for all FOI requests.
- Section 2: Fee Estimate – Complete this section for all general FOI requests where the total estimated fees for the MINISTRY are \$50 or more (check with FOI Coordinator if unsure).
- Section 3: Search Summary and Program Area Recommendations – Complete the search summary field for all FOI requests, including “no records responses” to demonstrate that the ministry exercised due diligence in determining its response. Complete the “harm” sections (the appropriate check box and the description field) if responsive records are located (see the Harms Assessments paragraphs below).
- Section 4: Contact Information – Complete this section for all FOI requests.

Harms Assessments

Completion of the above-referenced “harm” sections of the Call for Records form is critical. When doing this, ministries are not being asked to sever records or to identify applicable sections of FOIPPA. As the “knowledgeable owners” of their records, ministries are being asked to identify information in the records that could reasonably be expected to cause harm if released, and to identify the type(s) of anticipated harm. Most of the FOIPPA exceptions to disclosure are harms-based. IAO reviews the ministry-supplied responsive records and accompanying harms assessments, and provides ministries with informed recommendations on how FOIPPA may be applied correctly to sever information that meets the stipulated harms tests.

An example of a harms assessment statement is “If the cost estimate figures in Schedule 1 of Document A are released, this will reveal and harm the ministry’s negotiating position for the upcoming round of contracts”. Depending on the content and context of the referenced record, IAO likely would respond to this harms assessment by recommending that the referenced cost estimate figures be severed from the record under FOIPPA section 17 (disclosure harmful to the financial or economic interests of a public body).

Cabinet Confidences

FOIPPA section 12 requires severing of information that would reveal the substance of deliberations of Cabinet or its committees from records that are released through FOI. Where responsive records have been prepared for, or used to inform, a decision of Cabinet or any of its committees, ministries need to identify the applicable records and to answer the following two questions:

1. What is the status of the issue that went to Cabinet or one of its committees?
2. Has the decision been made public or implemented?

The Call for Records form asks ministries to include this information in the Harms Assessments that they provide with their responsive records to IAO. This information enables IAO to recommend appropriate section 12 severing to ministries.

Sign-off Best Practices

FOI Coordinator’s Role

Once IAO has completed its review of the ministry-provided responsive records and harms assessments (and any necessary external consultations or notifications), IAO prepares and sends an FOI sign-off package (through the ministry’s central FOI e-mailbox if it has one) to the ministry FOI Coordinator. The FOI Coordinator manages the ministry’s internal FOI sign-off process, by routing the sign-off package through the appropriate ministry officials to the “delegated head” with authority to sign-off on that particular FOI response (see Delegate Sign-off Authority paragraph below). The FOI Coordinator investigates sign-off delays, and advises IAO if changes to the sign-off package are required by the “delegated head”. When sign-off is obtained, the FOI Coordinator e-mails the completed sign-off package/approval back to IAO.

Managing Timelines

Six business days are notionally allocated for ministry FOI sign-offs, but this time period might be reduced when the statutory response date is approaching or increased for large and complex files if sufficient additional time is available. IAO needs time to do a final check of all FOI response packages after sign-offs are received from ministries and before records are released to applicants. These final checks are necessary to minimize the likelihood of privacy breaches or other information incidents. If FOI sign-offs are not sent to IAO until the statutory response dates, there may not be time for IAO to do the necessary final checks that same day, in which case, responses to applicants will go out late.

Delegate Sign-off Authority to Lowest Level Based on Risk

FOIPPA section 66 permits the head of a public body to delegate his or her FOIPPA-related responsibilities and authorities to other persons or positions. It is recommended that Deputy Ministers delegate their FOIPPA-related responsibilities and authorities to the lowest level organizational positions with which they are comfortable, based on risk. Delegating to the most appropriate level expedites FOI processing by providing ministries with the flexibility to allow incumbents of specified lower level positions to exercise authorities and sign-off on responses to low risk FOI requests; but it does not preclude the incumbents of positions at higher levels in the same lines of authority, including Deputy Ministers, from exercising their authorities or signing off on select FOI responses.

Limit Internal Signatures Required before Sign-off

It is recommended that ministry “delegated heads” limit the number of internal signatures that they require before signing off on FOI responses, as requiring multiple internal signatures prior to sign-offs increases the likelihood that responses to FOI applicants will be late. FOIPPA’s very tight timelines do not facilitate multiple internal approvals prior to formal ministry sign-offs.

Complaints and Reviews Best Practices

Time is of the Essence

FOI applicants have the right to file a complaint or request a review by the Office of the Information and Privacy Commissioner (OIPC) when they are dissatisfied with the processing of an FOI request. For example, applicants may question or challenge: the adequacy of search for requested records; FOI fees estimated or collected; the severing applied to records that are released; or the failure to respond to an FOI request by the statutory deadline (an “alleged deemed refusal”). When applicant complaints or requests for review are received, ministries and IAO need to work with the OIPC to resolve the issue(s) raised as expeditiously as possible. Issues that cannot be resolved to an applicant’s satisfaction may be referred to inquiry, which is a time-consuming process involving legal counsel that can be very costly to ministries.

Resolve through Mediation where Possible

When the OIPC opens a review or complaint file, it may request through IAO copies of correspondence with the applicant, or it may send a list of questions about the processing of the FOI file at various stages. Depending on its initial findings, the OIPC may request that the ministry reconsider its earlier decisions to sever or withhold records. Working in partnership with IAO to respond to those OIPC questions and requests as quickly as possible can lead to an early resolution of the issue(s) and prevent the file from going to inquiry.

Comply with OIPC Orders

When FOI applicant complaints and requests for review go to inquiry, the usual result is an OIPC order. Frequently these orders are to release records. OIPC orders have the force of law and must be carried

out within the time frames stipulated in those orders (unless a judicial review is requested before the deadline). Please work with IAO to comply with all OIPC orders.

Appendix: ROLES AND RESPONSIBILITIES FOR PROCESSING FOI REQUESTS

PREAMBLE: The processing of FOI requests is a partnership between IAO and its client ministries. The respective roles and responsibilities for this process are assigned to the parties that are best-positioned to undertake them; i.e.:

- IAO is the client ministries' service provider to FOI applicants. IAO holds the expert knowledge of FOIPPA and how it can be applied in various situations, and provides advice and recommendations to client ministries regarding same. IAO also provides FOI activity data to client ministries, and coordinates client responses to reviews and complaints from applicants.
- Client ministries have custody and control of their records, and are the "knowledgeable owners" of those records. They are best-positioned to determine whether their records are responsive to applicants' requests, and whether release of information in those records will result in harms. Client ministries approve the application of FOI exceptions to disclosure based on recommendations from IAO, and they approve the release of records to applicants.

It is assumed that both parties will make the best use of available technology to streamline the process.

1. INTAKE – IAO

- Determine whether request complies with FOIPPA and is addressed to an IAO client
- If requirements above are met, log request in and open file
- Assign request to appropriate IAO Team
- Send formal acknowledgement of request to applicant
- IAO Team to issue Call for Records to client ministry FOI Coordinator

2. RECORD GATHERING – Client Ministry

- Determine if request is sufficiently voluminous to warrant a fee and, if so, complete Fee Estimate information on the Call for Records form and email it to IAO ASAP
- If request proceeds, locate all responsive records, and send them electronically to IAO, along with the completed Call for Records form, which includes a harms assessment
- Where information revealing Cabinet confidences is identified, provide required information to support FOIPPA section 12 severing with the records and harms assessment

3. REVIEW & ANALYSIS – IAO

- Issue fee estimate to applicant where applicable
- Analyze and provide recommendations to client on any fee waiver requests
- Initiate and process any necessary consultations or third party notifications
- Review responsive records and harms assessments provided by client, and consultation responses where applicable
- Apply for OIPC extensions where warranted
- Determine appropriate severing recommendations and prepare sign-off package for client ministry
- email sign-off package to client ministry FOI Coordinator

4. SIGN-OFF – Client Ministry

- Manage client's internal review and sign-off process
- Route sign-off package through appropriate parties determined by client ministry; obtain approval signature from ministry's delegated FOI approval authority
- email completed sign-off package back to IAO

5. RELEASE – IAO

- Finalize release package
- Issue response to applicant
- Close file



Shared
ServicesBC

Logistics and Business Services

FREEDOM OF INFORMATION

Presented June 2014

FREEDOM OF INFORMATION

1. What you need to know about the FOI Act
2. Records Management
3. FOI
4. How the FOI process works
5. Trends in FOI
6. Calendars
7. Open Information
8. FOI Contacts

PURPOSES OF THE ACT

Accountability to the Public

- Legislated right to access all government records - specifying limited exceptions (i.e. make what is commonly referred to as an 'FOI request')

Protection of Privacy

- Provides a right of access to individuals own personal information
- Regulates how public bodies collect, use and disclose personal information
- Right to request correction of personal information

Independent Oversight by the Office of the Information & Privacy Commissioner

- Conducts reviews on decisions regarding disclosure

Purposes of the Act

ACCOUNTABILITY

RIGHT OF ACCESS TO
RECORDS



PRIVACY

PREVENT UNAUTHORIZED
COLLECTION, USE OR
DISCLOSURE OF PERSONAL
INFORMATION

INDEPENDENT OVERSIGHT

WHO IS COVERED BY THE ACT

All provincial ministries, and most provincial agencies, boards, commissions, Crown corporations and smaller agencies

Local public bodies

- School Districts
- Colleges and universities
- Regional health boards

Self-governing professions and occupations

- Teachers
- Doctors
- Nurses

➤ Government is only responsible for requests to BC government ministries

WHAT RECORDS ARE COVERED BY THE ACT

All records in the **custody** or under the **control** of a public body

What is a Record?

- Any information recorded or stored by any means whether in hard copy or in electronic format
- Regardless of content and subject matter, the following are subject to an FOI request:
 - briefing notes
 - vouchers
 - telephone records
 - notebooks/daybooks
 - contractor records
 - email
 - records on your smart phone
 - transitory records

TRANSITORY RECORDS

- Are records of temporary usefulness not required to document decisions and actions or to support ongoing government business
- Should be regularly deleted as their usefulness ends (e.g.: transitory emails of no further use can be deleted)
- The Transitory Records Schedule does not apply to personal or MLA records

RECORDS MANAGEMENT

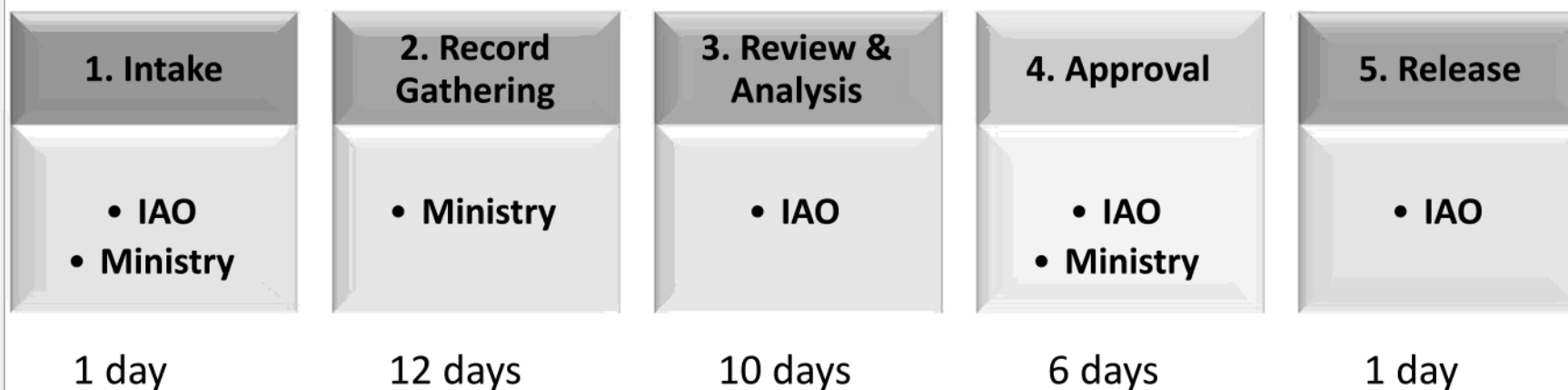
- Records created or received while doing Government business must be managed according to legislation, litigation requirements and Government policy and are subject to FOI and Government policy regardless of where they are located.
- Government email must be conducted using approved Government email systems, not personal email systems. This is essential for information security, privacy protection and effective management of the information
- Government records that are not transitory should be filed in the office's record-keeping system (e.g., TRIM or LAN) and must not be destroyed without an approved schedule (e.g., ARCS/ORCS) or before the schedule allows
- Employees must keep Government records separate from material relating to ministers' constituency matters, legislative committee involvement and other MLA activities. Those, and personal (e.g., family) records, are not Government records

RESPONSES WITH RECORDS AND NO RECORDS

Fiscal Year	Number of Closed Requests	On-Time Requests	Percentage of No Records Responses
2009/10	7,750	6,984	21%
2010/11	7,939	7,145	24%
2011/12	8,212	7,392	21%
2012/13	9,524	8,325	25%

CROSS GOVERNMENT REQUEST – TIMELINES

30 DAYS!



Unless.....

The request necessitates a 30 Day Extension under the Act

WHAT HAPPENS WHEN AN FOI REQUEST IS RECEIVED?

- Standard Call for Records Forms and Guidelines for record submissions are provided to all ministry program areas
- Ministry responsibilities include provision of the following information to IAO:
 - where search for records was conducted (i.e. TRIM files, databases, off-site records)
 - duration of search time by ministry program area
 - who conducted the record search
 - potential HARMS that could result from disclosure of records gathered
 - ISSUES associated with disclosure of records gathered
 - regional locations where records pertaining to this request may reside

How the FOI Process Works

Mandatory Exceptions	
Section 12	Cabinet confidence
Section 21	Third party business information
Section 22	Personal information
Discretionary Exceptions	
Section 13	Policy advice/recommendations
Section 14	Legal advice
Section 15	Law enforcement
Section 16	Intergovernmental relations
Section 17	Financial or economic interests
Section 18	Heritage sites
Section 19	Personal health or safety
Section 20	Information soon to be published

FOI APPROVAL PROCESS

- FOI requests are sent to program areas (ministries) for review and sign-off
- The DM or delegated head of the public body is responsible for final sign-off on all requests
- The DM or delegated head of the public body exercises discretion with respect to disclosure recommendations

FOI FAST FACTS

Government has maintained an on-time rate of **87%** despite a 57% increase in volume since 2008/09

In fiscal 2012/13, media requests were up by **68%** and political party requests were up by **48%**

For the first time, government is receiving almost as many **general** requests as **personal** requests

Government received over **10,000** FOI requests in 2012/13, a 22% increase over last fiscal

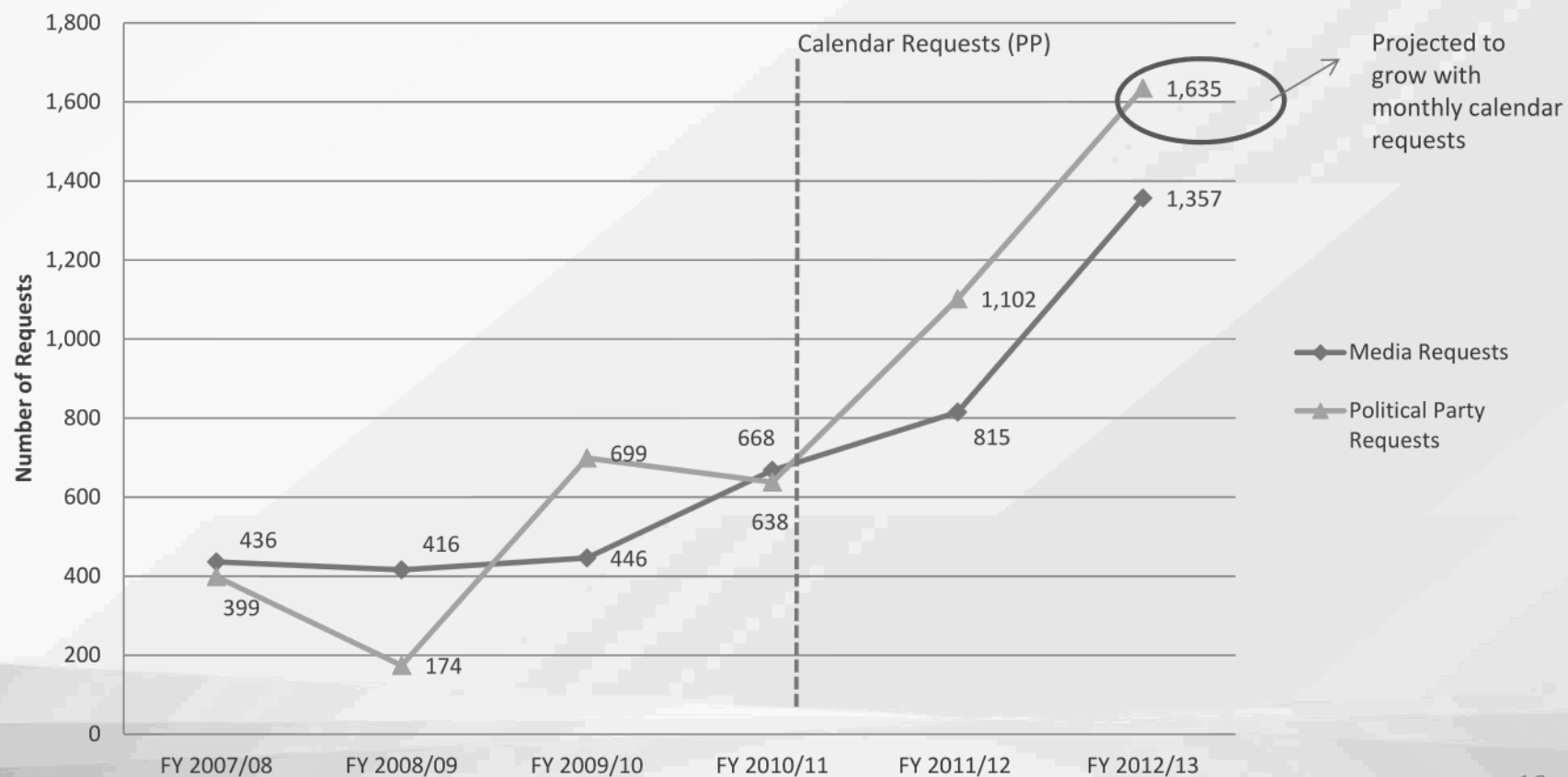
One media applicant made over **700 FOI requests** in 2012/13, and over 1,000 in the past 2 years

DEMAND FOR FOI REQUESTS CONTINUES TO INCREASE

Fiscal Year	General Requests	Personal Requests	Total Requests Received	% On-Time
2007/08	1,805	3,589	5,394	71
2008/09	1,693	4,877	6,570	74
2009/10	2,532	5,122	7,654	90
2010/11	2,756	5,073	7,829	93
2011/12	3,329	5,094	8,423	90
2012/13	4,815	5,484	10,299	87
2013/14 (projected)	4,000	5,500	9,500	75

CHANGING NATURE OF FOI APPLICANTS

Requests from Political Parties and Media



CALENDAR MANAGEMENT

- Government generally receives monthly or bi-monthly requests for DM, ADM and ED calendars and about 25 positions in the Office of the Premier. In November 2013, calendars for Ministers' Office Executive Assistants were included.

OUTLOOK CALENDARS

- Be wary of embedded documents, as the calendar and the attachments have different life spans
- Ensure calendar consistency and clarity
 - be clear about the subject of the meeting and who is expected to attend
 - keep the meeting subject concise
- Keep calendars current
 - update the calendar as changes occur
 - delete meetings that did not occur or were not attended
 - update the calendar to record the names and titles of individual(s) who actually attended the meeting as the calendar owner's representative
- Personal appointments
 - mark as "private" – details will not show up in a printed copy or to anyone other than the calendar owner or a delegate
 - caution – ensure that only personal appointments are labeled as "private". Calendar records must be accurate and are subject to a formal access request under FOIPPA
 - consider deleting "private" or personal appointments immediately after they occur

SEVERING GUIDELINES - CALENDAR ENTRIES

Entry or Description of Entry	Severed or Not Severed
Blackberry/cell phone numbers for government employees	Severed under section 17 (unless public)
"Cabinet" or "Cabinet Retreat"	Not Severed
"Treasury Board"	Not Severed
Accommodation details	Severed under section 15
Meeting location details	Severed under section 15
Constituency related – any entries in the Minister's calendar that relate to his/her duties as a Member of the Legislative Assembly (MLA)	Out of Scope - under section 3 - As the office of a Member of the Legislative Assembly is not a public body, any entries in a Minister's calendar that relate to his/her duties as an MLA will be severed as outside the scope of FOIPPA
360's (executive performance review), mentoring, EPDP	Severed under section 22

OPEN INFORMATION

- Introduced July 2011 with policy guidelines
- 2,300 General FOI requests posted (no Personals)
- Over 1,000 Minister and Deputy Minister travel expense summaries posted
- Over 52,000 visits to and 38,000 downloads from the Open Information website
- Proactively released 53 per cent of eligible general requests
- Requests are exempt from publication due to security concerns (72 per cent), personal information (14 per cent), and business information (12 per cent)



Contact Information

Brad Williams, a/Executive Director, FOI

250 356-7343

FOI Managers:

Sector

Manager

Justice/Social

Vicki Hudson

250 356-0845

Central Agencies

Cindy Elbahir

250 952-6355

Natural Resources

Kris Ghag

250 356-5702

Business/Infrastructure

Russ Fuller

250 387-4503

Health/Education

Maxine Vanzetta

250 387-9805

Personals

Vivian McDonald

250 356-6266

Intake

Cindy Kukucska

250 387-7356

Open Information

Chad Hoskins

250 387-2044



Logistics and Business Services

FREEDOM OF INFORMATION

Presented October 2013

FREEDOM OF INFORMATION

1. What you need to know about the FOI Act
2. How the FOI process works
3. Email
4. Trends in FOI
5. Calendars
6. Open Information
7. FOI Contacts

PURPOSES OF THE ACT

Accountability to the Public

- Legislated right to access all government records - specifying limited exceptions (i.e. make what is commonly referred to as an 'FOI request')

Protection of Privacy

- Provides a right of access to individuals own personal information
- Regulates how public bodies collect, use and disclose personal information
- Right to request correction of personal information

Body's decision(s) made under FOIPPA

- The independent reviews extend beyond decisions regarding disclosure

Purposes of the Act

ACCOUNTABILITY

RIGHT OF ACCESS TO
RECORDS



PRIVACY

PREVENT UNAUTHORIZED
COLLECTION, USE OR
DISCLOSURE OF PERSONAL
INFORMATION

INDEPENDENT OVERSIGHT

WHO IS COVERED BY THE ACT

All provincial ministries, and most provincial agencies, boards, commissions, Crown corporations and smaller agencies

Local public bodies

- School Districts
- Colleges and universities
- Regional health boards

Self-governing professions and occupations

- Teachers
- Doctors
- Nurses

➤ Government is only responsible for requests to BC government ministries

WHAT RECORDS ARE COVERED BY THE ACT

All records in the **custody** or under the **control** of a public body

What is a Record?

- Any information recorded or stored by any means whether in hard copy or in electronic format
- Regardless of content and subject matter, the following are subject to an FOI request:
 - briefing notes
 - vouchers
 - telephone records
 - notebooks/daybooks
 - contractor records
 - email
 - records on your smart phone
 - transitory records

CROSS GOVERNMENT REQUEST – TIMELINES

30 DAYS!



Unless.....

The request necessitates a 30 Day Extension under the Act

WHAT HAPPENS WHEN AN FOI REQUEST IS RECEIVED?

- Standard Call for Records Forms and Guidelines for record submissions are provided to all ministry program areas
- Ministry responsibilities include provision of the following information to IAO:
 - where search for records was conducted (i.e. TRIM files, databases, off-site records)
 - duration of search time by ministry program area
 - who conducted the record search
 - potential HARMS that could result from disclosure of records gathered
 - ISSUES associated with disclosure of records gathered
 - regional locations where records pertaining to this request may reside

How FOI Works

Mandatory Exceptions	
Section 12	Cabinet confidence
Section 21	Third party business information
Section 22	Personal information
Discretionary Exceptions	
Section 13	Policy advice/recommendations
Section 14	Legal advice
Section 15	Law enforcement
Section 16	Intergovernmental relations
Section 17	Financial or economic interests
Section 18	Heritage sites
Section 19	Personal health or safety
Section 20	Information soon to be published

FOI APPROVAL PROCESS

- FOI requests are sent to program areas (ministries) for review and sign-off
- The DM or delegated head of the public body is responsible for final sign-off on all requests
- The DM or delegated head of the public body exercises discretion with respect to disclosure recommendations

EMAIL MANAGEMENT

- Email messages created or received while doing Government business are records and must be managed according to legislation, litigation requirements and Government policy. They are subject to FOI and Government policy regardless of where they are located.
- Government email must be conducted using approved Government email systems, not personal email systems. This is essential for information security, privacy protection and effective management of the information.
 - Government email that is not transitory should be filed in the office's record-keeping system (e.g., TRIM or LAN) and must not be destroyed without an approved schedule (e.g., ARCS/ORCS) or before the schedule allows.
 - Transitory emails are of temporary usefulness and needed only to complete a routine action or prepare a final record (e.g., convenience copies, preliminary drafts, routine messages not needed to document a decision or action). These should be deleted when of no further use.
 - Employees must keep Government email separate from material relating to ministers' constituency matters, legislative committee involvement and other MLA activities. Those, and personal (e.g., family) records, are not Government records.

FOI FAST FACTS

Government has maintained an on-time rate of **87%** despite a 57% increase in volume since 2008/09

In fiscal 2012/13, media requests were up by **68%** and political party requests were up by **48%**

For the first time, government is receiving almost as many **general** requests as **personal** requests

Government received over **10,000** FOI requests in 2012/13, a 22% increase over last fiscal

One media applicant made over **700 FOI requests** in 2012/13, and over 1,000 in the past 2 years

DEMAND FOR FOI REQUESTS CONTINUES TO INCREASE

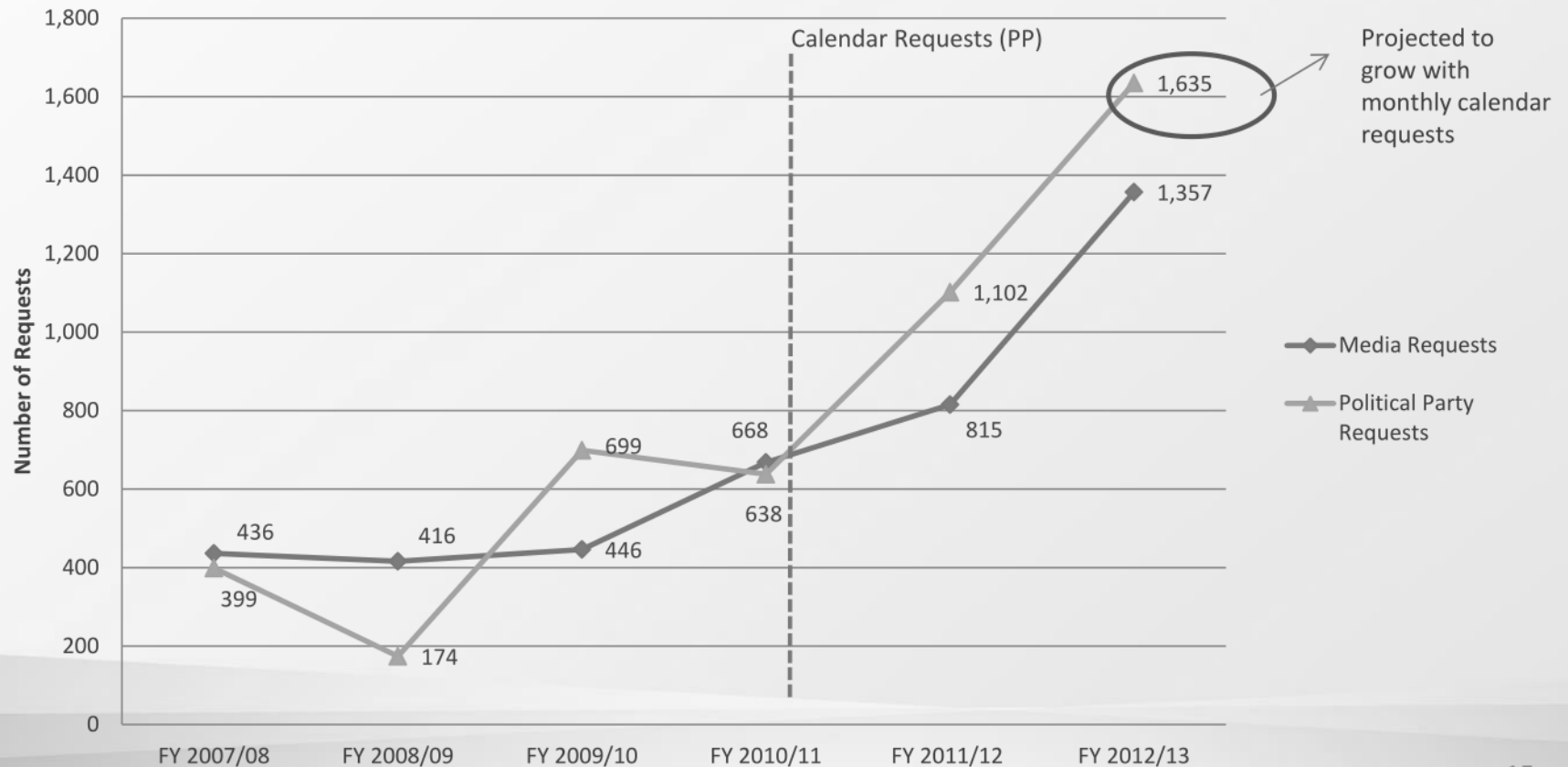
Fiscal Year	General Requests	Personal Requests	Total Requests Received	% On-Time
2007/08	1,805	3,589	5,394	71
2008/09	1,693	4,877	6,570	74
2009/10	2,532	5,122	7,654	90
2010/11	2,756	5,073	7,829	93
2011/12	3,329	5,094	8,423	90
2012/13	4,815	5,484	10,299	87
2013/14 (projected)	4,000	5,500	9,500	75

RESPONSES WITH RECORDS AND NO RECORDS

Fiscal Year	Number of Closed Requests	On-Time Requests	Percentage of No Records Responses
2009/10	7,750	6,984	21%
2010/11	7,939	7,145	24%
2011/12	8,212	7,392	21%
2012/13	9,524	8,325	25%

CHANGING NATURE OF FOI APPLICANTS

Requests from Political Parties and Media



CALENDAR MANAGEMENT

- Government generally receives monthly or bi-monthly requests for DM and ADM calendars. Last month, the requestor included ED calendars

OUTLOOK CALENDARS

- Be wary of embedded documents, as the calendar and the attachments have different life spans
- Ensure calendar consistency and clarity
 - be clear about the subject of the meeting and who is expected to attend
 - keep the meeting subject concise
- Keep calendars current
 - update the calendar as changes occur
 - delete meetings that did not occur or were not attended
 - update the calendar to record the names and titles of individual(s) who actually attended the meeting as the calendar owner's representative
- Personal appointments
 - mark as "private" – details will not show up in a printed copy or to anyone other than the calendar owner or a delegate
 - caution – ensure that only personal appointments are labeled as "private". Calendar records must be accurate and are subject to a formal access request under FOIPPA
 - consider deleting "private" or personal appointments immediately after they occur

SEVERING GUIDELINES - CALENDAR ENTRIES

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

OPEN INFORMATION

- Introduced July 2011 with policy guidelines
- 2,300 General FOI requests posted (no Personals)
- Over 1,000 Minister and Deputy Minister travel expense summaries posted
- Over 52,000 visits to and 38,000 downloads from the Open Information website
- Proactively released 53 per cent of eligible general requests
- Requests are exempt from publication due to security concerns (72 per cent), personal information (14 per cent), and business information (12 per cent)

Contact Information

Kathleen Ward, Executive Director, IAO

250 387-9807

Brad Williams, Director, FOI

250 356-7343

FOI Managers:

Sector

Manager

Justice/Social

Vicki Hudson

250 356-0845

Central Agencies

Cindy Elbahir

250 952-6355

Natural Resources

Kris Ghag

250 356-5702

Business/Infrastructure

Russ Fuller

250 387-4503

Health/Education

Maxine Vanzetta

250 387-9805

Personals

Vivian McDonald

250 356-6266

Intake

Cindy Kukucska

250 387-7356

Open Information

Chad Hoskins

250 387-2044



Logistics and Business Services

FREEDOM OF INFORMATION

Presented October 2013

FREEDOM OF INFORMATION

1. What you need to know about the FOI Act
2. Records Management
3. FOI
4. How the FOI process works
5. Trends in FOI
6. Calendars
7. Open Information
8. FOI Contacts

PURPOSES OF THE ACT

Accountability to the Public

- Legislated right to access all government records - specifying limited exceptions (i.e. make what is commonly referred to as an 'FOI request')

Protection of Privacy

- Provides a right of access to individuals own personal information
- Regulates how public bodies collect, use and disclose personal information
- Right to request correction of personal information

Body's decision(s) made under FOIPPA

- The independent reviews extend beyond decisions regarding disclosure

Purposes of the Act

ACCOUNTABILITY

RIGHT OF ACCESS TO
RECORDS



PRIVACY

PREVENT UNAUTHORIZED
COLLECTION, USE OR
DISCLOSURE OF PERSONAL
INFORMATION

INDEPENDENT OVERSIGHT

WHO IS COVERED BY THE ACT

All provincial ministries, and most provincial agencies, boards, commissions, Crown corporations and smaller agencies

Local public bodies

- School Districts
- Colleges and universities
- Regional health boards

Self-governing professions and occupations

- Teachers
- Doctors
- Nurses

➤ Government is only responsible for requests to BC government ministries

WHAT RECORDS ARE COVERED BY THE ACT

All records in the **custody** or under the **control** of a public body

What is a Record?

- Any information recorded or stored by any means whether in hard copy or in electronic format
- Regardless of content and subject matter, the following are subject to an FOI request:
 - briefing notes
 - vouchers
 - telephone records
 - notebooks/daybooks
 - contractor records
 - email
 - records on your smart phone
 - transitory records

TRANSITORY RECORDS

- Are records of temporary usefulness not required to document decisions and actions or to support ongoing government business (see handout)
- Should be regularly deleted as their usefulness ends (e.g. transitory emails of no further use can be deleted as you work through the following procedures)
- Does not apply to personal or MLA records

RECORDS MANAGEMENT

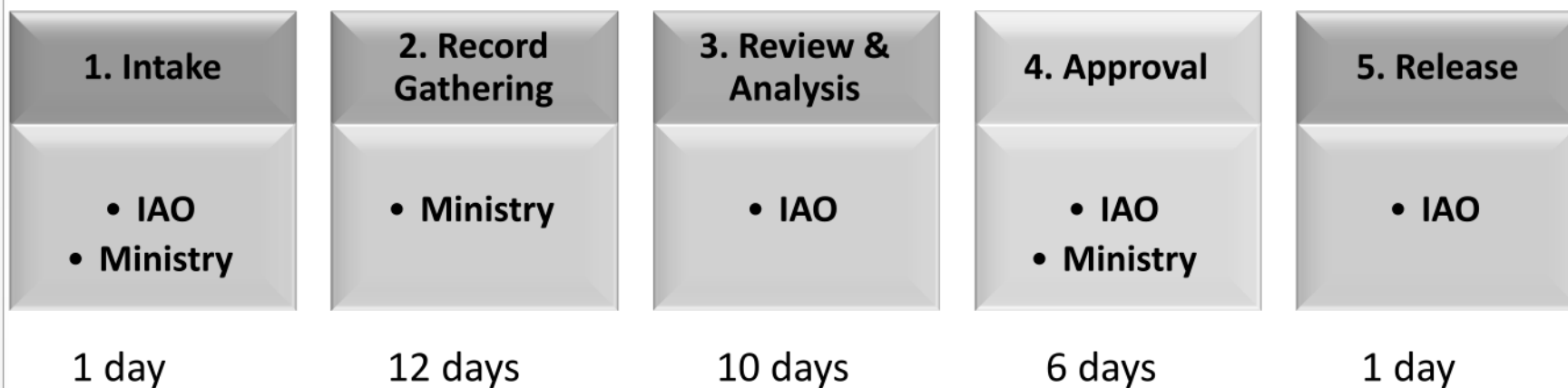
- Records created or received while doing Government business must be managed according to legislation, litigation requirements and Government policy and are subject to FOI and Government policy regardless of where they are located.
- Government email must be conducted using approved Government email systems, not personal email systems. This is essential for information security, privacy protection and effective management of the information.
- Government records that are not transitory should be filed in the office's record-keeping system (e.g., TRIM or LAN) and must not be destroyed without an approved schedule (e.g., ARCS/ORCS) or before the schedule allows.
- Employees must keep Government records separate from material relating to ministers' constituency matters, legislative committee involvement and other MLA activities. Those, and personal (e.g., family) records, are not Government records.

RESPONSES WITH RECORDS AND NO RECORDS

Fiscal Year	Number of Closed Requests	On-Time Requests	Percentage of No Records Responses
2009/10	7,750	6,984	21%
2010/11	7,939	7,145	24%
2011/12	8,212	7,392	21%
2012/13	9,524	8,325	25%

CROSS GOVERNMENT REQUEST – TIMELINES

30 DAYS!



Unless.....

The request necessitates a 30 Day Extension under the Act

WHAT HAPPENS WHEN AN FOI REQUEST IS RECEIVED?

- Standard Call for Records Forms and Guidelines for record submissions are provided to all ministry program areas
- Ministry responsibilities include provision of the following information to IAO:
 - where search for records was conducted (i.e. TRIM files, databases, off-site records)
 - duration of search time by ministry program area
 - who conducted the record search
 - potential HARMS that could result from disclosure of records gathered
 - ISSUES associated with disclosure of records gathered
 - regional locations where records pertaining to this request may reside

How FOI Works

Mandatory Exceptions	
Section 12	Cabinet confidence
Section 21	Third party business information
Section 22	Personal information
Discretionary Exceptions	
Section 13	Policy advice/recommendations
Section 14	Legal advice
Section 15	Law enforcement
Section 16	Intergovernmental relations
Section 17	Financial or economic interests
Section 18	Heritage sites
Section 19	Personal health or safety
Section 20	Information soon to be published

FOI APPROVAL PROCESS

- FOI requests are sent to program areas (ministries) for review and sign-off
- The DM or delegated head of the public body is responsible for final sign-off on all requests
- The DM or delegated head of the public body exercises discretion with respect to disclosure recommendations

FOI FAST FACTS

Government has maintained an on-time rate of **87%** despite a 57% increase in volume since 2008/09

In fiscal 2012/13, media requests were up by **68%** and political party requests were up by **48%**

For the first time, government is receiving almost as many **general** requests as **personal** requests

Government received over **10,000** FOI requests in 2012/13, a 22% increase over last fiscal

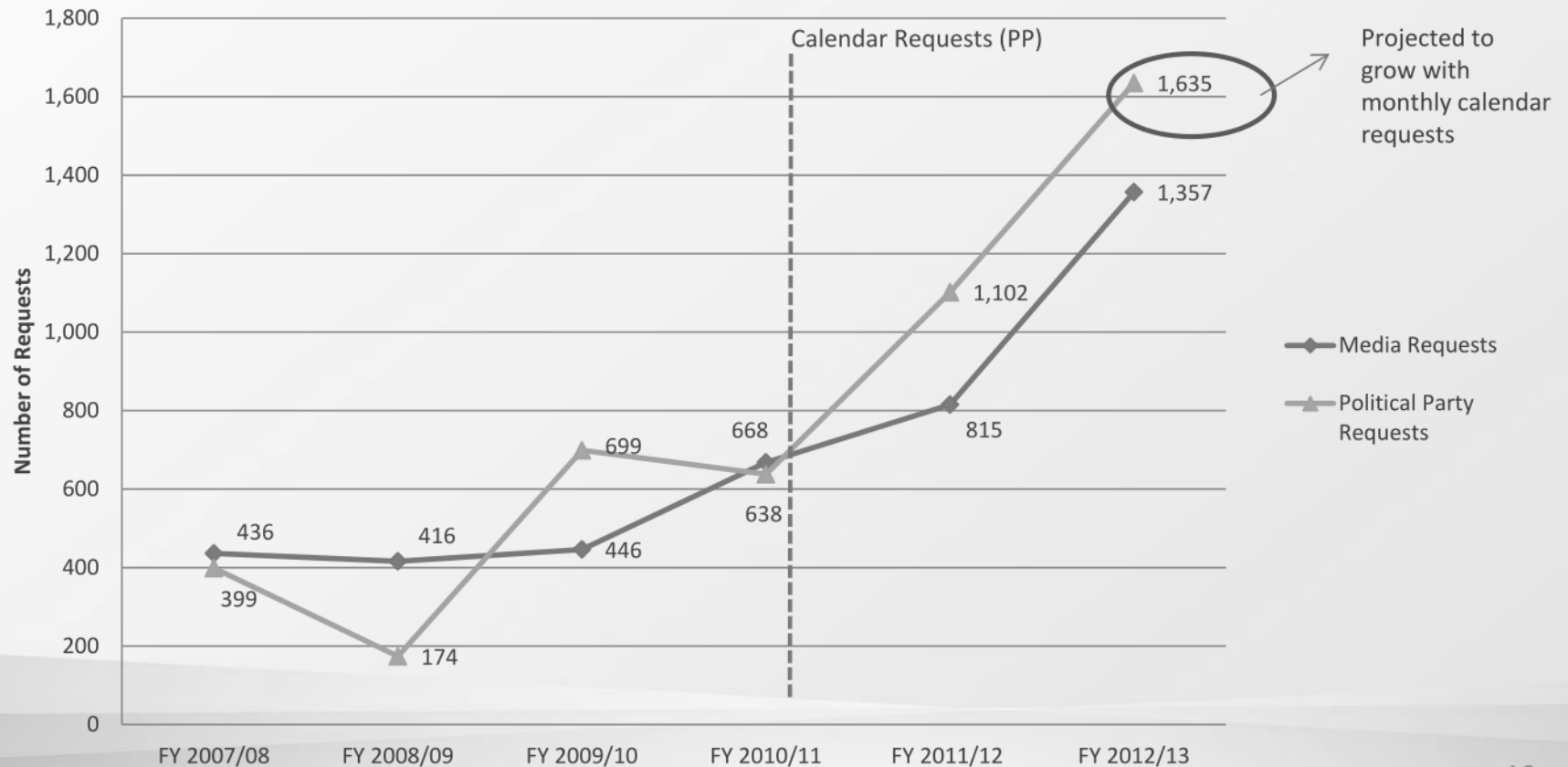
One media applicant made over **700 FOI requests** in 2012/13, and over 1,000 in the past 2 years

DEMAND FOR FOI REQUESTS CONTINUES TO INCREASE

Fiscal Year	General Requests	Personal Requests	Total Requests Received	% On-Time
2007/08	1,805	3,589	5,394	71
2008/09	1,693	4,877	6,570	74
2009/10	2,532	5,122	7,654	90
2010/11	2,756	5,073	7,829	93
2011/12	3,329	5,094	8,423	90
2012/13	4,815	5,484	10,299	87
2013/14 (projected)	4,000	5,500	9,500	75

CHANGING NATURE OF FOI APPLICANTS

Requests from Political Parties and Media



CALENDAR MANAGEMENT

- Government generally receives monthly or bi-monthly requests for DM and ADM calendars. Last month, the requestor included ED calendars

OUTLOOK CALENDARS

- Be wary of embedded documents, as the calendar and the attachments have different life spans
- Ensure calendar consistency and clarity
 - be clear about the subject of the meeting and who is expected to attend
 - keep the meeting subject concise
- Keep calendars current
 - update the calendar as changes occur
 - delete meetings that did not occur or were not attended
 - update the calendar to record the names and titles of individual(s) who actually attended the meeting as the calendar owner's representative
- Personal appointments
 - mark as "private" – details will not show up in a printed copy or to anyone other than the calendar owner or a delegate
 - caution – ensure that only personal appointments are labeled as "private". Calendar records must be accurate and are subject to a formal access request under FOIPPA
 - consider deleting "private" or personal appointments immediately after they occur

SEVERING GUIDELINES - CALENDAR ENTRIES

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

OPEN INFORMATION

- Introduced July 2011 with policy guidelines
- 2,300 General FOI requests posted (no Personals)
- Over 1,000 Minister and Deputy Minister travel expense summaries posted
- Over 52,000 visits to and 38,000 downloads from the Open Information website
- Proactively released 53 per cent of eligible general requests
- Requests are exempt from publication due to security concerns (72 per cent), personal information (14 per cent), and business information (12 per cent)

Contact Information

Kathleen Ward, Executive Director, IAO

250 387-9807

Brad Williams, Director, FOI

250 356-7343

FOI Managers:

Sector

Manager

Justice/Social

Vicki Hudson

250 356-0845

Central Agencies

Cindy Elbahir

250 952-6355

Natural Resources

Kris Ghag

250 356-5702

Business/Infrastructure

Russ Fuller

250 387-4503

Health/Education

Maxine Vanzetta

250 387-9805

Personals

Vivian McDonald

250 356-6266

Intake

Cindy Kukucska

250 387-7356

Open Information

Chad Hoskins

250 387-2044



Logistics and Business Services

FREEDOM OF INFORMATION

Presented September 2013

FREEDOM OF INFORMATION

1. What you need to know about the FOI Act
2. How the FOI process works
3. Email
4. Trends in FOI
5. Calendars
6. Open Information
7. FOI Contacts

PURPOSES OF THE ACT

Accountability to the Public

- Legislated right to access all government records - specifying limited exceptions (i.e. make what is commonly referred to as an 'FOI request')

Protection of Privacy

- Provides a right of access to individuals own personal information
- Regulates how public bodies collect, use and disclose personal information
- Right to request correction of personal information

Body's decision(s) made under FOIPPA

- The independent reviews extend beyond decisions regarding disclosure

Purposes of the Act

ACCOUNTABILITY

RIGHT OF ACCESS TO
RECORDS



PRIVACY

PREVENT UNAUTHORIZED
COLLECTION, USE OR
DISCLOSURE OF PERSONAL
INFORMATION

INDEPENDENT OVERSIGHT

WHO IS COVERED BY THE ACT

All provincial ministries, and most provincial agencies, boards, commissions, Crown corporations and smaller agencies

Local public bodies

- School Districts
- Colleges and universities
- Regional health boards

Self-governing professions and occupations

- Teachers
- Doctors
- Nurses

➤ Government is only responsible for requests to BC government ministries

WHAT RECORDS ARE COVERED BY THE ACT

All records in the **custody** or under the **control** of a public body

What is a Record?

- Any information recorded or stored by any means whether in hard copy or in electronic format
- Regardless of content and subject matter, the following are subject to an FOI request:
 - briefing notes
 - vouchers
 - telephone records
 - notebooks/daybooks
 - contractor records
 - email
 - records on your smart phone
 - transitory records

CROSS GOVERNMENT REQUEST – TIMELINES

30 DAYS!



Unless.....

The request necessitates a 30 Day Extension under the Act

WHAT HAPPENS WHEN AN FOI REQUEST IS RECEIVED?

- Standard Call for Records Forms and Guidelines for record submissions are provided to all ministry program areas
- Ministry responsibilities include provision of the following information to IAO:
 - where search for records was conducted (i.e. TRIM files, databases, off-site records)
 - duration of search time by ministry program area
 - who conducted the record search
 - potential HARMS that could result from disclosure of records gathered
 - ISSUES associated with disclosure of records gathered
 - regional locations where records pertaining to this request may reside

How FOI Works

Mandatory Exceptions	
Section 12	Cabinet confidence
Section 21	Third party business information
Section 22	Personal information
Discretionary Exceptions	
Section 13	Policy advice/recommendations
Section 14	Legal advice
Section 15	Law enforcement
Section 16	Intergovernmental relations
Section 17	Financial or economic interests
Section 18	Heritage sites
Section 19	Personal health or safety
Section 20	Information soon to be published

FOI APPROVAL PROCESS

- FOI requests are sent to program areas (ministries) for review and sign-off
- The DM or delegated head of the public body is responsible for final sign-off on all requests
- The DM or delegated head of the public body exercises discretion with respect to disclosure recommendations

EMAIL MANAGEMENT

- Email messages created or received while doing Government business are records and must be managed according to legislation, litigation requirements and Government policy. They are subject to FOI and Government policy regardless of where they are located.
- Government email must be conducted using approved Government email systems, not personal email systems. This is essential for information security, privacy protection and effective management of the information.
 - Government email that is not transitory should be filed in the office's record-keeping system (e.g., TRIM or LAN) and must not be destroyed without an approved schedule (e.g., ARCS/ORCS) or before the schedule allows.
 - Transitory emails are of temporary usefulness and needed only to complete a routine action or prepare a final record (e.g., convenience copies, preliminary drafts, routine messages not needed to document a decision or action). These should be deleted when of no further use.
 - Employees must keep Government email separate from material relating to ministers' constituency matters, legislative committee involvement and other MLA activities. Those, and personal (e.g., family) records, are not Government records.

FOI FAST FACTS

Government has maintained an on-time rate of **87%** despite a 57% increase in volume since 2008/09

In fiscal 2012/13, media requests were up by **68%** and political party requests were up by **48%**

For the first time, government is receiving almost as many **general** requests as **personal** requests

Government received over **10,000** FOI requests in 2012/13, a 22% increase over last fiscal

One media applicant made over **700 FOI requests** in 2012/13, and over 1,000 in the past 2 years

DEMAND FOR FOI REQUESTS CONTINUES TO INCREASE

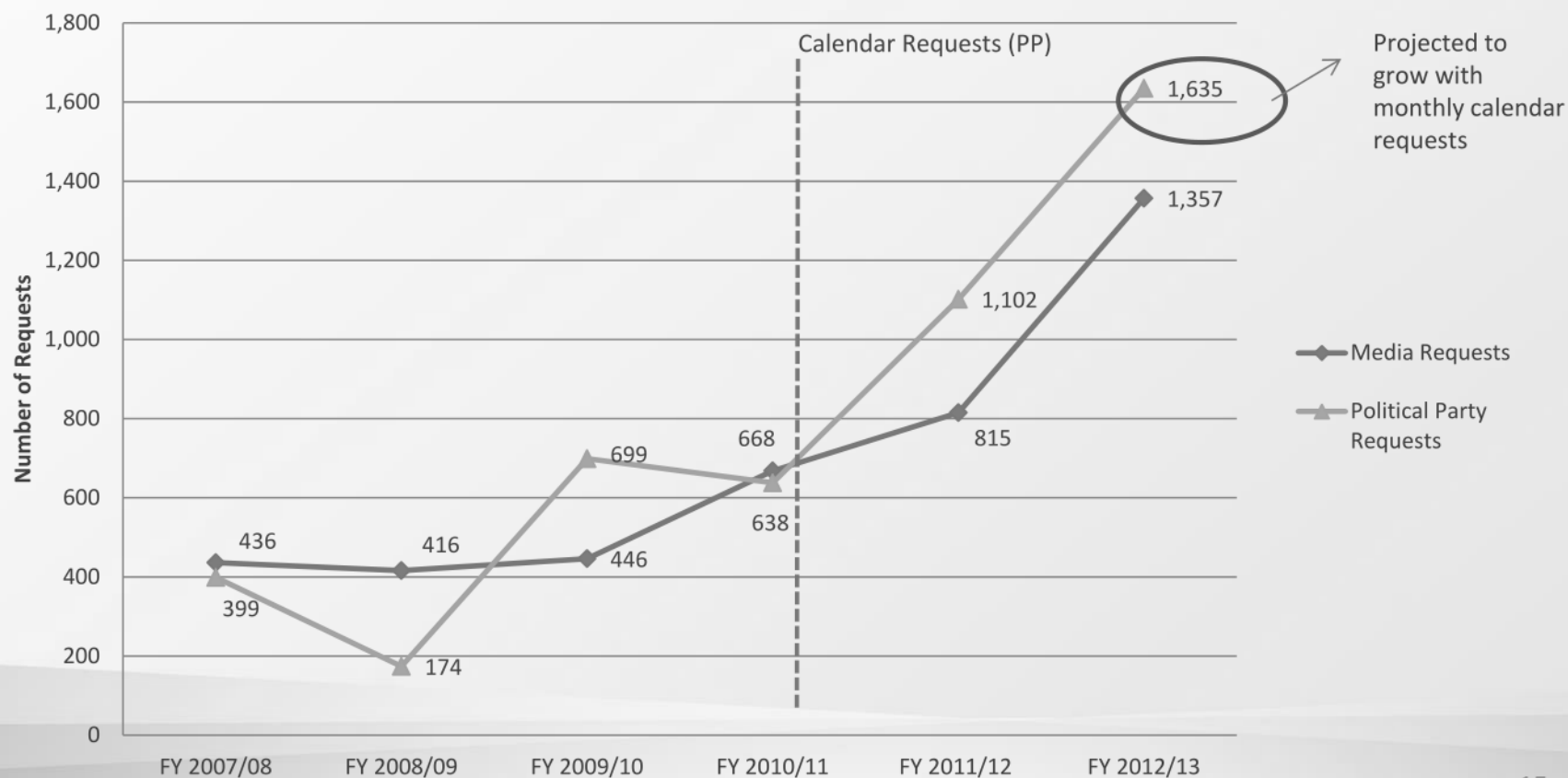
Fiscal Year	General Requests	Personal Requests	Total Requests Received	% On-Time
2007/08	1,805	3,589	5,394	71
2008/09	1,693	4,877	6,570	74
2009/10	2,532	5,122	7,654	90
2010/11	2,756	5,073	7,829	93
2011/12	3,329	5,094	8,423	90
2012/13	4,815	5,484	10,299	87
2013/14 (projected)	4,000	5,500	9,500	75

RESPONSES WITH RECORDS AND NO RECORDS

Fiscal Year	Number of Closed Requests	On-Time Requests	Percentage of No Records Responses
2009/10	7,750	6,984	21%
2010/11	7,939	7,145	24%
2011/12	8,212	7,392	21%
2012/13	9,524	8,325	25%

CHANGING NATURE OF FOI APPLICANTS

Requests from Political Parties and Media



CALENDAR MANAGEMENT

- Government generally receives monthly or bi-monthly requests for DM and ADM calendars. Last month, the requestor included ED calendars

OUTLOOK CALENDARS

- Be wary of embedded documents, as the calendar and the attachments have different life spans
- Ensure calendar consistency and clarity
 - be clear about the subject of the meeting and who is expected to attend
 - keep the meeting subject concise
- Keep calendars current
 - update the calendar as changes occur
 - delete meetings that did not occur or were not attended
 - update the calendar to record the names and titles of individual(s) who actually attended the meeting as the calendar owner's representative
- Personal appointments
 - mark as "private" – details will not show up in a printed copy or to anyone other than the calendar owner or a delegate
 - caution – ensure that only personal appointments are labeled as "private". Calendar records must be accurate and are subject to a formal access request under FOIPPA
 - consider deleting "private" or personal appointments immediately after they occur

SEVERING GUIDELINES - CALENDAR ENTRIES

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

OPEN INFORMATION

- Introduced July 2011 with policy guidelines
- 2,300 General FOI requests posted (no Personals)
- Over 1,000 Minister and Deputy Minister travel expense summaries posted
- Over 52,000 visits to and 38,000 downloads from the Open Information website
- Proactively released 53 per cent of eligible general requests
- Requests are exempt from publication due to security concerns (72 per cent), personal information (14 per cent), and business information (12 per cent)

Contact Information

Kathleen Ward, Executive Director, IAO

250 387-9807

Brad Williams, Director, FOI

250 356-7343

FOI Managers:

Sector

Manager

Justice/Social

Vicki Hudson

250 356-0845

Central Agencies

Cindy Elbahir

250 952-6355

Natural Resources

Kris Ghag

250 356-5702

Business/Infrastructure

Russ Fuller

250 387-4503

Health/Education

Maxine Vanzetta

250 356-7349

Personals

Vivian McDonald

250 356-6266

Intake

Cindy Kukucska

250 387-7356

Open Information

Chad Hoskins

250 387-2044



Logistics and Business Services

FREEDOM OF INFORMATION

Presented April 2014

FREEDOM OF INFORMATION

1. What you need to know about the FOI Act
2. Records Management
3. FOI
4. How the FOI process works
5. Trends in FOI
6. Calendars
7. Open Information
8. FOI Contacts

PURPOSES OF THE ACT

Accountability to the Public

- Legislated right to access all government records - specifying limited exceptions (i.e. make what is commonly referred to as an 'FOI request')

Protection of Privacy

- Provides a right of access to individuals own personal information
- Regulates how public bodies collect, use and disclose personal information
- Right to request correction of personal information

Independent Oversight by the Office of the Information & Privacy Commissioner

- Conducts reviews on decisions regarding disclosure

Purposes of the Act

ACCOUNTABILITY

RIGHT OF ACCESS TO
RECORDS



PRIVACY

PREVENT UNAUTHORIZED
COLLECTION, USE OR
DISCLOSURE OF PERSONAL
INFORMATION

INDEPENDENT OVERSIGHT

WHO IS COVERED BY THE ACT

All provincial ministries, and most provincial agencies, boards, commissions, Crown corporations and smaller agencies

Local public bodies

- School Districts
- Colleges and universities
- Regional health boards

Self-governing professions and occupations

- Teachers
 - Doctors
 - Nurses
- Government is only responsible for requests to BC government ministries

WHAT RECORDS ARE COVERED BY THE ACT

All records in the **custody** or under the **control** of a public body

What is a Record?

- Any information recorded or stored by any means whether in hard copy or in electronic format
- Regardless of content and subject matter, the following are subject to an FOI request:
 - briefing notes
 - vouchers
 - telephone records
 - notebooks/daybooks
 - contractor records
 - email
 - records on your smart phone
 - transitory records

TRANSITORY RECORDS

- Are records of temporary usefulness not required to document decisions and actions or to support ongoing government business
- Should be regularly deleted as their usefulness ends (e.g.: transitory emails of no further use can be deleted)
- The Transitory Records Schedule does not apply to personal or MLA records

RECORDS MANAGEMENT

- Records created or received while doing Government business must be managed according to legislation, litigation requirements and Government policy and are subject to FOI and Government policy regardless of where they are located.
- Government email must be conducted using approved Government email systems, not personal email systems. This is essential for information security, privacy protection and effective management of the information
- Government records that are not transitory should be filed in the office's record-keeping system (e.g., TRIM or LAN) and must not be destroyed without an approved schedule (e.g., ARCS/ORCS) or before the schedule allows
- Employees must keep Government records separate from material relating to ministers' constituency matters, legislative committee involvement and other MLA activities. Those, and personal (e.g., family) records, are not Government records

RESPONSES WITH RECORDS AND NO RECORDS

Fiscal Year	Number of Closed Requests	On-Time Requests	Percentage of No Records Responses
2009/10	7,750	6,984	21%
2010/11	7,939	7,145	24%
2011/12	8,212	7,392	21%
2012/13	9,524	8,325	25%

CROSS GOVERNMENT REQUEST – TIMELINES

30 DAYS!



Unless.....

The request necessitates a 30 Day Extension under the Act

WHAT HAPPENS WHEN AN FOI REQUEST IS RECEIVED?

- Standard Call for Records Forms and Guidelines for record submissions are provided to all ministry program areas
- Ministry responsibilities include provision of the following information to IAO:
 - where search for records was conducted (i.e. TRIM files, databases, off-site records)
 - duration of search time by ministry program area
 - who conducted the record search
 - potential HARMS that could result from disclosure of records gathered
 - ISSUES associated with disclosure of records gathered
 - regional locations where records pertaining to this request may reside

How the FOI Process Works

Mandatory Exceptions	
Section 12	Cabinet confidence
Section 21	Third party business information
Section 22	Personal information
Discretionary Exceptions	
Section 13	Policy advice/recommendations
Section 14	Legal advice
Section 15	Law enforcement
Section 16	Intergovernmental relations
Section 17	Financial or economic interests
Section 18	Heritage sites
Section 19	Personal health or safety
Section 20	Information soon to be published

FOI APPROVAL PROCESS

- FOI requests are sent to program areas (ministries) for review and sign-off
- The DM or delegated head of the public body is responsible for final sign-off on all requests
- The DM or delegated head of the public body exercises discretion with respect to disclosure recommendations

FOI FAST FACTS

Government has maintained an on-time rate of **87%** despite a 57% increase in volume since 2008/09

In fiscal 2012/13, media requests were up by **68%** and political party requests were up by **48%**

For the first time, government is receiving almost as many **general** requests as **personal** requests

Government received over **10,000** FOI requests in 2012/13, a 22% increase over last fiscal

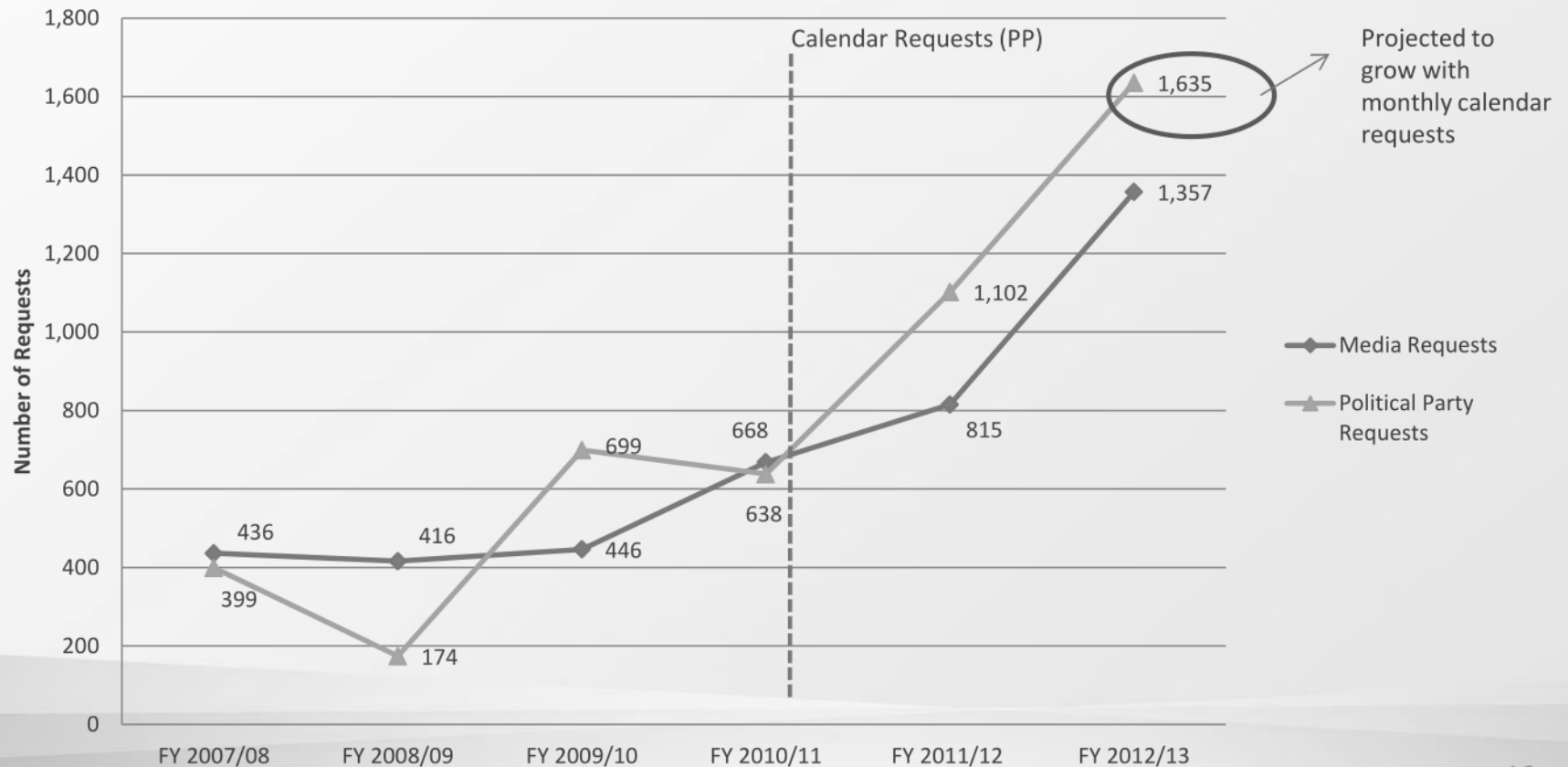
One media applicant made over **700 FOI requests** in 2012/13, and over 1,000 in the past 2 years

DEMAND FOR FOI REQUESTS CONTINUES TO INCREASE

Fiscal Year	General Requests	Personal Requests	Total Requests Received	% On-Time
2007/08	1,805	3,589	5,394	71
2008/09	1,693	4,877	6,570	74
2009/10	2,532	5,122	7,654	90
2010/11	2,756	5,073	7,829	93
2011/12	3,329	5,094	8,423	90
2012/13	4,815	5,484	10,299	87
2013/14 (projected)	4,000	5,500	9,500	75

CHANGING NATURE OF FOI APPLICANTS

Requests from Political Parties and Media



CALENDAR MANAGEMENT

- Government generally receives monthly or bi-monthly requests for DM, ADM and ED calendars and about 25 positions in the Office of the Premier. In November 2013, calendars for Ministers' Office Executive Assistants were included.

OUTLOOK CALENDARS

- Be wary of embedded documents, as the calendar and the attachments have different life spans
- Ensure calendar consistency and clarity
 - be clear about the subject of the meeting and who is expected to attend
 - keep the meeting subject concise
- Keep calendars current
 - update the calendar as changes occur
 - delete meetings that did not occur or were not attended
 - update the calendar to record the names and titles of individual(s) who actually attended the meeting as the calendar owner's representative
- Personal appointments
 - mark as "private" – details will not show up in a printed copy or to anyone other than the calendar owner or a delegate
 - caution – ensure that only personal appointments are labeled as "private". Calendar records must be accurate and are subject to a formal access request under FOIPPA
 - consider deleting "private" or personal appointments immediately after they occur

SEVERING GUIDELINES - CALENDAR ENTRIES

Entry or Description of Entry	Severed or Not Severed
Blackberry/cell phone numbers for government employees	Severed under section 17 (unless public)
"Cabinet" or "Cabinet Retreat"	Not Severed
"Treasury Board"	Not Severed
Accommodation details	Severed under section 15
Meeting location details	Severed under section 15
Constituency related – any entries in the Minister's calendar that relate to his/her duties as a Member of the Legislative Assembly (MLA)	Out of Scope - under section 3 - As the office of a Member of the Legislative Assembly is not a public body, any entries in a Minister's calendar that relate to his/her duties as an MLA will be severed as outside the scope of FOIPPA
360's (executive performance review), mentoring, EPDP	Severed under section 22

OPEN INFORMATION

- Introduced July 2011 with policy guidelines
- 2,300 General FOI requests posted (no Personals)
- Over 1,000 Minister and Deputy Minister travel expense summaries posted
- Over 52,000 visits to and 38,000 downloads from the Open Information website
- Proactively released 53 per cent of eligible general requests
- Requests are exempt from publication due to security concerns (72 per cent), personal information (14 per cent), and business information (12 per cent)

Contact Information

Brad Williams, a/Executive Director, FOI

250 356-7343

FOI Managers:

Sector

Manager

Justice/Social

Vicki Hudson

250 356-0845

Central Agencies

Cindy Elbahir

250 952-6355

Natural Resources

Kris Ghag

250 356-5702

Business/Infrastructure

Russ Fuller

250 387-4503

Health/Education

Maxine Vanzetta

250 387-9805

Personals

Vivian McDonald

250 356-6266

Intake

Cindy Kukucska

250 387-7356

Open Information

Chad Hoskins

250 387-2044

Logistics and Business Services

FREEDOM OF INFORMATION

Presented April 2015



FREEDOM OF INFORMATION

1. What you need to know about the FOI Act
2. Records Management
3. FOI
4. How the FOI process works
5. Trends in FOI
6. Calendars
7. Open Information
8. FOI Contacts



PURPOSES OF THE ACT

Accountability to the Public

- Legislated right to access all government records - specifying limited exceptions (i.e. make what is commonly referred to as an 'FOI request')

Protection of Privacy

- Provides a right of access to individuals own personal information
- Regulates how public bodies collect, use and disclose personal information
- Right to request correction of personal information

Independent Oversight by the Office of the Information & Privacy Commissioner

- Conducts reviews on decisions regarding disclosure

Purposes of the Act

ACCOUNTABILITY
RIGHT OF ACCESS
TO RECORDS



PRIVACY
PREVENT UNAUTHORIZED
COLLECTION, USE OR
DISCLOSURE OF
PERSONAL INFORMATION

INDEPENDENT OVERSIGHT



WHO IS COVERED BY THE ACT

All provincial ministries, and most provincial agencies, boards, commissions, Crown corporations and smaller agencies

Local public bodies

- School Districts
- Colleges and universities
- Regional health boards

Self-governing professions and occupations

- Teachers
- Doctors
- Nurses

➤ Government is only responsible for requests to BC government ministries



WHAT RECORDS ARE COVERED BY THE ACT

All records in the **custody** or under the **control** of a public body

What is a Record?

- Any information recorded or stored by any means whether in hard copy or in electronic format
- Regardless of content and subject matter, the following are subject to an FOI request:
 - briefing notes
 - vouchers
 - telephone records
 - notebooks/daybooks
 - contractor records
 - email
 - records on your smart phone
 - transitory records

TRANSITORY RECORDS

- Are records of temporary usefulness not required to document decisions and actions or to support ongoing government business
- Should be regularly deleted as their usefulness ends (e.g.: transitory emails of no further use can be deleted)
- The Transitory Records Schedule does not apply to personal or MLA records



RECORDS MANAGEMENT

- Records created or received while doing Government business must be managed according to legislation, litigation requirements and Government policy and are subject to FOI and Government policy regardless of where they are located.
- Government email must be conducted using approved Government email systems, not personal email systems. This is essential for information security, privacy protection and effective management of the information
- Government records that are not transitory should be filed in the office's record-keeping system (e.g., TRIM or LAN) and must not be destroyed without an approved schedule (e.g., ARCS/ORCS) or before the schedule allows
- Employees must keep Government records separate from material relating to ministers' constituency matters, legislative committee involvement and other MLA activities. Those, and personal (e.g., family) records, are not Government records

RESPONSES WITH RECORDS AND NO RECORDS

Fiscal Year	Number of Closed Requests	On-Time Requests	Percentage of No Records Responses
2009/10	7,750	6,984	21%
2010/11	7,939	7,145	24%
2011/12	8,212	7,392	21%
2012/13	9,524	8,325	25%
2013/14	9,827	7,272	19%
2014/15	8,377	6,588	17%



CROSS GOVERNMENT REQUEST – TIMELINES

30 DAYS!



Unless.....

The request necessitates a 30 Day Extension under the Act



WHAT HAPPENS WHEN AN FOI REQUEST IS RECEIVED?

- Standard Call for Records Forms and Guidelines for record submissions are provided to all ministry program areas
- Ministry responsibilities include provision of the following information to IAO:
 - where search for records was conducted (i.e. TRIM files, databases, off-site records)
 - duration of search time by ministry program area
 - who conducted the record search
 - potential HARMS that could result from disclosure of records gathered
 - ISSUES associated with disclosure of records gathered
 - regional locations where records pertaining to this request may reside

Mandatory Exceptions

Section 12	Cabinet confidence
Section 21	Third party business information
Section 22	Personal information

Discretionary Exceptions

Section 13	Policy advice/recommendations
Section 14	Legal advice
Section 15	Law enforcement
Section 16	Intergovernmental relations
Section 17	Financial or economic interests
Section 18	Heritage sites
Section 19	Personal health or safety
Section 20	Information soon to be published



FOI APPROVAL PROCESS

- FOI requests are sent to program areas (ministries) for review and sign-off
- The DM or delegated head of the public body is responsible for final sign-off on all requests
- The DM or delegated head of the public body exercises discretion with respect to disclosure recommendations

FOI FAST FACTS

Timeliness was down in 2013/14, but government is still responding to more requests **on-time** than it did prior to centralization in 2009.

Political party
requests
increased by
64% in
2013/14.

2013/14 was the
first year in which
government
received more
general than
personal requests.

Government received
close to **10,000** FOI
requests in 2013/14, a
25% increase over
2009/10.

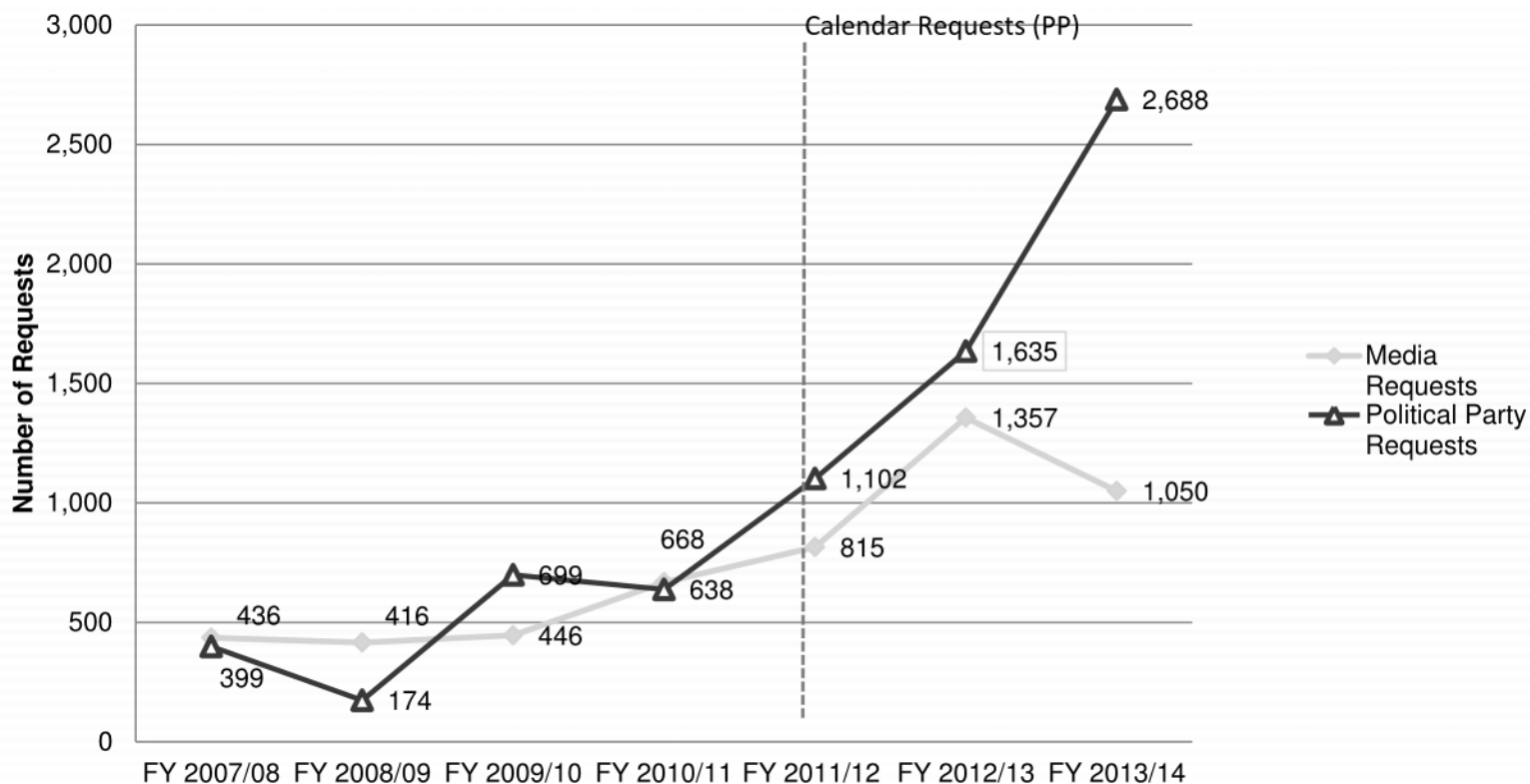
Government received
1,800 requests for the
calendars of senior
government
officials/employees.

DEMAND FOR FOI REQUESTS CONTINUES TO INCREASE

Fiscal Year	General Requests	Personal Requests	Total Requests Received	% On-Time
2008/09	1,693	4,877	6,570	74
2009/10	2,532	5,122	7,654	90
2010/11	2,756	5,073	7,829	93
2011/12	3,329	5,094	8,423	90
2012/13	4,815	5,484	10,299	87
2013/14	5,200	4,400	9,600	74
2014/15	4,124	4,151	8,275	79

CHANGING NATURE OF FOI APPLICANTS

Requests from Political Parties and Media





CALENDAR MANAGEMENT

- Government generally receives monthly or bi-monthly requests for DM, ADM and ED calendars and about 25 positions in the Office of the Premier. In November 2013, calendars for Ministers' Office Executive Assistants were included.

OUTLOOK CALENDARS

- Be wary of embedded documents, as the calendar and the attachments have different life spans
- Ensure calendar consistency and clarity
 - be clear about the subject of the meeting and who is expected to attend
 - keep the meeting subject concise
- Keep calendars current
 - update the calendar as changes occur
 - delete meetings that did not occur or were not attended
 - update the calendar to record the names and titles of individual(s) who actually attended the meeting as the calendar owner's representative
- Personal appointments
 - mark as "private" – details will not show up in a printed copy or to anyone other than the calendar owner or a delegate
 - caution – ensure that only personal appointments are labeled as "private". Calendar records must be accurate and are subject to a formal access request under FOIPPA
 - consider deleting "private" or personal appointments immediately after they occur



SEVERING GUIDELINES - CALENDAR ENTRIES

Entry or Description of Entry	Severed or Not Severed
Blackberry/cell phone numbers for government employees	Severed under section 17 (unless public)
"Cabinet" or "Cabinet Retreat"	Not Severed
"Treasury Board"	Not Severed
Accommodation details	Severed under section 15
Meeting location details	Severed under section 15
Constituency related – any entries in the Minister's calendar that relate to his/her duties as a Member of the Legislative Assembly (MLA)	Out of Scope - under section 3 - As the office of a Member of the Legislative Assembly is not a public body, any entries in a Minister's calendar that relate to his/her duties as an MLA will be severed as outside the scope of FOIPPA
360's (executive performance review), mentoring, EPDP	Severed under section 22



OPEN INFORMATION

- Introduced July 2011 with policy guidelines
- Over 5,000 General FOI requests posted (no Personals)
- Over 1,700 Minister and Deputy Minister travel expense summaries posted
- Over 21,000 visits to and 15,000 downloads from the Open Information website in 2013/14
- Proactively released 48 per cent of eligible general requests in 2013/14
- Requests are exempt from publication due to security concerns (82 per cent), business information (10 per cent), and personal information (7 per cent)



Contact Information

Brad Williams, Executive Director, FOI

250 357-9807

Chad Hoskins, Senior Director, FOI

250 356-7343

FOI Managers:

Sector

Manager

Justice/Social

Vicki Hudson

250 356-0845

Central Agencies

Cindy Elbahir

250 952-6355

Natural Resources

Kris Ghag

250 356-5702

Business/Infrastructure

Russ Fuller

250 387-4503

Health/Education

Maxine Vanzetta

250 387-9805

Personals

Vivian McDonald

250 356-6266

Intake/Open Information

Cindy Kukucska

250 387-7356



Shared
ServicesBC

Logistics and Business Services

FREEDOM OF INFORMATION

Presented August 2014

FREEDOM OF INFORMATION

1. What you need to know about the FOI Act
2. Records Management
3. FOI
4. How the FOI process works
5. Trends in FOI
6. Calendars
7. Open Information
8. FOI Contacts

PURPOSES OF THE ACT

Accountability to the Public

- Legislated right to access all government records - specifying limited exceptions (i.e. make what is commonly referred to as an 'FOI request')

Protection of Privacy

- Provides a right of access to individuals own personal information
- Regulates how public bodies collect, use and disclose personal information
- Right to request correction of personal information

Independent Oversight by the Office of the Information & Privacy Commissioner

- Conducts reviews on decisions regarding disclosure

Purposes of the Act

ACCOUNTABILITY

RIGHT OF ACCESS TO
RECORDS



PRIVACY

PREVENT UNAUTHORIZED
COLLECTION, USE OR
DISCLOSURE OF PERSONAL
INFORMATION

INDEPENDENT OVERSIGHT

WHO IS COVERED BY THE ACT

All provincial ministries, and most provincial agencies, boards, commissions, Crown corporations and smaller agencies

Local public bodies

- School Districts
- Colleges and universities
- Regional health boards

Self-governing professions and occupations

- Teachers
- Doctors
- Nurses

➤ Government is only responsible for requests to BC government ministries

WHAT RECORDS ARE COVERED BY THE ACT

All records in the **custody** or under the **control** of a public body

What is a Record?

- Any information recorded or stored by any means whether in hard copy or in electronic format
- Regardless of content and subject matter, the following are subject to an FOI request:
 - briefing notes
 - vouchers
 - telephone records
 - notebooks/daybooks
 - contractor records
 - email
 - records on your smart phone
 - transitory records

TRANSITORY RECORDS

- Are records of temporary usefulness not required to document decisions and actions or to support ongoing government business
- Should be regularly deleted as their usefulness ends (e.g.: transitory emails of no further use can be deleted)
- The Transitory Records Schedule does not apply to personal or MLA records

RECORDS MANAGEMENT

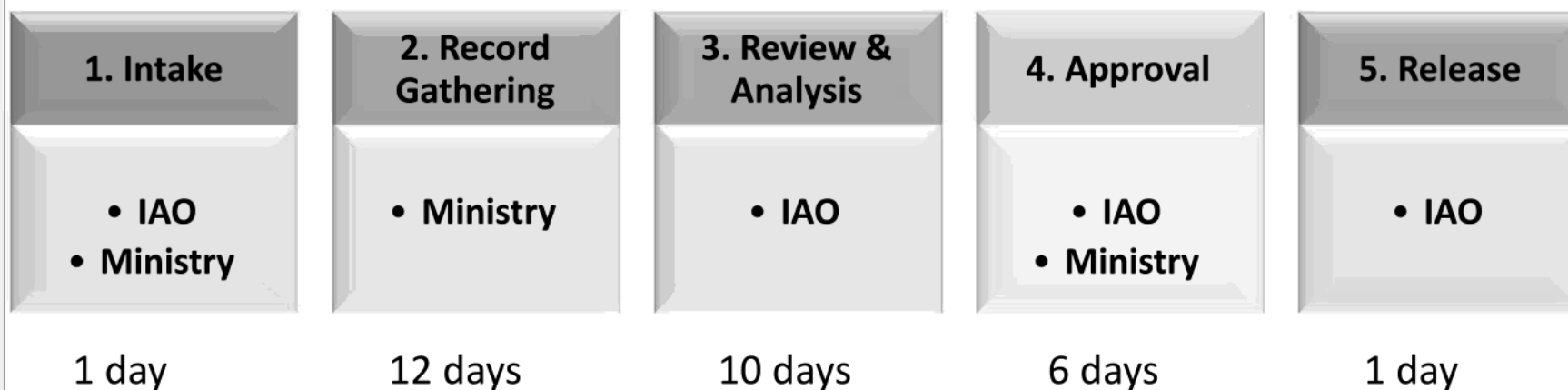
- Records created or received while doing Government business must be managed according to legislation, litigation requirements and Government policy and are subject to FOI and Government policy regardless of where they are located.
- Government email must be conducted using approved Government email systems, not personal email systems. This is essential for information security, privacy protection and effective management of the information
- Government records that are not transitory should be filed in the office's record-keeping system (e.g., TRIM or LAN) and must not be destroyed without an approved schedule (e.g., ARCS/ORCS) or before the schedule allows
- Employees must keep Government records separate from material relating to ministers' constituency matters, legislative committee involvement and other MLA activities. Those, and personal (e.g., family) records, are not Government records

RESPONSES WITH RECORDS AND NO RECORDS

Fiscal Year	Number of Closed Requests	On-Time Requests	Percentage of No Records Responses
2009/10	7,750	6,984	21%
2010/11	7,939	7,145	24%
2011/12	8,212	7,392	21%
2012/13	9,524	8,325	25%

CROSS GOVERNMENT REQUEST – TIMELINES

30 DAYS!



Unless.....

The request necessitates a 30 Day Extension under the Act

WHAT HAPPENS WHEN AN FOI REQUEST IS RECEIVED?

- Standard Call for Records Forms and Guidelines for record submissions are provided to all ministry program areas
- Ministry responsibilities include provision of the following information to IAO:
 - where search for records was conducted (i.e. TRIM files, databases, off-site records)
 - duration of search time by ministry program area
 - who conducted the record search
 - potential HARMS that could result from disclosure of records gathered
 - ISSUES associated with disclosure of records gathered
 - regional locations where records pertaining to this request may reside

How the FOI Process Works

Mandatory Exceptions	
Section 12	Cabinet confidence
Section 21	Third party business information
Section 22	Personal information
Discretionary Exceptions	
Section 13	Policy advice/recommendations
Section 14	Legal advice
Section 15	Law enforcement
Section 16	Intergovernmental relations
Section 17	Financial or economic interests
Section 18	Heritage sites
Section 19	Personal health or safety
Section 20	Information soon to be published

FOI APPROVAL PROCESS

- FOI requests are sent to program areas (ministries) for review and sign-off
- The DM or delegated head of the public body is responsible for final sign-off on all requests
- The DM or delegated head of the public body exercises discretion with respect to disclosure recommendations

FOI FAST FACTS

Government has maintained an on-time rate of **87%** despite a 57% increase in volume since 2008/09

In fiscal 2012/13, media requests were up by **68%** and political party requests were up by **48%**

For the first time, government is receiving almost as many **general** requests as **personal** requests

Government received over **10,000** FOI requests in 2012/13, a 22% increase over last fiscal

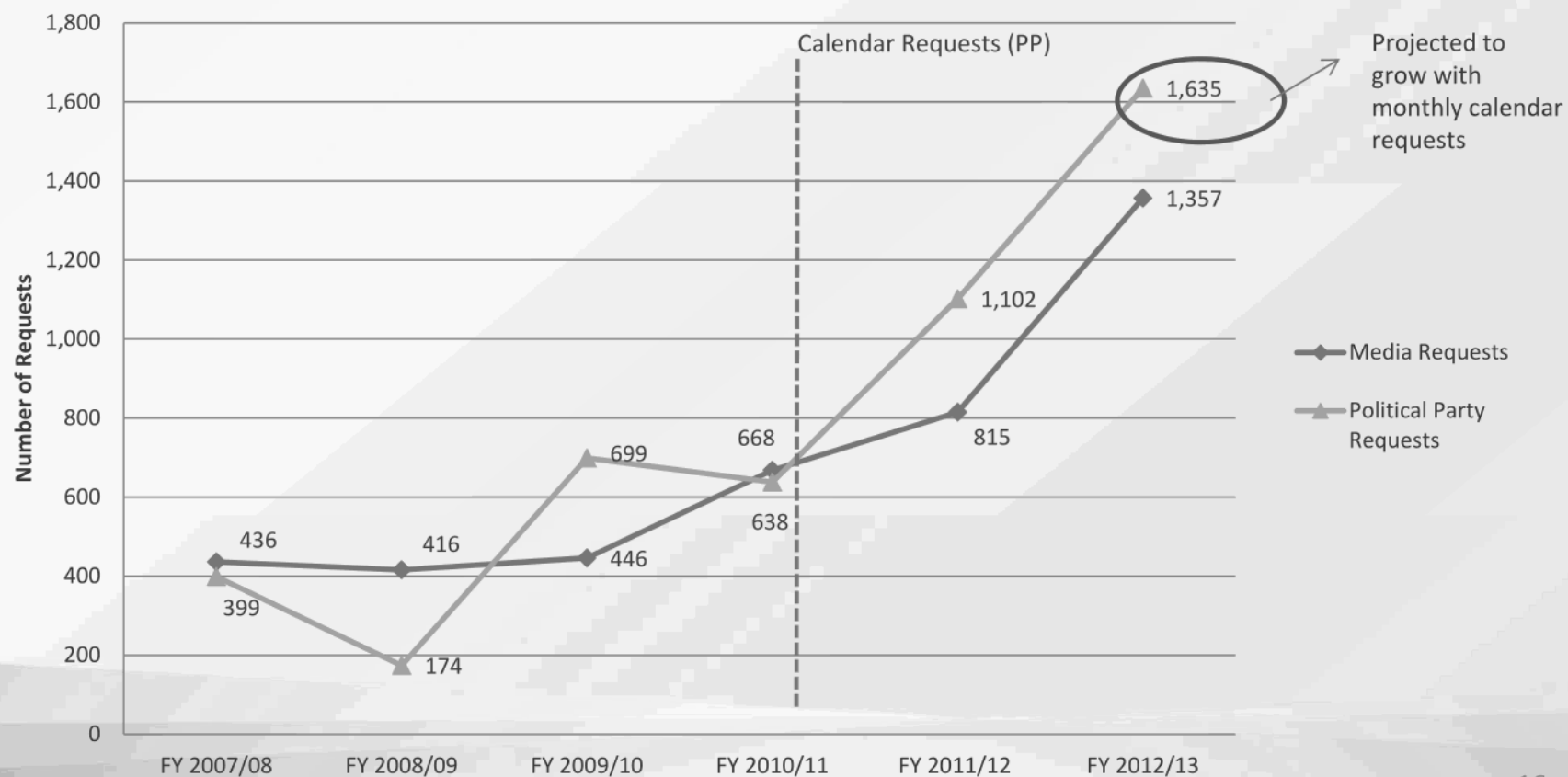
One media applicant made over **700 FOI requests** in 2012/13, and over 1,000 in the past 2 years

DEMAND FOR FOI REQUESTS CONTINUES TO INCREASE

Fiscal Year	General Requests	Personal Requests	Total Requests Received	% On-Time
2007/08	1,805	3,589	5,394	71
2008/09	1,693	4,877	6,570	74
2009/10	2,532	5,122	7,654	90
2010/11	2,756	5,073	7,829	93
2011/12	3,329	5,094	8,423	90
2012/13	4,815	5,484	10,299	87
2013/14 (projected)	4,000	5,500	9,500	75

CHANGING NATURE OF FOI APPLICANTS

Requests from Political Parties and Media



CALENDAR MANAGEMENT

- Government generally receives monthly or bi-monthly requests for DM, ADM and ED calendars and about 25 positions in the Office of the Premier. In November 2013, calendars for Ministers' Office Executive Assistants were included.

OUTLOOK CALENDARS

- Be wary of embedded documents, as the calendar and the attachments have different life spans
- Ensure calendar consistency and clarity
 - be clear about the subject of the meeting and who is expected to attend
 - keep the meeting subject concise
- Keep calendars current
 - update the calendar as changes occur
 - delete meetings that did not occur or were not attended
 - update the calendar to record the names and titles of individual(s) who actually attended the meeting as the calendar owner's representative
- Personal appointments
 - mark as "private" – details will not show up in a printed copy or to anyone other than the calendar owner or a delegate
 - caution – ensure that only personal appointments are labeled as "private". Calendar records must be accurate and are subject to a formal access request under FOIPPA
 - consider deleting "private" or personal appointments immediately after they occur

SEVERING GUIDELINES - CALENDAR ENTRIES

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

OPEN INFORMATION

- Introduced July 2011 with policy guidelines
- 2,300 General FOI requests posted (no Personals)
- Over 1,000 Minister and Deputy Minister travel expense summaries posted
- Over 52,000 visits to and 38,000 downloads from the Open Information website
- Proactively released 53 per cent of eligible general requests
- Requests are exempt from publication due to security concerns (72 per cent), personal information (14 per cent), and business information (12 per cent)



Contact Information

Brad Williams, a/Executive Director, FOI

250 356-7343

FOI Managers:

Sector

Manager

Justice/Social

Vicki Hudson

250 356-0845

Central Agencies

Cindy Elbahir

250 952-6355

Natural Resources

Kris Ghag

250 356-5702

Business/Infrastructure

Russ Fuller

250 387-4503

Health/Education

Maxine Vanzetta

250 387-9805

Personals

Vivian McDonald

250 356-6266

Intake

Cindy Kukucska

250 387-7356

Open Information

Chad Hoskins

250 387-2044



Logistics and Business Services

FREEDOM OF INFORMATION

Presented February 2015

FREEDOM OF INFORMATION

1. What you need to know about the FOI Act
2. Records Management
3. FOI
4. How the FOI process works
5. Trends in FOI
6. Calendars
7. Open Information
8. FOI Contacts

PURPOSES OF THE ACT

Accountability to the Public

- Legislated right to access all government records - specifying limited exceptions (i.e. make what is commonly referred to as an 'FOI request')

Protection of Privacy

- Provides a right of access to individuals own personal information
- Regulates how public bodies collect, use and disclose personal information
- Right to request correction of personal information

Independent Oversight by the Office of the Information & Privacy Commissioner

- Conducts reviews on decisions regarding disclosure

Purposes of the Act

ACCOUNTABILITY

RIGHT OF ACCESS TO
RECORDS



PRIVACY

PREVENT UNAUTHORIZED
COLLECTION, USE OR
DISCLOSURE OF PERSONAL
INFORMATION

INDEPENDENT OVERSIGHT

WHO IS COVERED BY THE ACT

All provincial ministries, and most provincial agencies, boards, commissions, Crown corporations and smaller agencies

Local public bodies

- School Districts
- Colleges and universities
- Regional health boards

Self-governing professions and occupations

- Teachers
 - Doctors
 - Nurses
- Government is only responsible for requests to BC government ministries

WHAT RECORDS ARE COVERED BY THE ACT

All records in the **custody** or under the **control** of a public body

What is a Record?

- Any information recorded or stored by any means whether in hard copy or in electronic format
- Regardless of content and subject matter, the following are subject to an FOI request:
 - briefing notes
 - vouchers
 - telephone records
 - notebooks/daybooks
 - contractor records
 - email
 - records on your smart phone
 - transitory records

TRANSITORY RECORDS

- Are records of temporary usefulness not required to document decisions and actions or to support ongoing government business
- Should be regularly deleted as their usefulness ends (e.g.: transitory emails of no further use can be deleted)
- The Transitory Records Schedule does not apply to personal or MLA records

RECORDS MANAGEMENT

- Records created or received while doing Government business must be managed according to legislation, litigation requirements and Government policy and are subject to FOI and Government policy regardless of where they are located.
- Government email must be conducted using approved Government email systems, not personal email systems. This is essential for information security, privacy protection and effective management of the information
- Government records that are not transitory should be filed in the office's record-keeping system (e.g., TRIM or LAN) and must not be destroyed without an approved schedule (e.g., ARCS/ORCS) or before the schedule allows
- Employees must keep Government records separate from material relating to ministers' constituency matters, legislative committee involvement and other MLA activities. Those, and personal (e.g., family) records, are not Government records

RESPONSES WITH RECORDS AND NO RECORDS

Fiscal Year	Number of Closed Requests	On-Time Requests	Percentage of No Records Responses
2009/10	7,750	6,984	21%
2010/11	7,939	7,145	24%
2011/12	8,212	7,392	21%
2012/13	9,524	8,325	25%
2013/14	9,827	7,272	19%

CROSS GOVERNMENT REQUEST – TIMELINES

30 DAYS!



Unless.....

The request necessitates a 30 Day Extension under the Act

WHAT HAPPENS WHEN AN FOI REQUEST IS RECEIVED?

- Standard Call for Records Forms and Guidelines for record submissions are provided to all ministry program areas
- Ministry responsibilities include provision of the following information to IAO:
 - where search for records was conducted (i.e. TRIM files, databases, off-site records)
 - duration of search time by ministry program area
 - who conducted the record search
 - potential HARMS that could result from disclosure of records gathered
 - ISSUES associated with disclosure of records gathered
 - regional locations where records pertaining to this request may reside

How the FOI Process Works

Mandatory Exceptions	
Section 12	Cabinet confidence
Section 21	Third party business information
Section 22	Personal information
Discretionary Exceptions	
Section 13	Policy advice/recommendations
Section 14	Legal advice
Section 15	Law enforcement
Section 16	Intergovernmental relations
Section 17	Financial or economic interests
Section 18	Heritage sites
Section 19	Personal health or safety
Section 20	Information soon to be published

FOI APPROVAL PROCESS

- FOI requests are sent to program areas (ministries) for review and sign-off
- The DM or delegated head of the public body is responsible for final sign-off on all requests
- The DM or delegated head of the public body exercises discretion with respect to disclosure recommendations

FOI FAST FACTS

Timeliness was down in 2013/14, but government is still responding to more requests **on-time** than it did prior to centralization in 2009.

Political party
requests
increased by
64% in 2013/14.

2013/14 was the
first year in which
government
received more
general than
personal requests.

Government received close
to **10,000** FOI requests in
2013/14, a 25% increase
over 2009/10.

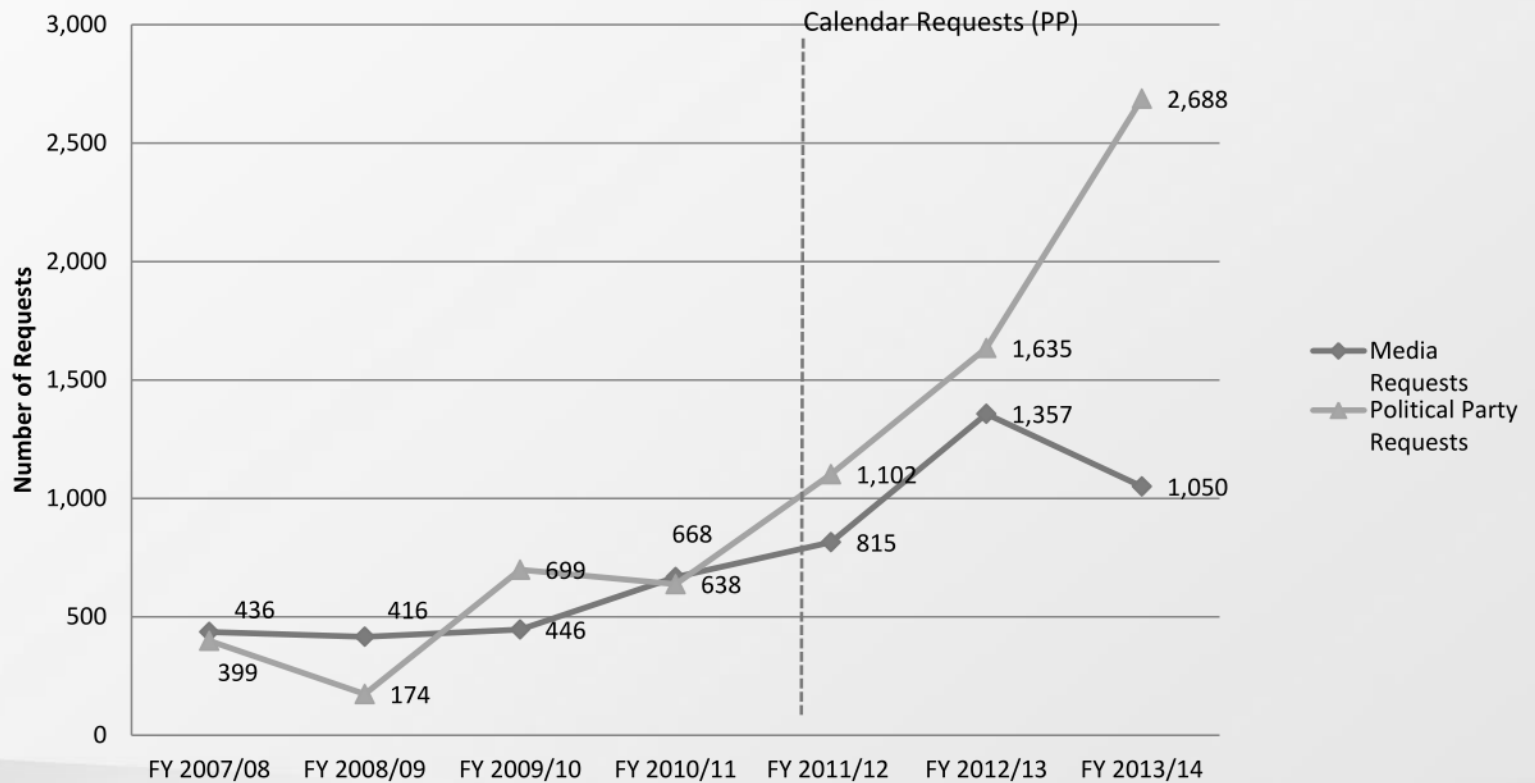
Government received
1,800 requests for the
calendars of senior
government
officials/employees.

DEMAND FOR FOI REQUESTS CONTINUES TO INCREASE

Fiscal Year	General Requests	Personal Requests	Total Requests Received	% On-Time
2007/08	1,805	3,589	5,394	71
2008/09	1,693	4,877	6,570	74
2009/10	2,532	5,122	7,654	90
2010/11	2,756	5,073	7,829	93
2011/12	3,329	5,094	8,423	90
2012/13	4,815	5,484	10,299	87
2013/14	5,200	4,400	9,600	74

CHANGING NATURE OF FOI APPLICANTS

Requests from Political Parties and Media



CALENDAR MANAGEMENT

- Government generally receives monthly or bi-monthly requests for DM, ADM and ED calendars and about 25 positions in the Office of the Premier. In November 2013, calendars for Ministers' Office Executive Assistants were included.

OUTLOOK CALENDARS

- Be wary of embedded documents, as the calendar and the attachments have different life spans
- Ensure calendar consistency and clarity
 - be clear about the subject of the meeting and who is expected to attend
 - keep the meeting subject concise
- Keep calendars current
 - update the calendar as changes occur
 - delete meetings that did not occur or were not attended
 - update the calendar to record the names and titles of individual(s) who actually attended the meeting as the calendar owner's representative
- Personal appointments
 - mark as "private" – details will not show up in a printed copy or to anyone other than the calendar owner or a delegate
 - caution – ensure that only personal appointments are labeled as "private". Calendar records must be accurate and are subject to a formal access request under FOIPPA
 - consider deleting "private" or personal appointments immediately after they occur

SEVERING GUIDELINES - CALENDAR ENTRIES

Entry or Description of Entry	Severed or Not Severed
Blackberry/cell phone numbers for government employees	Severed under section 17 (unless public)
"Cabinet" or "Cabinet Retreat"	Not Severed
"Treasury Board"	Not Severed
Accommodation details	Severed under section 15
Meeting location details	Severed under section 15
Constituency related – any entries in the Minister's calendar that relate to his/her duties as a Member of the Legislative Assembly (MLA)	Out of Scope - under section 3 - As the office of a Member of the Legislative Assembly is not a public body, any entries in a Minister's calendar that relate to his/her duties as an MLA will be severed as outside the scope of FOIPPA
360's (executive performance review), mentoring, EPDP	Severed under section 22

OPEN INFORMATION

- Introduced July 2011 with policy guidelines
- Over 4,000 General FOI requests posted (no Personals)
- Over 1,500 Minister and Deputy Minister travel expense summaries posted
- Over 21,000 visits to and 15,000 downloads from the Open Information website in 2013/14
- Proactively released 48 per cent of eligible general requests in 2013/14
- Requests are exempt from publication due to security concerns (82 per cent), business information (10 per cent), and personal information (7 per cent)

Contact Information

Brad Williams, Executive Director, IAO

250 387-9807

FOI Managers:

Sector

Manager

Justice/SocialVicki Hudson

250 356-0845

Central AgenciesCindy Elbahir

250 952-6355

Natural ResourcesKris Ghag

250 356-5702

Business/InfrastructureRuss Fuller

250 387-4503

Health/EducationMaxine Vanzetta

250 387-9805

PersonalsVivian McDonald

250 356-6266

IntakeCindy Kukucska

250 387-7356

Open InformationCindy Kukucska

250 387-7356



Logistics and Business Services

FREEDOM OF INFORMATION

Presented January 2014

FREEDOM OF INFORMATION

1. What you need to know about the FOI Act
2. Records Management
3. FOI
4. How the FOI process works
5. Trends in FOI
6. Calendars
7. Open Information
8. FOI Contacts

PURPOSES OF THE ACT

Accountability to the Public

- Legislated right to access all government records - specifying limited exceptions (i.e. make what is commonly referred to as an 'FOI request')

Protection of Privacy

- Provides a right of access to individuals own personal information
- Regulates how public bodies collect, use and disclose personal information
- Right to request correction of personal information

Independent Oversight by the Office of the Information & Privacy Commissioner

- Conducts reviews on decisions regarding disclosure

Purposes of the Act

ACCOUNTABILITY

RIGHT OF ACCESS TO
RECORDS



PRIVACY

PREVENT UNAUTHORIZED
COLLECTION, USE OR
DISCLOSURE OF PERSONAL
INFORMATION

INDEPENDENT OVERSIGHT

WHO IS COVERED BY THE ACT

All provincial ministries, and most provincial agencies, boards, commissions, Crown corporations and smaller agencies

Local public bodies

- School Districts
- Colleges and universities
- Regional health boards

Self-governing professions and occupations

- Teachers
 - Doctors
 - Nurses
- Government is only responsible for requests to BC government ministries

WHAT RECORDS ARE COVERED BY THE ACT

All records in the **custody** or under the **control** of a public body

What is a Record?

- Any information recorded or stored by any means whether in hard copy or in electronic format
- Regardless of content and subject matter, the following are subject to an FOI request:
 - briefing notes
 - vouchers
 - telephone records
 - notebooks/daybooks
 - contractor records
 - email
 - records on your smart phone
 - transitory records

TRANSITORY RECORDS

- Are records of temporary usefulness not required to document decisions and actions or to support ongoing government business
- Should be regularly deleted as their usefulness ends (e.g.: transitory emails of no further use can be deleted)
- The Transitory Records Schedule does not apply to personal or MLA records

RECORDS MANAGEMENT

- Records created or received while doing Government business must be managed according to legislation, litigation requirements and Government policy and are subject to FOI and Government policy regardless of where they are located.
- Government email must be conducted using approved Government email systems, not personal email systems. This is essential for information security, privacy protection and effective management of the information.
- Government records that are not transitory should be filed in the office's record-keeping system (e.g., TRIM or LAN) and must not be destroyed without an approved schedule (e.g., ARCS/ORCS) or before the schedule allows.
- Employees must keep Government records separate from material relating to ministers' constituency matters, legislative committee involvement and other MLA activities. Those, and personal (e.g., family) records, are not Government records.

RESPONSES WITH RECORDS AND NO RECORDS

Fiscal Year	Number of Closed Requests	On-Time Requests	Percentage of No Records Responses
2009/10	7,750	6,984	21%
2010/11	7,939	7,145	24%
2011/12	8,212	7,392	21%
2012/13	9,524	8,325	25%

CROSS GOVERNMENT REQUEST – TIMELINES

30 DAYS!



Unless.....

The request necessitates a 30 Day Extension under the Act

WHAT HAPPENS WHEN AN FOI REQUEST IS RECEIVED?

- Standard Call for Records Forms and Guidelines for record submissions are provided to all ministry program areas
- Ministry responsibilities include provision of the following information to IAO:
 - where search for records was conducted (i.e. TRIM files, databases, off-site records)
 - duration of search time by ministry program area
 - who conducted the record search
 - potential HARMS that could result from disclosure of records gathered
 - ISSUES associated with disclosure of records gathered
 - regional locations where records pertaining to this request may reside

How the FOI Process Works

Mandatory Exceptions	
Section 12	Cabinet confidence
Section 21	Third party business information
Section 22	Personal information
Discretionary Exceptions	
Section 13	Policy advice/recommendations
Section 14	Legal advice
Section 15	Law enforcement
Section 16	Intergovernmental relations
Section 17	Financial or economic interests
Section 18	Heritage sites
Section 19	Personal health or safety
Section 20	Information soon to be published

FOI APPROVAL PROCESS

- FOI requests are sent to program areas (ministries) for review and sign-off
- The DM or delegated head of the public body is responsible for final sign-off on all requests
- The DM or delegated head of the public body exercises discretion with respect to disclosure recommendations

FOI FAST FACTS

Government has maintained an on-time rate of **87%** despite a 57% increase in volume since 2008/09

In fiscal 2012/13, media requests were up by **68%** and political party requests were up by **48%**

For the first time, government is receiving almost as many **general** requests as **personal** requests

Government received over **10,000** FOI requests in 2012/13, a 22% increase over last fiscal

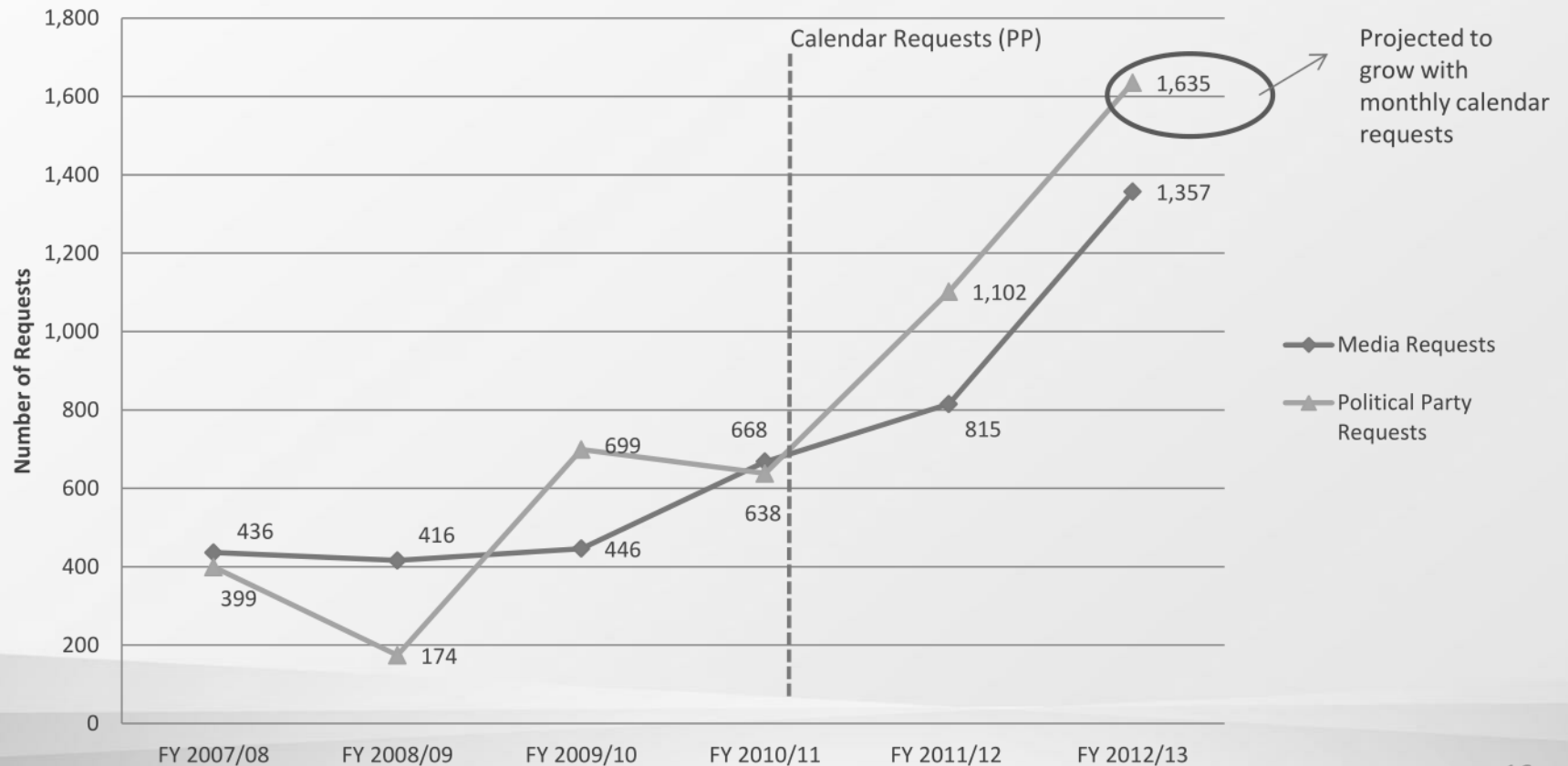
One media applicant made over **700 FOI requests** in 2012/13, and over 1,000 in the past 2 years

DEMAND FOR FOI REQUESTS CONTINUES TO INCREASE

Fiscal Year	General Requests	Personal Requests	Total Requests Received	% On-Time
2007/08	1,805	3,589	5,394	71
2008/09	1,693	4,877	6,570	74
2009/10	2,532	5,122	7,654	90
2010/11	2,756	5,073	7,829	93
2011/12	3,329	5,094	8,423	90
2012/13	4,815	5,484	10,299	87
2013/14 (projected)	4,000	5,500	9,500	75

CHANGING NATURE OF FOI APPLICANTS

Requests from Political Parties and Media



CALENDAR MANAGEMENT

- Government generally receives monthly or bi-monthly requests for DM, ADM and ED calendars and about 25 positions in the Office of the Premier. In November 2013, calendars for Ministers' Office Executive Assistants were included.

OUTLOOK CALENDARS

- Be wary of embedded documents, as the calendar and the attachments have different life spans
- Ensure calendar consistency and clarity
 - be clear about the subject of the meeting and who is expected to attend
 - keep the meeting subject concise
- Keep calendars current
 - update the calendar as changes occur
 - delete meetings that did not occur or were not attended
 - update the calendar to record the names and titles of individual(s) who actually attended the meeting as the calendar owner's representative
- Personal appointments
 - mark as "private" – details will not show up in a printed copy or to anyone other than the calendar owner or a delegate
 - caution – ensure that only personal appointments are labeled as "private". Calendar records must be accurate and are subject to a formal access request under FOIPPA
 - consider deleting "private" or personal appointments immediately after they occur

SEVERING GUIDELINES - CALENDAR ENTRIES

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

OPEN INFORMATION

- Introduced July 2011 with policy guidelines
- 2,300 General FOI requests posted (no Personals)
- Over 1,000 Minister and Deputy Minister travel expense summaries posted
- Over 52,000 visits to and 38,000 downloads from the Open Information website
- Proactively released 53 per cent of eligible general requests
- Requests are exempt from publication due to security concerns (72 per cent), personal information (14 per cent), and business information (12 per cent)

Contact Information

Kathleen Ward, Executive Director, IAO

250 387-9807

Brad Williams, Director, FOI

250 356-7343

FOI Managers:

Sector

Manager

Justice/Social

Vicki Hudson

250 356-0845

Central Agencies

Cindy Elbahir

250 952-6355

Natural Resources

Kris Ghag

250 356-5702

Business/Infrastructure

Russ Fuller

250 387-4503

Health/Education

Maxine Vanzetta

250 387-9805

Personals

Vivian McDonald

250 356-6266

Intake

Cindy Kukucska

250 387-7356

Open Information

Chad Hoskins

250 387-2044



Logistics and Business Services

FREEDOM OF INFORMATION

Presented October 2014

FREEDOM OF INFORMATION

1. What you need to know about the FOI Act
2. Records Management
3. FOI
4. How the FOI process works
5. Trends in FOI
6. Calendars
7. Open Information
8. FOI Contacts

PURPOSES OF THE ACT

Accountability to the Public

- Legislated right to access all government records - specifying limited exceptions (i.e. make what is commonly referred to as an 'FOI request')

Protection of Privacy

- Provides a right of access to individuals own personal information
- Regulates how public bodies collect, use and disclose personal information
- Right to request correction of personal information

Independent Oversight by the Office of the Information & Privacy Commissioner

- Conducts reviews on decisions regarding disclosure

Purposes of the Act

ACCOUNTABILITY

RIGHT OF ACCESS TO
RECORDS



PRIVACY

PREVENT UNAUTHORIZED
COLLECTION, USE OR
DISCLOSURE OF PERSONAL
INFORMATION

INDEPENDENT OVERSIGHT

WHO IS COVERED BY THE ACT

All provincial ministries, and most provincial agencies, boards, commissions, Crown corporations and smaller agencies

Local public bodies

- School Districts
- Colleges and universities
- Regional health boards

Self-governing professions and occupations

- Teachers
 - Doctors
 - Nurses
- Government is only responsible for requests to BC government ministries

WHAT RECORDS ARE COVERED BY THE ACT

All records in the **custody** or under the **control** of a public body

What is a Record?

- Any information recorded or stored by any means whether in hard copy or in electronic format
- Regardless of content and subject matter, the following are subject to an FOI request:
 - briefing notes
 - vouchers
 - telephone records
 - notebooks/daybooks
 - contractor records
 - email
 - records on your smart phone
 - transitory records

TRANSITORY RECORDS

- Are records of temporary usefulness not required to document decisions and actions or to support ongoing government business
- Should be regularly deleted as their usefulness ends (e.g.: transitory emails of no further use can be deleted)
- The Transitory Records Schedule does not apply to personal or MLA records

RECORDS MANAGEMENT

- Records created or received while doing Government business must be managed according to legislation, litigation requirements and Government policy and are subject to FOI and Government policy regardless of where they are located.
- Government email must be conducted using approved Government email systems, not personal email systems. This is essential for information security, privacy protection and effective management of the information
- Government records that are not transitory should be filed in the office's record-keeping system (e.g., TRIM or LAN) and must not be destroyed without an approved schedule (e.g., ARCS/ORCS) or before the schedule allows
- Employees must keep Government records separate from material relating to ministers' constituency matters, legislative committee involvement and other MLA activities. Those, and personal (e.g., family) records, are not Government records

RESPONSES WITH RECORDS AND NO RECORDS

Fiscal Year	Number of Closed Requests	On-Time Requests	Percentage of No Records Responses
2009/10	7,750	6,984	21%
2010/11	7,939	7,145	24%
2011/12	8,212	7,392	21%
2012/13	9,524	8,325	25%

CROSS GOVERNMENT REQUEST – TIMELINES

30 DAYS!



Unless.....

The request necessitates a 30 Day Extension under the Act

WHAT HAPPENS WHEN AN FOI REQUEST IS RECEIVED?

- Standard Call for Records Forms and Guidelines for record submissions are provided to all ministry program areas
- Ministry responsibilities include provision of the following information to IAO:
 - where search for records was conducted (i.e. TRIM files, databases, off-site records)
 - duration of search time by ministry program area
 - who conducted the record search
 - potential HARMS that could result from disclosure of records gathered
 - ISSUES associated with disclosure of records gathered
 - regional locations where records pertaining to this request may reside

How the FOI Process Works

Mandatory Exceptions	
Section 12	Cabinet confidence
Section 21	Third party business information
Section 22	Personal information
Discretionary Exceptions	
Section 13	Policy advice/recommendations
Section 14	Legal advice
Section 15	Law enforcement
Section 16	Intergovernmental relations
Section 17	Financial or economic interests
Section 18	Heritage sites
Section 19	Personal health or safety
Section 20	Information soon to be published

FOI APPROVAL PROCESS

- FOI requests are sent to program areas (ministries) for review and sign-off
- The DM or delegated head of the public body is responsible for final sign-off on all requests
- The DM or delegated head of the public body exercises discretion with respect to disclosure recommendations

FOI FAST FACTS

Government has maintained an on-time rate of **87%** despite a 57% increase in volume since 2008/09

In fiscal 2012/13, media requests were up by **68%** and political party requests were up by **48%**

For the first time, government is receiving almost as many **general** requests as **personal** requests

Government received over **10,000** FOI requests in 2012/13, a 22% increase over last fiscal

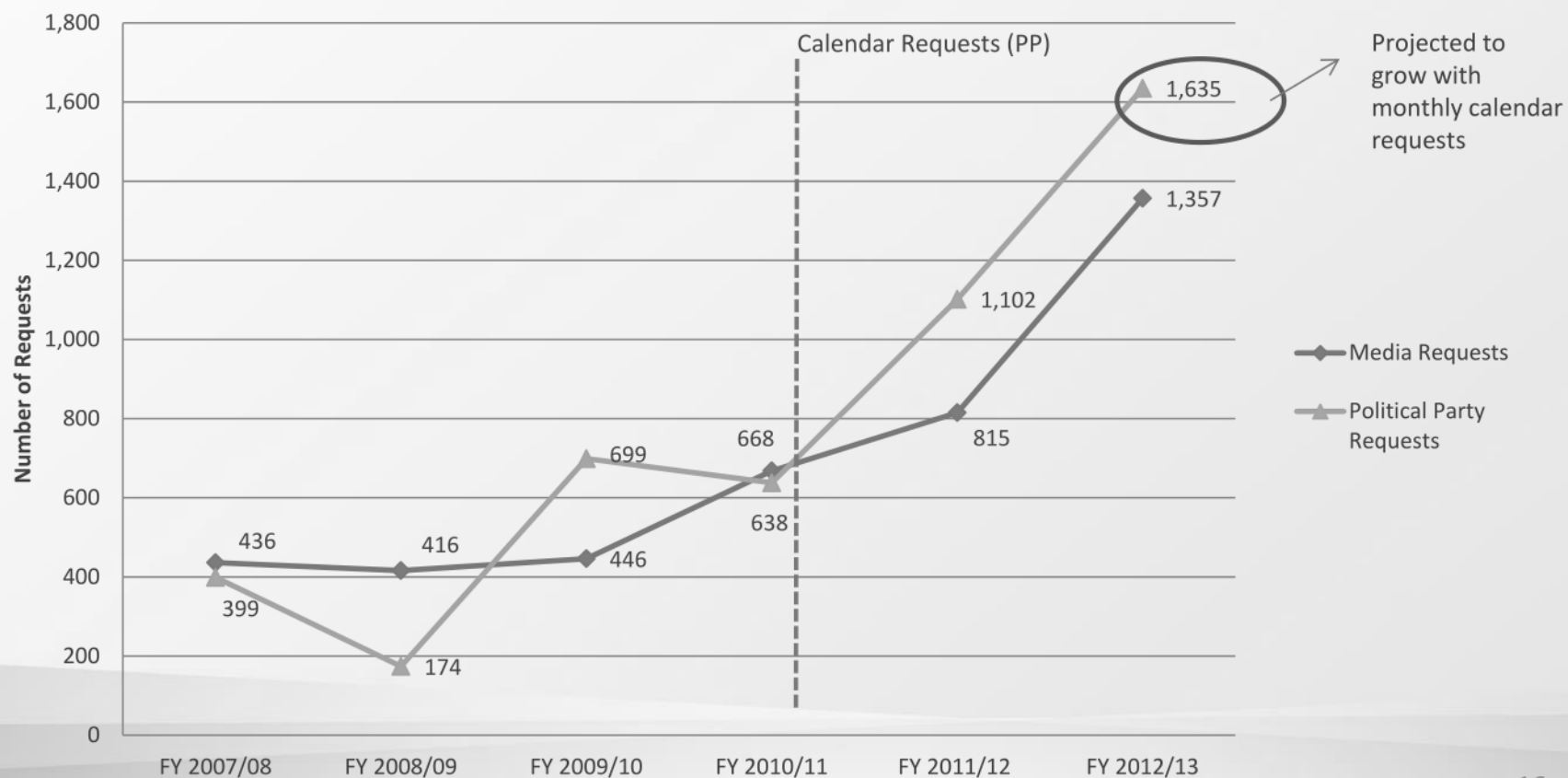
One media applicant made over **700 FOI requests** in 2012/13, and over 1,000 in the past 2 years

DEMAND FOR FOI REQUESTS CONTINUES TO INCREASE

Fiscal Year	General Requests	Personal Requests	Total Requests Received	% On-Time
2007/08	1,805	3,589	5,394	71
2008/09	1,693	4,877	6,570	74
2009/10	2,532	5,122	7,654	90
2010/11	2,756	5,073	7,829	93
2011/12	3,329	5,094	8,423	90
2012/13	4,815	5,484	10,299	87
2013/14 (projected)	4,000	5,500	9,500	75

CHANGING NATURE OF FOI APPLICANTS

Requests from Political Parties and Media



CALENDAR MANAGEMENT

- Government generally receives monthly or bi-monthly requests for DM, ADM and ED calendars and about 25 positions in the Office of the Premier. In November 2013, calendars for Ministers' Office Executive Assistants were included.

OUTLOOK CALENDARS

- Be wary of embedded documents, as the calendar and the attachments have different life spans
- Ensure calendar consistency and clarity
 - be clear about the subject of the meeting and who is expected to attend
 - keep the meeting subject concise
- Keep calendars current
 - update the calendar as changes occur
 - delete meetings that did not occur or were not attended
 - update the calendar to record the names and titles of individual(s) who actually attended the meeting as the calendar owner's representative
- Personal appointments
 - mark as "private" – details will not show up in a printed copy or to anyone other than the calendar owner or a delegate
 - caution – ensure that only personal appointments are labeled as "private". Calendar records must be accurate and are subject to a formal access request under FOIPPA
 - consider deleting "private" or personal appointments immediately after they occur

SEVERING GUIDELINES - CALENDAR ENTRIES

Entry or Description of Entry	Severed or Not Severed
Blackberry/cell phone numbers for government employees	Severed under section 17 (unless public)
"Cabinet" or "Cabinet Retreat"	Not Severed
"Treasury Board"	Not Severed
Accommodation details	Severed under section 15
Meeting location details	Severed under section 15
Constituency related – any entries in the Minister's calendar that relate to his/her duties as a Member of the Legislative Assembly (MLA)	Out of Scope - under section 3 - As the office of a Member of the Legislative Assembly is not a public body, any entries in a Minister's calendar that relate to his/her duties as an MLA will be severed as outside the scope of FOIPPA
360's (executive performance review), mentoring, EPDP	Severed under section 22

OPEN INFORMATION

- Introduced July 2011 with policy guidelines
- 2,300 General FOI requests posted (no Personals)
- Over 1,000 Minister and Deputy Minister travel expense summaries posted
- Over 52,000 visits to and 38,000 downloads from the Open Information website
- Proactively released 53 per cent of eligible general requests
- Requests are exempt from publication due to security concerns (72 per cent), personal information (14 per cent), and business information (12 per cent)

Contact Information

Brad Williams, a/Executive Director, FOI

250 356-7343

FOI Managers:

Sector

Manager

Justice/Social

Vicki Hudson

250 356-0845

Central Agencies

Cindy Elbahir

250 952-6355

Natural Resources

Kris Ghag

250 356-5702

Business/Infrastructure

Russ Fuller

250 387-4503

Health/Education

Maxine Vanzetta

250 387-9805

Personals

Vivian McDonald

250 356-6266

Intake

Cindy Kukucska

250 387-7356

Open Information

Chad Hoskins

250 387-2044

Logistics and Business Services

FREEDOM OF INFORMATION

Presented October 2015



FREEDOM OF INFORMATION

1. What you need to know about the FOI Act
2. Records Management
3. FOI
4. How the FOI process works
5. Trends in FOI
6. Calendars
7. Open Information
8. FOI Contacts



PURPOSES OF THE ACT

Accountability to the Public

- Legislated right to access all government records - specifying limited exceptions (i.e. make what is commonly referred to as an 'FOI request')

Protection of Privacy

- Provides a right of access to individuals own personal information
- Regulates how public bodies collect, use and disclose personal information
- Right to request correction of personal information

Independent Oversight by the Office of the Information & Privacy Commissioner

- Conducts reviews on decisions regarding disclosure

Purposes of the Act

ACCOUNTABILITY
RIGHT OF ACCESS
TO RECORDS



PRIVACY
PREVENT UNAUTHORIZED
COLLECTION, USE OR
DISCLOSURE OF
PERSONAL INFORMATION

INDEPENDENT OVERSIGHT



WHO IS COVERED BY THE ACT

All provincial ministries, and most provincial agencies, boards, commissions, Crown corporations and smaller agencies

Local public bodies

- School Districts
- Colleges and universities
- Regional health boards

Self-governing professions and occupations

- Teachers
- Doctors
- Nurses

➤ Government is only responsible for requests to BC government ministries



WHAT RECORDS ARE COVERED BY THE ACT

All records in the **custody** or under the **control** of a public body

What is a Record?

- Any information recorded or stored by any means whether in hard copy or in electronic format
- Regardless of content and subject matter, the following are subject to an FOI request:
 - briefing notes
 - vouchers
 - telephone records
 - notebooks/daybooks
 - contractor records
 - email
 - records on your smart phone
 - transitory records



TRANSITORY RECORDS

- Are records of temporary usefulness not required to document decisions and actions or to support ongoing government business
- Should be regularly deleted as their usefulness ends (e.g.: transitory emails of no further use can be deleted)
- The Transitory Records Schedule does not apply to personal or MLA records



RECORDS MANAGEMENT

- Records created or received while doing Government business must be managed according to legislation, litigation requirements and Government policy and are subject to FOI and Government policy regardless of where they are located.
- Government email must be conducted using approved Government email systems, not personal email systems. This is essential for information security, privacy protection and effective management of the information
- Government records that are not transitory should be filed in the office's record-keeping system (e.g., TRIM or LAN) and must not be destroyed without an approved schedule (e.g., ARCS/ORCS) or before the schedule allows
- Employees must keep Government records separate from material relating to ministers' constituency matters, legislative committee involvement and other MLA activities. Those, and personal (e.g., family) records, are not Government records

RESPONSES WITH RECORDS AND NO RECORDS

Fiscal Year	Number of Closed Requests	On-Time Requests	Percentage of No Records Responses
2009/10	7,750	6,984	21%
2010/11	7,939	7,145	24%
2011/12	8,212	7,392	21%
2012/13	9,524	8,325	25%
2013/14	9,827	7,272	19%
2014/15	8,377	6,588	17%



CROSS GOVERNMENT REQUEST – TIMELINES

30 DAYS!



Unless.....

The request necessitates a 30 Day Extension under the Act



WHAT HAPPENS WHEN AN FOI REQUEST IS RECEIVED?

- Standard Call for Records Forms and Guidelines for record submissions are provided to all ministry program areas
- Ministry responsibilities include provision of the following information to IAO:
 - where search for records was conducted (i.e. TRIM files, databases, off-site records)
 - duration of search time by ministry program area
 - who conducted the record search
 - potential HARMS that could result from disclosure of records gathered
 - ISSUES associated with disclosure of records gathered
 - regional locations where records pertaining to this request may reside

Mandatory Exceptions

Section 12	Cabinet confidence
Section 21	Third party business information
Section 22	Personal information

Discretionary Exceptions

Section 13	Policy advice/recommendations
Section 14	Legal advice
Section 15	Law enforcement
Section 16	Intergovernmental relations
Section 17	Financial or economic interests
Section 18	Heritage sites
Section 19	Personal health or safety
Section 20	Information soon to be published



FOI APPROVAL PROCESS

- FOI requests are sent to program areas (ministries) for review and sign-off
- The DM or delegated head of the public body is responsible for final sign-off on all requests
- The DM or delegated head of the public body exercises discretion with respect to disclosure recommendations

FOI FAST FACTS

Timeliness was down in 2013/14, but government is still responding to more requests **on-time** than it did prior to centralization in 2009.

Political party
requests
increased by
64% in
2013/14.

2013/14 was the
first year in which
government
received more
general than
personal requests.

Government received
close to **10,000** FOI
requests in 2013/14, a
25% increase over
2009/10.

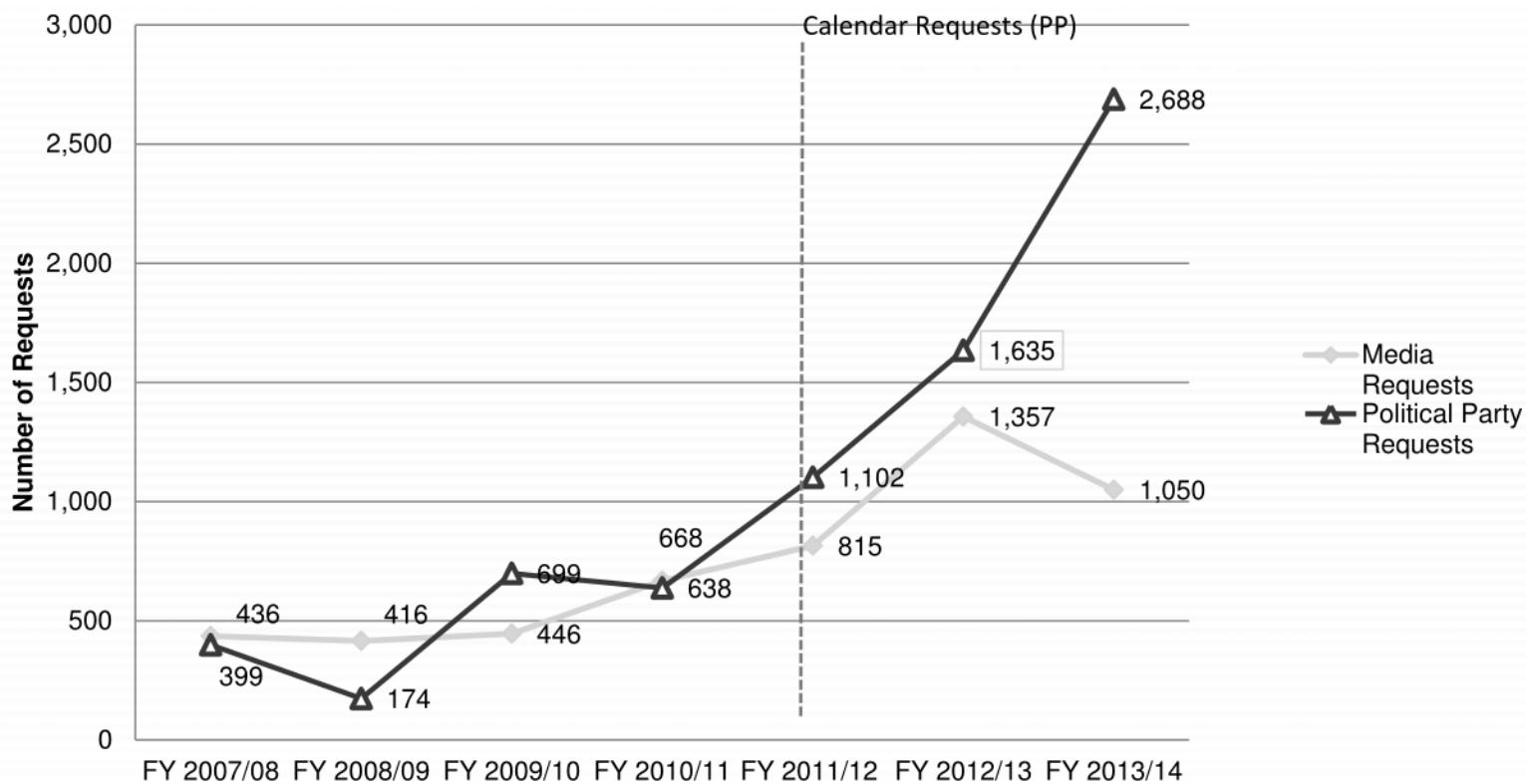
Government received
1,800 requests for the
calendars of senior
government
officials/employees.

DEMAND FOR FOI REQUESTS CONTINUES TO INCREASE

Fiscal Year	General Requests	Personal Requests	Total Requests Received	% On-Time
2008/09	1,693	4,877	6,570	74
2009/10	2,532	5,122	7,654	90
2010/11	2,756	5,073	7,829	93
2011/12	3,329	5,094	8,423	90
2012/13	4,815	5,484	10,299	87
2013/14	5,200	4,400	9,600	74
2014/15	4,124	4,151	8,275	79

CHANGING NATURE OF FOI APPLICANTS

Requests from Political Parties and Media





CALENDAR MANAGEMENT

- Government generally receives monthly or bi-monthly requests for DM, ADM and ED calendars and about 25 positions in the Office of the Premier. In November 2013, calendars for Ministers' Office Executive Assistants were included.

OUTLOOK CALENDARS

- Be wary of embedded documents, as the calendar and the attachments have different life spans
- Ensure calendar consistency and clarity
 - be clear about the subject of the meeting and who is expected to attend
 - keep the meeting subject concise
- Keep calendars current
 - update the calendar as changes occur
 - delete meetings that did not occur or were not attended
 - update the calendar to record the names and titles of individual(s) who actually attended the meeting as the calendar owner's representative
- Personal appointments
 - mark as "private" – details will not show up in a printed copy or to anyone other than the calendar owner or a delegate
 - caution – ensure that only personal appointments are labeled as "private". Calendar records must be accurate and are subject to a formal access request under FOIPPA
 - consider deleting "private" or personal appointments immediately after they occur



SEVERING GUIDELINES - CALENDAR ENTRIES

Entry or Description of Entry	Severed or Not Severed
Blackberry/cell phone numbers for government employees	Severed under section 17 (unless public)
"Cabinet" or "Cabinet Retreat"	Not Severed
"Treasury Board"	Not Severed
Accommodation details	Severed under section 15
Meeting location details	Severed under section 15
Constituency related – any entries in the Minister's calendar that relate to his/her duties as a Member of the Legislative Assembly (MLA)	Out of Scope - under section 3 - As the office of a Member of the Legislative Assembly is not a public body, any entries in a Minister's calendar that relate to his/her duties as an MLA will be severed as outside the scope of FOIPPA
360's (executive performance review), mentoring, EPDP	Severed under section 22



OPEN INFORMATION

- Introduced July 2011 with policy guidelines
- Over 5,000 General FOI requests posted (no Personals)
- Over 1,700 Minister and Deputy Minister travel expense summaries posted
- Over 21,000 visits to and 15,000 downloads from the Open Information website in 2013/14
- Proactively released 48 per cent of eligible general requests in 2013/14
- Requests are exempt from publication due to security concerns (82 per cent), business information (10 per cent), and personal information (7 per cent)



Contact Information

Brad Williams, Executive Director, FOI

250 357-9807

Chad Hoskins, Senior Director, FOI

250 356-7343

FOI Managers:

Sector

Manager

Justice/Social

Kris Ghag

250 387-9801

Central Agencies

Cindy Elbahir

250 952-6355

Natural Resources

Ken Bejcek

250 387-0572

Business/Infrastructure

Russ Fuller

250 387-4503

Health/Education

Maxine Vanzetta

250 387-9805

Personals

Vivian McDonald

250 356-6266

Intake/Open Information

Cindy Kukucska

250 387-7356



Shared
ServicesBC

Logistics and Business Services

FREEDOM OF INFORMATION

Presented July 2013

FREEDOM OF INFORMATION

1. What you need to know about the FOI Act
2. How the FOI process works
3. Trends in FOI
4. Calendars
5. Open Information
6. FOI Contacts

PURPOSES OF THE ACT

Accountability to the Public

- Legislated right to access all government records - specifying limited exceptions (i.e. make what is commonly referred to as an 'FOI request')

Protection of Privacy

- Provides a right of access to individuals own personal information
- Regulates how public bodies collect, use and disclose personal information
- Right to request correction of personal information

Body's decision(s) made under FOIPPA

- The independent reviews extend beyond decisions regarding disclosure

Purposes of the Act

ACCOUNTABILITY

RIGHT OF ACCESS TO
RECORDS



PRIVACY

PREVENT UNAUTHORIZED
COLLECTION, USE OR
DISCLOSURE OF PERSONAL
INFORMATION

INDEPENDENT OVERSIGHT

WHO IS COVERED BY THE ACT

All provincial ministries, and most provincial agencies, boards, commissions, Crown corporations and smaller agencies

Local public bodies

- School Districts
- Colleges and universities
- Regional health boards

Self-governing professions and occupations

- Teachers
- Doctors
- Nurses

➤ Government is only responsible for requests to BC government ministries

WHAT RECORDS ARE COVERED BY THE ACT

All records in the **custody** or under the **control** of a public body

What is a Record?

- Any information recorded or stored by any means whether in hard copy or in electronic format
- Regardless of content and subject matter, the following are subject to an FOI request:
 - briefing notes
 - vouchers
 - telephone records
 - notebooks/daybooks
 - contractor records
 - email
 - records on your smart phone
 - transitory records

CROSS GOVERNMENT REQUEST – TIMELINES

30 DAYS!



Unless.....

The request necessitates a 30 Day Extension under the Act

WHAT HAPPENS WHEN AN FOI REQUEST IS RECEIVED?

- Standard Call for Records Forms and Guidelines for record submissions are provided to all ministry program areas
- Ministry responsibilities include provision of the following information to IAO:
 - where search for records was conducted (i.e. TRIM files, databases, off-site records)
 - duration of search time by ministry program area
 - who conducted the record search
 - potential HARMS that could result from disclosure of records gathered
 - ISSUES associated with disclosure of records gathered
 - regional locations where records pertaining to this request may reside

Mandatory Exceptions	
Section 12	Cabinet confidence
Section 21	Third party business information
Section 22	Personal information
Discretionary Exceptions	
Section 13	Policy advice/recommendations
Section 14	Legal advice
Section 15	Law enforcement
Section 16	Intergovernmental relations
Section 17	Financial or economic interests
Section 18	Heritage sites
Section 19	Personal health or safety
Section 20	Information soon to be published

FOI APPROVAL PROCESS

- FOI requests are sent to program areas (ministries) for review and sign-off
- The DM or delegated head of the public body is responsible for final sign-off on all requests
- The DM or delegated head of the public body exercises discretion with respect to disclosure recommendations

FOI FAST FACTS

Government has maintained an on-time rate of **87%** despite a 57% increase in volume since 2008/09

In fiscal 2012/13, media requests were up by **68%** and political party requests were up by **48%**

For the first time, government is receiving almost as many **general** requests as **personal** requests

Government received over **10,000** FOI requests in 2012/13, a 22% increase over last fiscal

One media applicant made over **700 FOI requests** in 2012/13, and over 1,000 in the past 2 years

DEMAND FOR FOI REQUESTS CONTINUES TO INCREASE

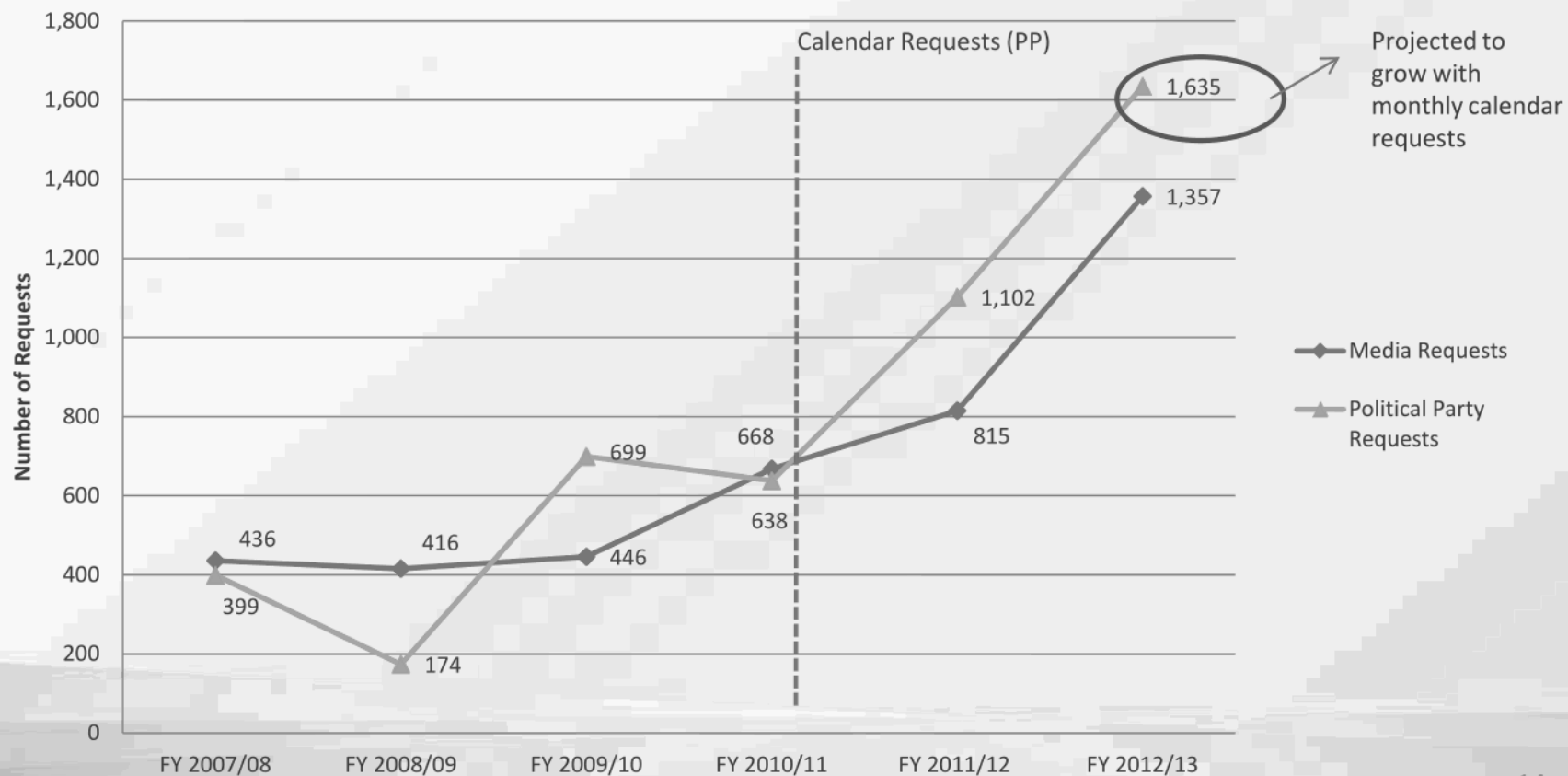
Fiscal Year	General Requests	Personal Requests	Total Requests Received	% On-Time
2007/08	1,805	3,589	5,394	71
2008/09	1,693	4,877	6,570	74
2009/10	2,532	5,122	7,654	90
2010/11	2,756	5,073	7,829	93
2011/12	3,329	5,094	8,423	90
2012/13	4,815	5,484	10,299	87
2013/14 (projected)	4,000	5,500	9,500	75

RESPONSES WITH RECORDS AND NO RECORDS

Fiscal Year	Number of Closed Requests	On-Time Requests	Percentage of No Records Responses
2009/10	7,750	6,984	21%
2010/11	7,939	7,145	24%
2011/12	8,212	7,392	21%
2012/13	9,524	8,325	25%

CHANGING NATURE OF FOI APPLICANTS

Requests from Political Parties and Media



CALENDAR MANAGEMENT

- Government generally receives monthly or bi-monthly requests for DM and ADM calendars. Last month, the requestor included ED calendars

OUTLOOK CALENDARS

- Be wary of embedded documents, as the calendar and the attachments have different life spans
- Ensure calendar consistency and clarity
 - be clear about the subject of the meeting and who is expected to attend
 - keep the meeting subject concise
- Keep calendars current
 - update the calendar as changes occur
 - delete meetings that did not occur or were not attended
 - update the calendar to record the names and titles of individual(s) who actually attended the meeting as the calendar owner's representative
- Personal appointments
 - mark as "private" – details will not show up in a printed copy or to anyone other than the calendar owner or a delegate
 - caution – ensure that only personal appointments are labeled as "private". Calendar records must be accurate and are subject to a formal access request under FOIPPA
 - consider deleting "private" or personal appointments immediately after they occur

SEVERING GUIDELINES - CALENDAR ENTRIES

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

OPEN INFORMATION

- Introduced July 2011 with policy guidelines
- 2,300 General FOI requests posted (no Personals)
- Over 1,000 Minister and Deputy Minister travel expense summaries posted
- Over 52,000 visits to and 38,000 downloads from the Open Information website
- Proactively released 53 per cent of eligible general requests
- Requests are exempt from publication due to security concerns (72 per cent), personal information (14 per cent), and business information (12 per cent)



Contact Information

Kathleen Ward, Executive Director, IAO

250 387-9807

Brad Williams, Director, FOI

250 356-7343

FOI Managers:

Sector

Manager

Justice/Social

Vicki Hudson

250 356-0845

Central Agencies

Cindy Elbahir

250 952-6355

Natural Resources

Kris Ghag

250 356-5702

Business/Infrastructure

Russ Fuller

250 387-4503

Health/Education

Maxine Vanzetta

250 356-7349

Personals

Vivian McDonald

250 356-6266

Intake

Cindy Kukucska

250 387-7356

Open Information

Chad Hoskins

250 387-2044



Logistics and Business Services

FREEDOM OF INFORMATION

Presented June 2013

FREEDOM OF INFORMATION

- Purposes of the Act
- Who is Covered by the Act
- What Records are Covered by the Act
- Cross Government Request - Timelines
- Overview of Standardized Call for Records Process
- Overview of the Three Mandatory Exceptions to Disclosure
- Overview of the Eight Discretionary Exceptions to Disclosure
- FOI Fast Facts
- Demand for FOI Requests
- On-Time Completion, Average Processing Days and Average Overdue Days
- Changing Nature of FOI Applicants
- Calendar Management
- Severing Guidelines

PURPOSES OF THE ACT

Accountability to the Public

- Legislated right to access all government records - specifying limited exceptions (i.e. make what is commonly referred to as a 'FOI request')

Protection of Privacy

- Provides a right of access to individuals own personal information
- Regulates how public bodies collect, use and disclose personal information
- Right to request correction of personal information

Body's decision(s) made under FOIPPA

- The independent reviews extend beyond decisions regarding disclosure

WHO IS COVERED BY THE ACT

All provincial ministries, and most provincial agencies, boards, commissions, Crown corporations and smaller agencies

Local public bodies

- School Districts
- Colleges and universities
- Regional health boards

Self-governing professions and occupations

- Teachers
- Doctors
- Nurses

WHAT RECORDS ARE COVERED BY THE ACT

All records in the **custody** or under the **control** of a public body.

What is a Record?

- Any information recorded or stored by any means whether in hard copy or in electronic format.
- Regardless of content and subject matter, the following are subject to an FOI request:
 - briefing notes
 - vouchers
 - telephone records
 - notebooks/daybooks
 - contractor records
 - email
 - records on your smartphone
 - transitory records

CROSS GOVERNMENT REQUEST – TIMELINES

30 DAYS!



Unless.....

The request necessitates a 30 Day Extension under the Act

OVERVIEW OF STANDARDIZED CALL FOR RECORDS PROCESS

- Standard Call for Records Forms and Guidelines for record submissions are provided to all ministry program areas.
- Ministry responsibilities include provision of the following information to IAO:
 - where search for records was conducted (i.e. TRIM files, databases, off-site records)
 - duration of search time by ministry program area
 - who conducted the record search
 - potential HARMS that could result from disclosure of records gathered
 - ISSUES associated with disclosure of records gathered
 - regional locations where records pertaining to this request may reside

OVERVIEW OF THE THREE MANDATORY EXCEPTIONS TO DISCLOSURE

The head must **not** release requested information:

- Cabinet Confidences – Section 12
- Third party business information – Section 21
- A third party's personal information – Section 22

OVERVIEW OF THE EIGHT DISCRETIONARY EXCEPTIONS TO DISCLOSURE

Gives the head of the public body discretion to refuse or to disclose information.

- Policy Advice or recommendations – Section 13
- Legal Advice (solicitor-client privilege) – Section 14
- Law Enforcement – Section 15
- Intergovernmental relations or negotiations – Section 16
- Financial or economic interests – Section 17
- Heritage sites and any rare or endangered living resources – Section 18
- Danger to health and safety – Section 19
- Information soon to be published or released – Section 20

FOI FAST FACTS

Government has maintained an on-time rate of **87%** despite a huge increase in volume and less staff

In fiscal 2012/13, media requests were up by **67%** and political party requests were up by **49%**

For the first time, government is receiving almost as many **general** requests as **personal** requests

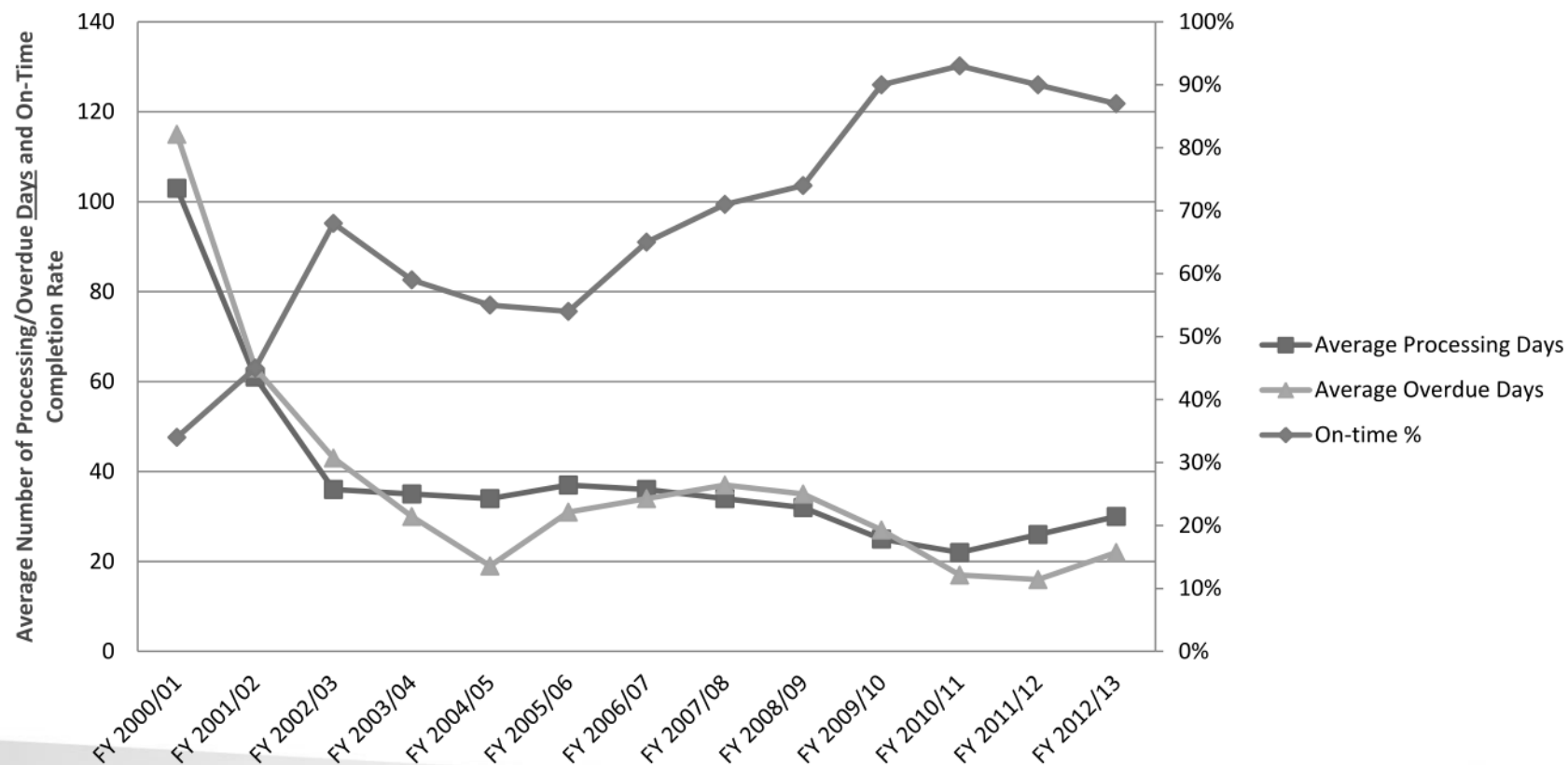
Government received over **10,000** FOI requests in 2012/13, a 23% increase over last fiscal

One media applicant made over **700 FOI requests** in 2012/13, and over 1,000 in the past 2 years

DEMAND FOR FOI REQUESTS CONTINUES TO INCREASE

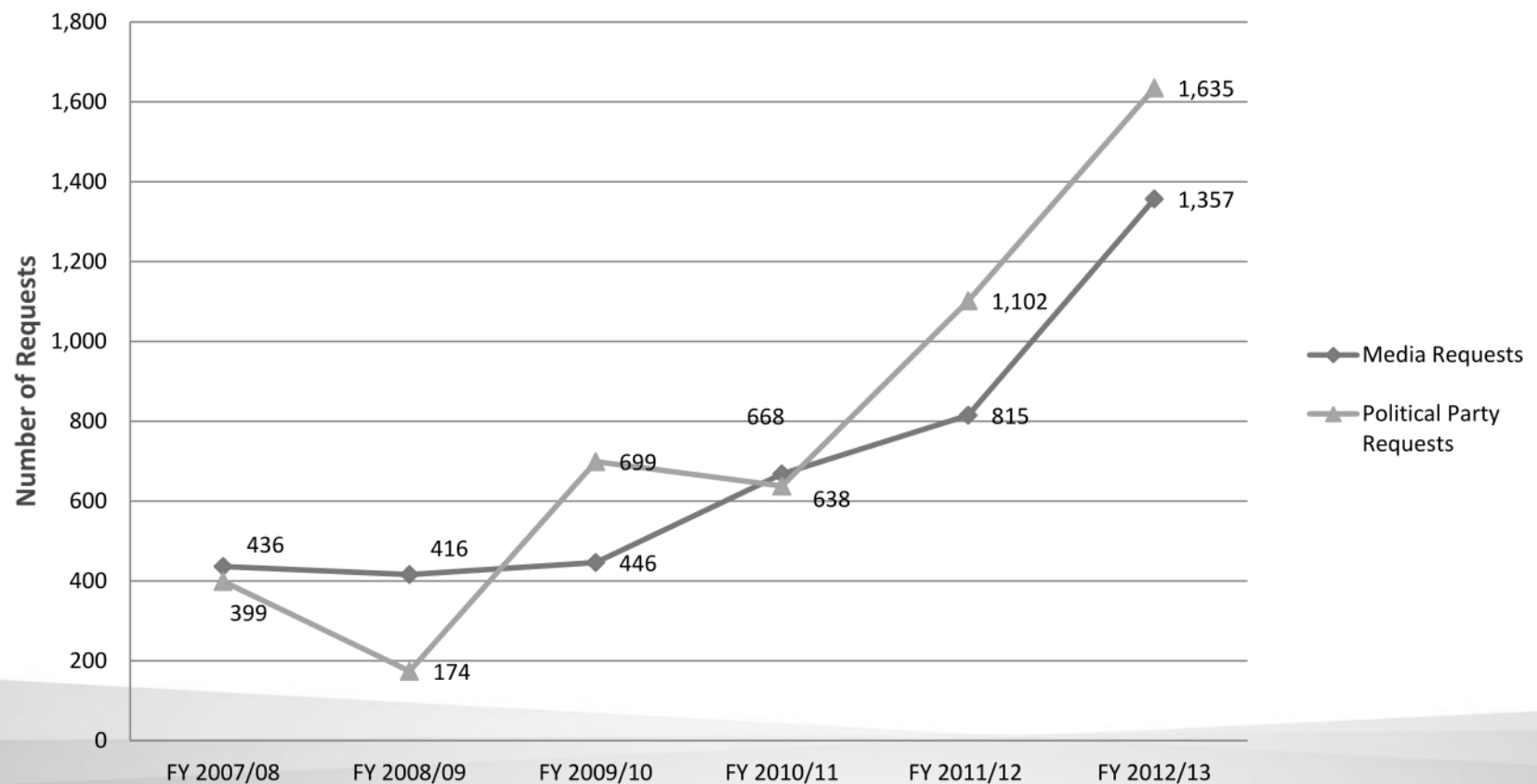
Fiscal Year	Total Requests Received	% On-Time
2007/08	5,394	71
2008/09	6,570	74
2009/10	7,654	90
2010/11	7,829	93
2011/12	8,423	90
2012/13	10,299	87

ON-TIME COMPLETION, AVERAGE PROCESSING DAYS AND AVERAGE OVERDUE DAYS (2001 TO 2012)



CHANGING NATURE OF FOI APPLICANTS

Requests from Political Parties and Media



CALENDAR MANAGEMENT

OUTLOOK CALENDARS

- Be wary of embedded documents, as the calendar and the attachments have different life spans
- Ensure calendar consistency and clarity
 - be clear about the subject of the meeting and who is expected to attend
 - keep the meeting subject concise
- Keep calendars current
 - update the calendar as changes occur
 - delete meetings that did not occur or were not attended
 - update the calendar to record the names and titles of individual(s) who actually attended the meeting as the calendar owner's representative
- Personal appointments
 - mark as "private" – details will not show up in a printed copy or to anyone other than the calendar owner or a delegate
 - caution – ensure that only personal appointments are labeled as "private". Calendar records must be accurate and are subject to a formal access request under the FOIPP Act
 - consider deleting "private" or personal appointments immediately after they occur

SEVERING GUIDELINES - CALENDAR ENTRIES

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



Logistics and Business Services

FREEDOM OF INFORMATION

Presented June 2013

FREEDOM OF INFORMATION

1. What you need to know about the FOI Act
2. How the FOI process works
3. Trends in FOI
4. Calendar requests
5. Next steps

PURPOSES OF THE ACT

Accountability to the Public

- Legislated right to access all government records - specifying limited exceptions (i.e. make what is commonly referred to as a 'FOI request')

Protection of Privacy

- Provides a right of access to individuals own personal information
- Regulates how public bodies collect, use and disclose personal information
- Right to request correction of personal information

Body's decision(s) made under FOIPPA

- The independent reviews extend beyond decisions regarding disclosure

Purposes of the Act

ACCOUNTABILITY

RIGHT OF ACCESS TO
RECORDS



PRIVACY

PREVENT UNAUTHORIZED
COLLECTION, USE OR
DISCLOSURE OF PERSONAL
INFORMATION

INDEPENDENT OVERSIGHT

WHO IS COVERED BY THE ACT

All provincial ministries, and most provincial agencies, boards, commissions, Crown corporations and smaller agencies

Local public bodies

- School Districts
- Colleges and universities
- Regional health boards

Self-governing professions and occupations

- Teachers
- Doctors
- Nurses

➤ Government is only responsible for requests to BC government ministries

WHAT RECORDS ARE COVERED BY THE ACT

All records in the **custody** or under the **control** of a public body

What is a Record?

- Any information recorded or stored by any means whether in hard copy or in electronic format
- Regardless of content and subject matter, the following are subject to an FOI request:
 - briefing notes
 - vouchers
 - telephone records
 - notebooks/daybooks
 - contractor records
 - email
 - records on your smartphone
 - transitory records

CROSS GOVERNMENT REQUEST – TIMELINES

30 DAYS!



Unless.....

The request necessitates a 30 Day Extension under the Act

WHAT HAPPENS WHEN AN FOI REQUEST IS RECEIVED?

- Standard Call for Records Forms and Guidelines for record submissions are provided to all ministry program areas
- Ministry responsibilities include provision of the following information to IAO:
 - where search for records was conducted (i.e. TRIM files, databases, off-site records)
 - duration of search time by ministry program area
 - who conducted the record search
 - potential HARMS that could result from disclosure of records gathered
 - ISSUES associated with disclosure of records gathered
 - regional locations where records pertaining to this request may reside

How FOI Works

Mandatory Exceptions	
Section 12	Cabinet confidence
Section 21	Third party business information
Section 22	Personal information
Discretionary Exceptions	
Section 13	Policy advice/recommendations
Section 14	Legal advice
Section 15	Law enforcement
Section 16	Intergovernmental relations
Section 17	Financial or economic interests
Section 18	Heritage sites
Section 19	Personal health or safety
Section 20	Information soon to be published

FOI APPROVAL PROCESS

- FOI requests are sent to program areas (ministries) for review and sign-off
- The DM or delegated head of the public body is responsible for final sign-off on all requests
- The DM or delegated head of the public body exercises discretion with respect to disclosure recommendations

FOI FAST FACTS

Government has maintained an on-time rate of **87%** despite a 57% increase in volume since 2008/09

In fiscal 2012/13, media requests were up by **68%** and political party requests were up by **48%**

For the first time, government is receiving almost as many **general** requests as **personal** requests

Government received over **10,000** FOI requests in 2012/13, a 22% increase over last fiscal

One media applicant made over **700 FOI requests** in 2012/13, and over 1,000 in the past 2 years

DEMAND FOR FOI REQUESTS CONTINUES TO INCREASE

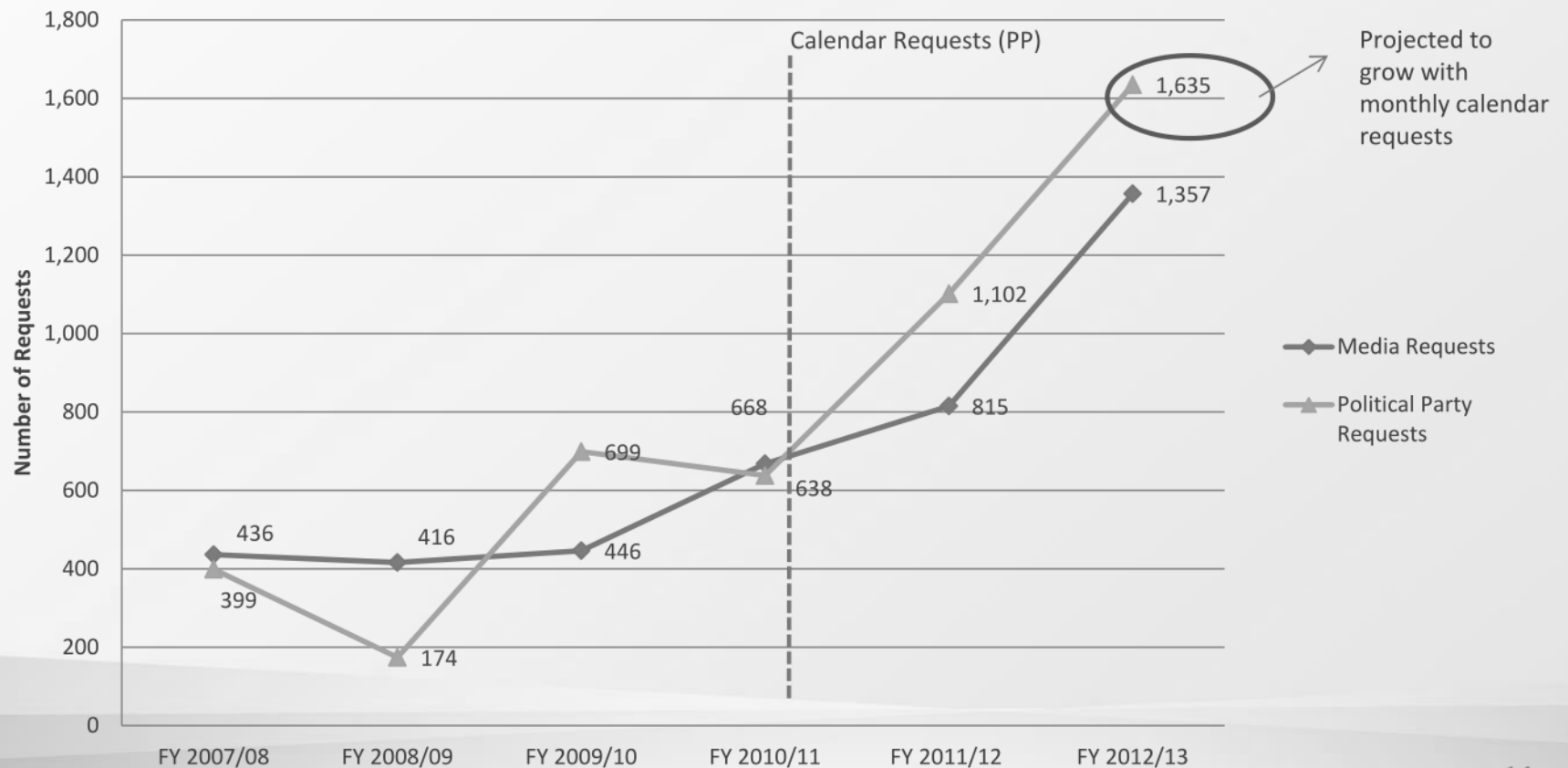
Fiscal Year	General Requests	Personal Requests	Total Requests Received	% On-Time
2007/08	1,805	3,589	5,394	71
2008/09	1,693	4,877	6,570	74
2009/10	2,532	5,122	7,654	90
2010/11	2,756	5,073	7,829	93
2011/12	3,329	5,094	8,423	90
2012/13	4,815	5,484	10,299	87
2013/14 (projected)	4,000	5,500	9,500	75

RESPONSES WITH RECORDS AND NO RECORDS

Fiscal Year	Number of Closed Requests	On-Time Requests	Percentage of No Records Responses
2009/10	7,750	6,984	21%
2010/11	7,939	7,145	24%
2011/12	8,212	7,392	21%
2012/13	9,524	8,325	25%

CHANGING NATURE OF FOI APPLICANTS

Requests from Political Parties and Media



CALENDAR MANAGEMENT

- Government generally receives monthly or bi-monthly requests for DM and ADM calendars. Last month, the requestor included ED calendars

OUTLOOK CALENDARS

- Be wary of embedded documents, as the calendar and the attachments have different life spans
- Ensure calendar consistency and clarity
 - be clear about the subject of the meeting and who is expected to attend
 - keep the meeting subject concise
- Keep calendars current
 - update the calendar as changes occur
 - delete meetings that did not occur or were not attended
 - update the calendar to record the names and titles of individual(s) who actually attended the meeting as the calendar owner's representative
- Personal appointments
 - mark as "private" – details will not show up in a printed copy or to anyone other than the calendar owner or a delegate
 - caution – ensure that only personal appointments are labeled as "private". Calendar records must be accurate and are subject to a formal access request under the FOIPP Act
 - consider deleting "private" or personal appointments immediately after they occur

SEVERING GUIDELINES - CALENDAR ENTRIES

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

TRENDS AND FORWARD THINKING

- Training for Minister's Office staff is planned
- For the past 6 years, FOI request volume has increased by an average of 14%. Expect volume to remain high
- OPIC will be releasing an investigation report on the multicultural outreach strategy in summer 2013

Good Practice Tips for Managing and Maintaining Calendars

This Good Practice Tips sheet is intended to provide tips to employees who are responsible for managing and maintaining calendars.

General Tips and Good Practices:

- ☐ Do not sever non personal information out of a calendar, let IAO help you.
- ☐ Avoid the use of any personal or editorializing comments in making calendar entries.
- ☐ Anything to do with the business of government must be shown in the calendar – Monday to Sunday – 24 hours a day.
- ☐ Do not include appointments of other people. (i.e. Minister or Deputy Minister).

Recording Entries:

- ☐ Ensure that calendar entries are **clear** and **consistent** at time of entry.
- ☐ Be **clear** about the subject of the meeting and who is expected to attend. Keep the meeting subject concise. More information may lead to unnecessary redaction.

Examples:

◆ **Concise entry** – “Meeting with John Smith, EFO, on Citizen Engagement”

This entry can likely be released in full.

◆ **Unnecessary degree of detail** – “Meeting with John Smith, EFO, re: cabinet submission on Citizen engagement”

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

- ☐ Be **consistent** at the time of entry – all those attending the meeting should have the same or similar calendar entry. When arranging meetings with other staff, provide a standard title for the meeting and ask that the other office use this title in recording the meeting - this promotes consistency across calendars in how the meeting is recorded and relayed to citizens.
- ◆ **Tip:** Consider using the Outlook “meeting request function” to schedule meetings; this will automatically assign the same title and description to the same meeting.

Personal Appointments:

- ☐ Consider recording personal appointments (doctor or dentist appointments, children’s events, etc.) as “**Private**” in the Outlook calendar which means that the printed record will simply show “private”, but the details of the entry will appear to the calendar owner (and anyone else with full access to the calendar).

- ◆ Caution: Ensure that only personal appointments are labeled as **private**. Calendar records must be accurate and are subject to a formal access request under the *FOIPPA Act*.
- ❑ Delete **Private** or personal appointments after they occur.
- ◆ Note: **Private** or personal appointments need to be redacted from a Calendar record. Deleting **private** or personal appointments after the appointment has occurred eliminates the need for IAO to redact the record.

Keeping Calendars Current:

- ❑ A calendar is a planning document to record scheduled meetings and events and who is expected to attend. To promote accuracy and completeness, the calendar record should always be current by updating the calendar as changes occur.

Examples:

- ◆ Delete meetings that did not occur, or where the calendar owner (or their representative) did not attend;
 - ◆ Where someone else attended on behalf of the calendar owner, update the calendar to record the names and titles of the individual(s) who actually attended the meeting as the calendar owner's representative.
- ❑ Calendars should be maintained when the calendar owner is on leave or otherwise absent. Where the absent calendar owner is invited to a meeting or event and someone else attends on the calendar owner's behalf, this meeting or event should be recorded in the calendar indicating who attended.

Point of Contact for IAO:

- ❑ Ministers', Deputy Ministers' and ADM's offices are asked to designate a primary and secondary contact for the IAO to respond to questions as necessary.

Severing Guidelines - Calendar Entries

ENTRY OR DESCRIPTION OF ENTRY	SEVERED OR NOT SEVERED
Blackberry/cellphone numbers for government employees	Severed under section 17 – Blackberry/cellphone numbers that constitute “business contact numbers” (i.e. they are part of a signature block) will be disclosed but “confidential, unlisted” Blackberry/cellphone numbers will be withheld under section 17. The financial harm to the public body is the high cost of constantly changing these phone numbers after every FOI request.
“Cabinet” or “Cabinet Retreat”	Not Severed – there is not enough information in this entry to reveal the substance of deliberations of the Executive Council or its committees.
“Chambers”	Not Severed
Constituency related – any entries in the Minister’s calendar that relate to his/her duties as a Member of the Legislative Assembly	Severed under section 3 - As the office of a Member of the Legislative Assembly is not a public body, any entries in a Minister’s calendar that relate to his/her duties as an MLA will be severed as outside the scope of FOIPA.
Confirmation numbers, Reservation numbers, frequent flyer numbers, etc.	Severed under sections 17, 22 – Most external to government organizations will readily provide additional information regarding a reservation/booking/account provided that you are able to provide these numbers. There is a financial harm to the public body if its credit information is divulged and there is an unreasonable invasion of privacy given that there is a personal credit verification required in order to obtain a corporate travel card.
Accommodation details	Severed under section 15
Meeting location details	Severed under section 15
“Caucus”	Severed under section 3
“Duty House Leader” / “House Duty”	Severed under section 3
“House”	Severed under section 3
Meetings with Officers of the Legislature (see schedule 1 definition), that relate to their duties/functions under an Act	Severed under section 3
Unpublished direct telephone numbers for Minister, DM, ADM, etc.	Severed under section 17 - see comments for severing Blackberry/cellphone numbers
“Issue Prep with Staff”	Not Severed
“QP, “QP Prep”, “QP Briefing”	Not Severed

Severing Guidelines - Calendar Entries

ENTRY OR DESCRIPTION OF ENTRY	SEVERED OR NOT SEVERED
Teleconference information: <ul style="list-style-type: none"> - Dial-in Number - Conference Reference - Participant Conference Access Code - PIN or moderator's code 	Severed under sections 15, 17 Severed under sections 15, 17 Severed under sections 15, 17 Severed under sections 15, 17
Telephone numbers (including cell numbers)/email addresses for people representing an organization (union, association, etc.) *Personal cell numbers for people representing an organization, where they are clearly identified as such	Not Severed – business contact information is not personal information. Severed under section 22
"Throne Speech"	Not Severed –the Throne Speech is considered an event that a Minister attends in both capacities (MLA and Minister).
"Treasury Board"	Not Severed – there is not enough information in this entry to reveal the substance of deliberations of the Executive Council or its committees.
"John Smith – vacation, Jane Doe Acting"	Severed under section 22 - "vacation" Not Severed - "Jane Doe Acting."
File paths printed on bottom of attachments	Not Severed - If a harms assessment determines that the security of a system would be harmed by releasing information included in a file path, the information will be withheld under section 15. This would not generally be the case, as a file path alone doesn't reveal certain specifics that would be required to identify the server which a mapped drive resides on.
360's (executive performance review), mentoring, EPDP	Severed under section 22
Staff/Christmas parties during business hours	Not Severed – the assumption here is that these parties are paid for using public funds and attended by staff within their paid hours of work.
Staff/Christmas parties outside of business hours	Severed under section 22 – the assumption here is that these parties are paid for using personal funds and attended by staff outside of their paid hours of work.

Severing Guidelines - Calendar Entries

Request Dependent Section

In some circumstances, the approach for severing calendar entries will be dependent on the wording of the applicant's request. If a Minister's calendar is requested and there are entries that relate to that individual's duties/functions as a Member of the Legislative Assembly, they would not be responsive to the request. If an applicant agrees to exclude phone numbers and email addresses from their request for a calendar, they would not be responsive to the request. The above are only intended to be examples of circumstances where it would be appropriate to use "not responsive" to remove information in response to an FOI request for calendars (i.e. they do not constitute an exhaustive list).



FREEDOM OF INFORMATION (FOI)

LEGISLATION OVERVIEW AND PRIORITIES AND ADMINISTRATION

Presented to Honourable Andrew Wilkinson

Bobbi Plecas, ADM, Logistics and Business Services
Charmaine Lowe, Executive Director, Legislation, Privacy & Policy

FREEDOM OF INFORMATION (FOI)

- *Freedom of Information and Protection of Privacy Act (FOIPPA)* Legislation
- Office of the Information and Privacy Commissioner (OIPC)
- FOI Administration

Purposes of the Act

ACCOUNTABILITY
RIGHT OF ACCESS
TO RECORDS



PRIVACY
PREVENT UNAUTHORIZED
COLLECTION, USE OR
DISCLOSURE OF
PERSONAL INFORMATION

INDEPENDENT OVERSIGHT

Mandatory Exceptions

Section 12	Cabinet confidence
Section 21	Third party business information
Section 22	Personal information

Discretionary Exceptions

Section 13	Policy advice/recommendations
Section 14	Legal advice
Section 15	Law enforcement
Section 16	Intergovernmental relations
Section 17	Financial or economic interests
Section 18	Heritage sites
Section 19	Personal health or safety
Section 20	Information soon to be published

2900 Public Bodies



COLLEGE OF PHARMACISTS
OF BRITISH COLUMBIA
Safe and Effective Pharmacy Care



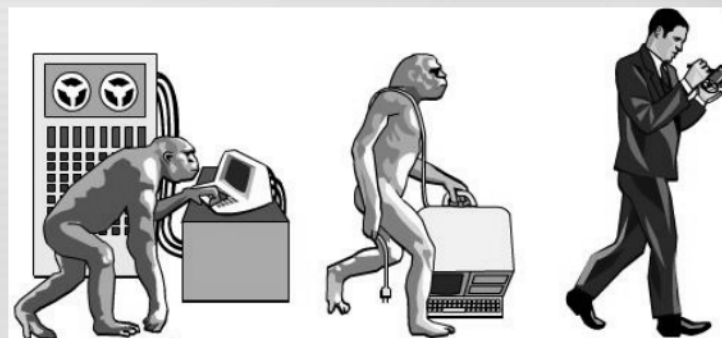
2011 Amendments

Most significant amendments to date:

- Modernized Act (recognized use of social media)
- Added key information sharing authorities to enable integrated and citizen centric service delivery
- Provincial identity management authorities
- Legislative Framework for Open Information/Open Data
- Special Committee recommendations

Balanced with:

- Privacy Impact Assessments
- Data Linking Rules
- Commissioner's oversight



Minister's Responsibilities

- Ministerial Regulations
(Schedule 2 and 3)
- Annual Report
- Personal Information Directory
- Issue directions on IDIM, PIAs, ISAs and Open Information





Legislation, Privacy and Policy Branch (LPP)

- Manage Legislation (FOIPPA, PIPA, DDA, ETA)
- Privacy management for government (PIAs, ISAs, PID, policies, strategic advice)
- Liaison with the Commissioner's office
- Privacy investigations
- Corporate Privacy Training and Awareness

s.22



IAO Responsibilities

s.22

Information Access Operations (IAO) is a highly transactional, citizen-facing operation.

Last year, IAO responded to 10,000 requests from citizens – nearly half of which were general requests.

IAO is responsible for posting responses to general FOI requests and travel expense summaries of senior government officials to Open Information.

Special Legislative Committee

- Must be struck every six years to review and report on the Act
- There have been three reviews (1999, 2004 and 2010)
- Next committee will convene in 2016



Committee	Recommendations	Amendment	Policy/Other	Under Consideration
2004	28	18	9	1
2010	35	18	10	7



Information and Privacy Commissioner



- Independent Officer of the Legislature
- Appointed for a six-year term
 - appointed May 2010
- Issues orders, reports and public comment on administration of the Act
- Strongest oversight powers of any Commissioner in Canada
- Also responsible for overseeing PIPA

COMMISSIONER'S REPORTS

Recent:

- “No responsive records”

Outstanding:

- Multicultural Strategic Outreach Plan
- Health Data Breach
- Privacy Management Program
- Open Government
- Section 25 – Disclosure in the Public Interest



OIPC REVIEW ON NO RECORDS RESPONSES (NRR)

Investigation report issued March 4, 2013 with 6 recommendations:

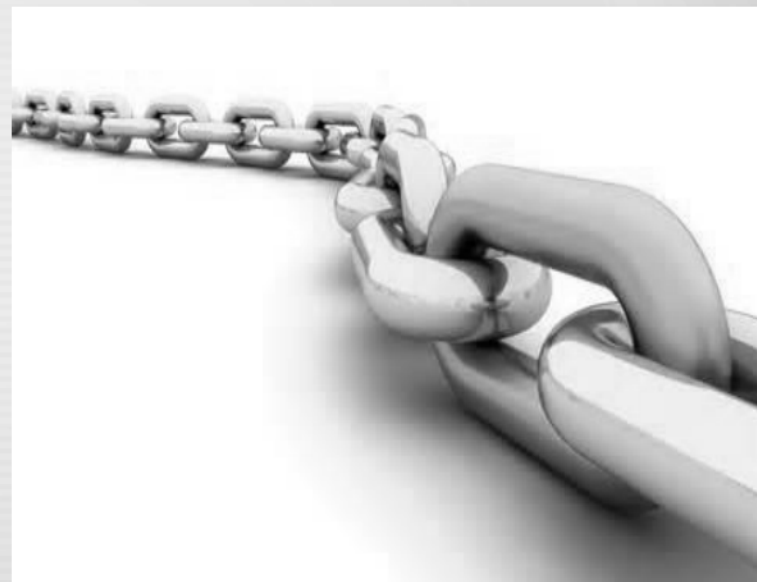
- Create legislative “duty to document” – deferred to 2016 Special Committee to Review FOIPPA
- More accurately record NRRs from multiple ministries – **implemented** (down from 25% to 15% NRR this year to date)
- Interpret requests more broadly (including calendars) – **implemented**
- Do not narrow requests if it will result in NRR – **implemented**
- Transfer requests to the correct ministry if misdirected – **implemented**
- Provide more detail about NRR to applicants – **implemented**

Commissioner's Priorities

1. Data Linking Activities
2. Subsidiary Corporations
3. Duty to Document
4. Privacy Management Program

Priority 1: Data Linking

- Data linking provisions added to FOIPPA in 2011
- Commissioner approved language
- Now concerned definitions too narrow
- Requests immediate amendment
- Public bodies universally opposed to broadening scope





Priority 2: Subsidiary Corporations

- 2010 Special Committee recommended coverage of subsidiary corporations
- Commissioner issued public letter calling for same
- Pressure from media and advocacy groups
- Public bodies opposed
- Ministry continues to develop and consult on options

Copyright

Priority 3: Duty to Document

- Commissioner issued public letter calling for “duty to document”
- March 2013 investigation report noted increase in “oral government”
- No other Canadian jurisdiction has this duty in FOIPPA
- Issue was raised with the 2010 Special Committee; did not recommend action

Copyright

Priority 4: Privacy Management Program (PMP)

- Commissioner is about to issue recommendations for privacy management program
- Related to her investigation into Ministry of Health data breach
- May recommend the decentralization of privacy functions in government
- LPP is currently enhancing and documenting its corporate privacy management program

Copyright

Future Legislative Plans

- Currently planned for Fall 2013 or Spring 2014:
 - Streamline Commissioner's review and complaint handling processes; align them with PIPA
 - Cover subsidiary corporations of local public bodies
 - Broaden data linking definitions
- Commissioner will likely express concern if these amendments, particularly data linking amendments, are not introduced at the next available opportunity

FOI ADMINISTRATION FAST FACTS

Government has maintained an on-time rate of **87%** despite a 57% increase in volume since 2008/09

In fiscal 2012/13, media requests were up by **68%** and political party requests were up by **48%**

IAO is approved for **115 FTEs**.

Currently, **93** positions are staffed. If staffing had kept pace with request increases since 2008/09, IAO would have **148 FOI staff**

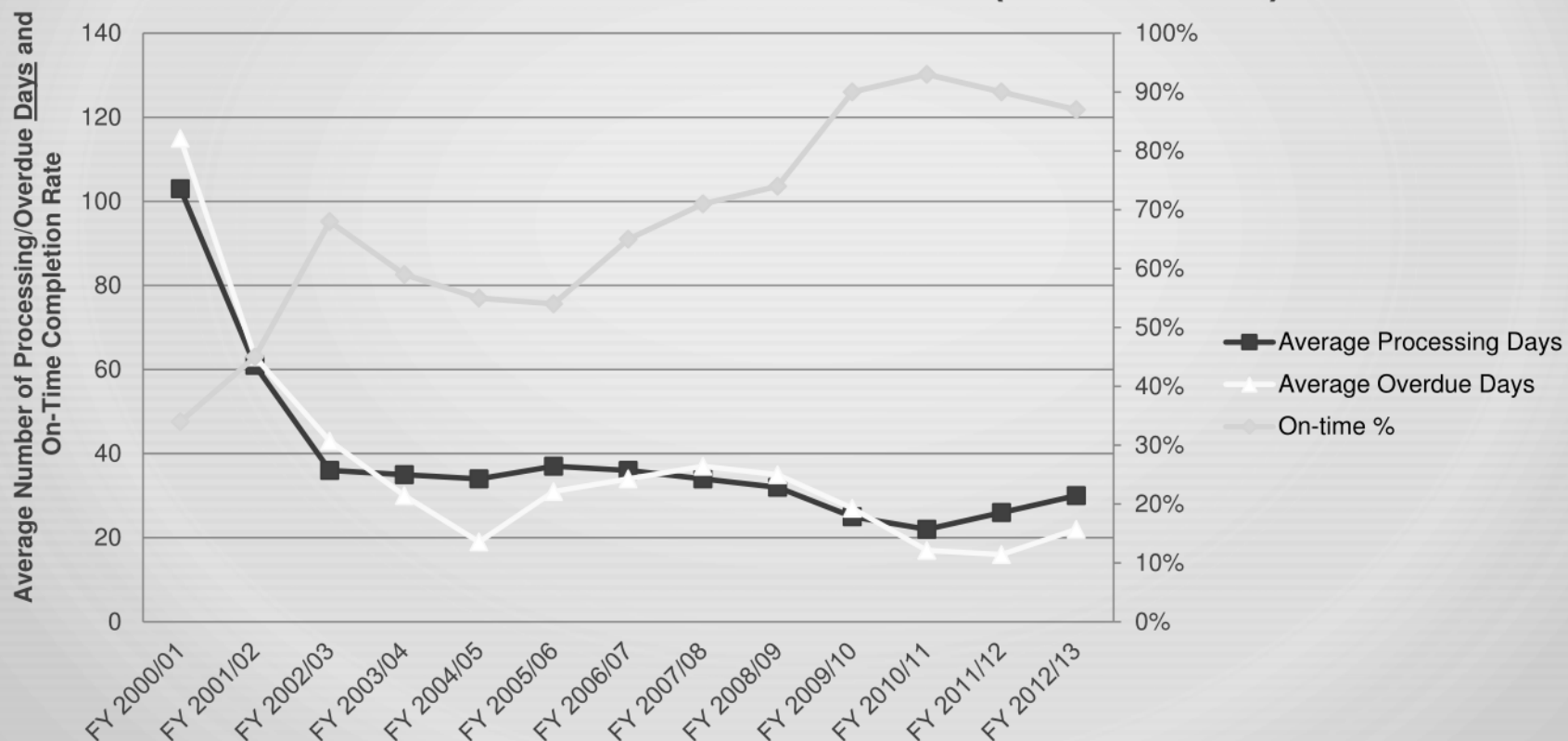
Government received over **10,000** FOI requests in 2012/13 (approx. 4,800 generals; 5,500 personals), a 22% increase over last fiscal

One media applicant made over **700 FOI requests** in 2012/13, and over **1,000** in the past 2 years

DEMAND FOR FOI REQUESTS CONTINUES TO INCREASE

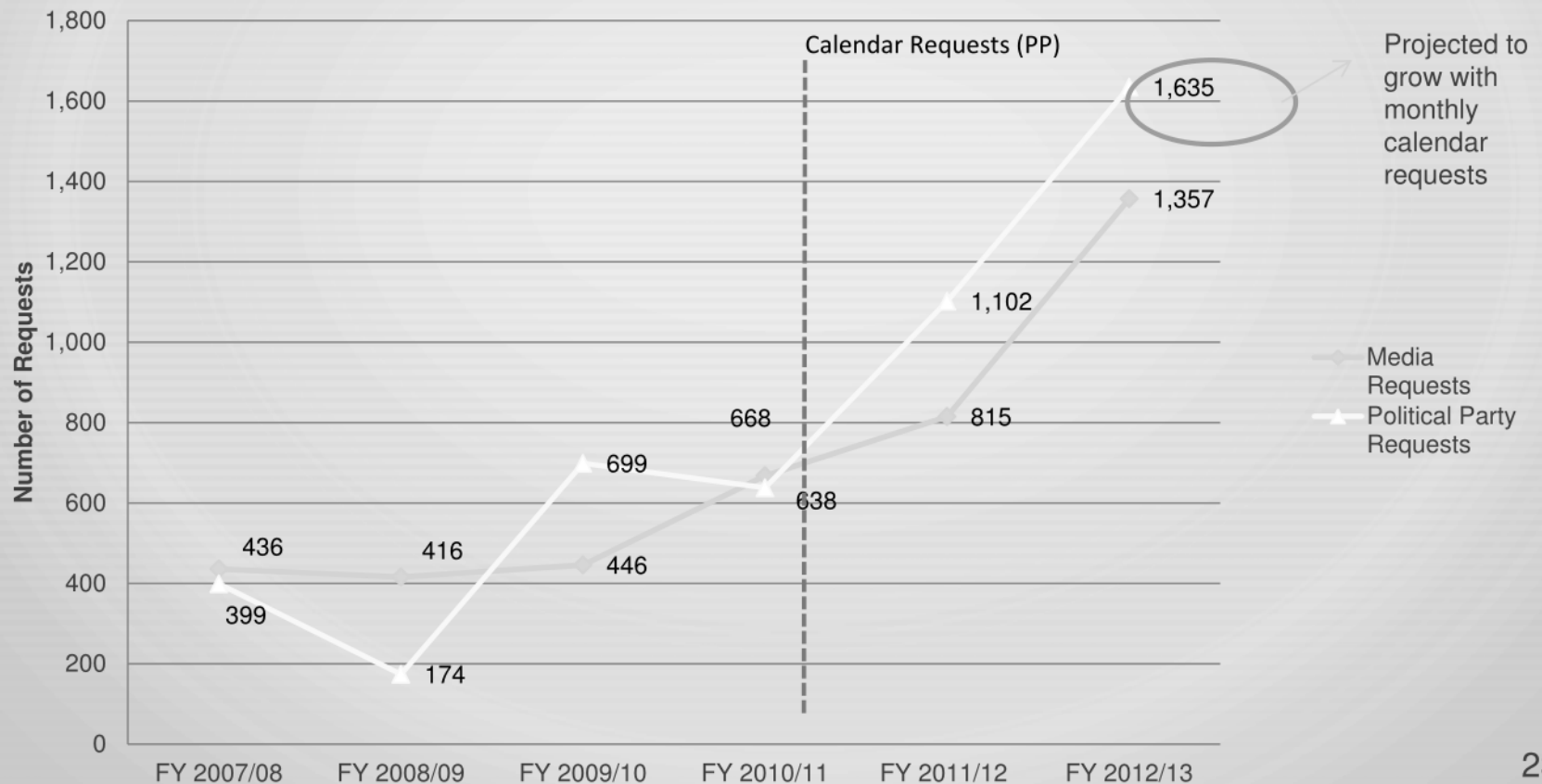
Fiscal Year	General Requests	Personal Requests	Total Requests Received	% On-Time
2007/08	1,805	3,589	5,394	71
2008/09	1,693	4,877	6,570	74
2009/10	2,532	5,122	7,654	90
2010/11	2,756	5,073	7,829	93
2011/12	3,329	5,094	8,423	90
2012/13	4,815	5,484	10,299	87
2013/14 (projected)	4,000	5,500	9,500	75

ON-TIME COMPLETION, AVERAGE PROCESSING DAYS AND AVERAGE OVERDUE DAYS (2001 to 2012)



CHANGING NATURE OF FOI APPLICANTS

Requests from Political Parties and Media



BUDGET AND FTES

2012/13 Budget		2013/14
Gross Expend (\$ Thousands)	Approved FTEs	Current Complement
7,883	115	93

- IAO received 22% more requests in 2012/13 over the previous fiscal year
- It takes approximately 6 months to train a new FOI analyst
- IAO has an annual staff churn of approximately 15 - 20%



RISKS TO INFORMATION ACCESS OPERATIONS

- **Timeliness:**

- Government is projecting to receive approximately 9,500 requests this fiscal year. IAO is currently at 77% on-time. If the remainder of this year's requests are closed at a rate of 90% on-time, government would end the year at 81% on-time. A more realistic projection is 75%
- There are approximately 450 requests in backlog that are already overdue

- **Volume Increase**

- Request volume has increased an average of 14% each year over the past 6 years

- **FOI Resources**

- IAO currently has 22 vacancies. It takes approximately 6 months to train a new FOI analyst
- FOI classifications have not kept pace with the changing nature of FOI work. This results in a high rate of staff leaving IAO for higher-paying positions in the public service

- **IT Implementation**

- IAO is launching a new end to end solution in November 2013. Administrative efficiencies will not be realized until 2014/15

STRATEGIES TO DEAL WITH 10K FOI REQUESTS

1. Business process improvements – continue with staff improvement program and leverage gains through corporate Lean initiative
2. Implementation of new IT system – government has procured an end to end FOI technical solution to reduce the administrative burden. Scheduled for launch in November 2013
3. Reclassify FOI positions – make IAO a workplace of choice and reduce churn
4. Staff up – IAO is currently 23% below its budgeted FTE allotment

Performance Projections	
Year	On-Time Percentage
2013/14	75
2014/15	90

OPEN INFORMATION

- Introduced July 2011 with policy guidelines
- 2,300 General FOI requests posted (no Personals)
- Over 1,000 Minister and Deputy Minister travel expense summaries posted
- Over 52,000 visits to and 38,000 downloads from the Open Information website
- Proactively released 53 per cent of eligible general requests
- Requests are exempt from publication due to security concerns (72 per cent), personal information (14 per cent), and business information (12 per cent)

QUESTIONS?

Government Records Service, Ministry of Technology, Innovation and Citizens' Services

Overview of published documentation of changes in policy or practice relating to retention of information, particularly e-mails and minutes of meetings and discussions (03/11/2011 To 10/24/2015).

The Government Records Service (GRS) provides services supporting records management for all B.C. Government ministries.

GRS services include provision of policies and best practice guides; training; and development of records retention and disposition schedules (records schedules).

Documentation of these policies, guides, training, and records schedules is published on the [GRS website](#). As described below, the documentation includes dates of publication or revision that can be used to identify which material is within the time period of interest.

Records schedules

- [ARCS Online](#) provides the current records scheduling requirements for administrative records (the records common to every ministry).
 - Primaries particularly relevant for retention of information re. meetings and discussions include
 - [102 Staff Meetings](#)
 - [255 Correspondence Management](#)
 - [280 Executive Services – General](#)
 - Amendments made over time to ARCS retention schedules are documented in the [consolidated amendment summary](#) available on the “About ARCS” page (with a column for the date each amendment was approved).
- The [ORCS e-library](#) provides most current operational records schedules used for the records of specific program areas, as well as lists of all such schedules approved over time.
 - There is a list sorted by [approval date](#) to show when an ORCS was first approved or subsequently amended (which will show which were changed within the time period in question).
- [Special schedules](#) cover particular types of records across government. For each schedule, the most recent approval/amendment date is indicated on the last line of the schedule itself.
- Special schedules of particular relevance to retention of email and Executive meetings include:
 - [Transitory records \(102901\)](#)
 - [Electronic Mail \(102903\)](#) (essentially is a pointer to other schedules)
 - [Executive Records \(102906\)](#)

Recorded Information Management (RIM) Policy Manual

The RIM Manual provides policies relating to the entire life cycle of government records of all types.

Of particular interest may be the policies on:

- [Government Records](#) and [Government Recordkeeping](#)
- [Records schedule development](#)
- [Records Destruction](#)

The RIM manual has undergone a major renovation in the past year. The majority of the changes have been stylistic changes (presentation format and language) rather than changes to key directions. The [concordance table](#) identifies the specific dates that policies were converted.

Records Management Guides

The GRS Guides assist provide records management practices guidance for government employees.

Included are

- Email and Collaboration Guides; e.g. ,[Email: Recordkeeping Responsibilities](#), [Live Meeting \(Online Meetings\)](#), [Instant and Text Messages](#)
- [Transitory Records Guide](#)

Additional resources

The [Training page](#) provides additional guidance for managing records

The [Records Transfer and Storage page](#) provides links to forms to be used for requesting authorization to destroy records (in accordance with policy and schedules).



Knowledge and Information Services Branch
Office of the Government CIO
Ministry of Citizens' Services

Chapter 12

Information and Technology Management Supplemental Manual

April 2010

DRAFT – CHAPTER 12 SUPPLEMENTAL

Publication history

Version	Date	Status
	Pre-2000	Part of Chapter 8, General Management Operating Manual
	2001	Separate manual established to support Chapter 12, Core Policy Manual
	2004	Minor edits
	2007	Extensive stakeholder consultation to align Supplemental with Chapter 12, Core Policy Manual
	Apr, 2010	Updating broken links and names of business units.

DRAFT – CHAPTER 12 SUPPLEMENTAL

Table of Contents

Preamble	3
Roles and Responsibilities	7
Government Chief Information Officer	7
Ministry Chief Information Officer	9
12.3.1 Employee Responsibility	11
12.3.1 a) Appropriate Use of Government Information Technology	11
12.3.2 Information and Technology Planning	17
12.3.2 (a) Information Resource Management Plan	17
12.3.2 (b) Vital Records and Information System Business Continuity Plans	19
12.3.3 Information Management	21
12.3.3 I (a) Data Architecture and Management	21
12.3.3 II (a) Privacy Impact Assessment	25
12.3.3 II (b) Information Sharing Agreement	28
12.3.3 II (c) Personal Information Banks	30
12.3.3 II (d) Personal Information Management	32
12.3.3 III (a) Governance of Records and Information	36
12.3.3 III (b) Classification, Scheduling and Maintenance of Government Records	44
12.3.3 III (c) Storage and Disposition of Government Records	47
12.3.3 IV (a) Routine Release of Information	51
12.3.3 IV (b) Internal Use of Government Information Assets	53
12.3.3 IV (c) Publication of Government Email Addresses	56
12.3.3 IV (d) Disclosure Requirements for Legal Proceedings	60
12.3.3 IV (e) Crown Copyright	62
12.3.3 IV (f) Disposal of Intellectual Property	64
12.3.5 Information Technology Management	66
12.3.5 (a) Information and Technology Project Management	66
12.3.5 (b) Information Technology Standards	67
12.3.5 (c) Information and Technology Procurement and Unsolicited Proposals	70
12.3.5 (d) Information Technology Operations and Evaluation	71
12.3.6 Information and Technology Security	73
12.3.6 (a) Information and Technology Security	73

DRAFT – CHAPTER 12 SUPPLEMENTAL

DRAFT – CHAPTER 12 SUPPLEMENTAL

Office of the Chief Information Officer	Effective Date:
Province of British Columbia	Scheduled Review:
12.3.3 Information Management	
12.3.3 III Managing Information	
12.3.3 III (a) Governance of Records and Information	
<p>From Chapter 12, Core Policy and Procedures:</p> <ol style="list-style-type: none"> 1. Government must manage all records created and received during the conduct of its business activities. 2. Ministries must establish and maintain a recorded information management program. 3. Ministries must establish and maintain a forms management program. 4. Government records must be managed and preserved to remain authentic, reliable, trustworthy, secure, complete and accessible over time and location regardless of media or format. 5. Ministries transferring records to off-site storage must use approved records centres. 	

Section Contents:

- 12.3.3 III (a) i. Identification and Management of Government Records
- 12.3.3 III (a) ii. Final Disposition of Government Records
- 12.3.3 III (a) iii. Components of a Recorded Information Management Program
- 12.3.3 III (a) iv. Ministry Records Officer
- 12.3.3 III (a) v. Forms Management Program
- 12.3.3 III (a) vi. Storage and Preservation of Government Records
- 12.3.3 III (a) vii. Financial Records
- 12.3.3 III (a) viii. Access to Information by the Office of the Auditor General

Purpose:

To ensure that government creates, retains and manages sufficient records to document its operational and business activities, support its decision-making processes, and meet all of its ongoing business, legal and accountability requirements.

12.3.3 III (a) i. Identification and Management of Government Records

- The *Interpretation Act* defines ‘record’ as ‘including 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’. In general, any record created or received by an employee, contractor or volunteer and used to support a government function or to conduct government business is a government record, regardless of media or format.

Ministries will identify, manage and retain government records as directed in the Recorded Information Management Manual and government standard records classification and scheduling systems. The Information Access Operations Records Management Branch will provide

DRAFT – CHAPTER 12 SUPPLEMENTAL

ministries with expert advice, assistance and guidelines on the management and scheduling of their records, regardless of media or format. Information Access Operations Records Management Branch will identify and select ministry records for preservation in the government archives. Information Access Operations Records Management Branch will also ensure that ministry operational records classification and scheduling systems meet government standards. Ministries are responsible for ensuring that ministry records retention and disposition schedules include records created or received in all media or formats (e.g., paper records, email, electronic information stored on Local Area Networks, other information systems or removable media).

Identification and Management of Government Records

- Ministries must establish a ministry recorded information management program with appropriate assignment of responsibilities. For guidance see the RIM Policy Manual.
- Employees must create and maintain complete and accurate records sufficient to document their decision-making and work activities.
- All government records are subject to the Document Disposal Act with the exception of records created by agencies identified through a legal opinion as not falling under the provisions of the Document Disposal Act. Contact the Ministry Records Officer or the Information Access Operations Records Management Branch for information on applicability of the Document Disposal Act to the records of a specific agency.
- Records in the physical custody of government contractors may be under the legal custody and control of a ministry and covered by the provisions of the Document Disposal Act and/or the Freedom of Information and Protection of Privacy Act (FOIPPA). Contracts must contain provisions regarding the custody, control, retention, disposition, use and security of, and access to, any records generated as a result of the contract.
- Records created or accumulated by Cabinet ministers (and their offices) in the execution of ministerial responsibilities are government records subject to both the Document Disposal Act and the Freedom of Information and Protection of Privacy Act. These records must be managed as part of the ministry records system.
- Records created or accumulated by Commissions of Inquiry established under the Inquiry Act are government records and subject to both the Document Disposal Act and the Freedom of Information and Protection of Privacy Act.
- Records created by volunteers performing work under the direction of a government employee are government records and subject to the Document Disposal Act and the Freedom of Information and Protection of Privacy Act.

Security of Government Records

- Security measures must be implemented to ensure that records are created, acquired, updated, handled, used, transmitted, transported, filed, stored and destroyed in a manner appropriate to their sensitivity and value.
- Security measures must ensure the integrity of government records, protecting them from unauthorized access or disclosure and from damage, loss or unauthorized changes.
- Policy governing information security categories, access to information, information exchange with other governments, and secure handling of records is covered in the Core Policy and Procedures Manual, Chapter 15 – Security.

Physical and Legal Custody of Government Records

- A protocol agreement must be in place when physical custody (but not legal custody or the authority to apply final disposition) of records is transferred to an agency not covered by the Document Disposal Act. The agreement must identify the records in question, define the rights retained by the Crown and ensure that the records will be managed in accordance with government legislation, regulations, policies, standards and approved records schedules. The agreement may include provisions such as:
 - The transferring ministry or agency may restrict access to, or the disposition of, records created after the transfer;
 - New records created or documentation added to existing records may become government property;
 - Records must be returned to government once they are no longer required or if the information is requested by government; and
 - Intellectual property rights (such as patents and copyright) must be retained by government.
- When physical and legal custody of records is transferred between ministries and agencies covered by the Document Disposal Act, a protocol agreement may be appropriate. Agreements should address issues such as:
 - Production of file lists, finding aids or other documentation used to control or manage the records being transferred; and
 - Responsibility for developing retention and disposition schedules for unscheduled records.

These procedures ensure that government is able to:

- Apply recorded information management policies and standards uniformly across government, and to all government records regardless of media or format (e.g., paper records, email, electronic information stored on Local Area Networks, other information systems or removable media);
- Establish areas and levels of responsibility and accountability;
- Reduce costs and ensure efficient access to and retrieval of government records throughout their lifecycle (information creation to final disposition);
- Provide guidelines and standards for ministries to adhere to;
- Encourage the development of recorded information management practices and procedures within individual ministries;
- Reinforce recorded information management concepts, terms and practices; and
- Increase awareness of the benefits, as well as legal obligations, of diligently following recorded information management standards and guidelines.

For additional information, see the following sources:

- the Recorded Information Management Manual contains policies on identifying and managing government records;
- the Standard ORCS Kit provides the government standard for developing operational records classification systems;
- the Recorded Information Management Glossary provides definitions for records management terminology used in the BC Government; and,

DRAFT – CHAPTER 12 SUPPLEMENTAL

- Information Access Operations Records Management Branch's Recommended Practices and FAQs provide guidelines on managing government email.

12.3.3 III (a) ii. Final Disposition of Government Records

Ministries and the Information Access Operations Records Management Branch will apply final disposition actions to government records in accordance with approved records schedules including the Administrative Records Classification System (ARCS), Operational Records Classification Systems (ORCS), Ongoing Records Systems (ORS), and one-time and special schedules.

See section 12.3.3.III (c) of this manual, Storage and Disposition of Government Records, for details on storage and disposition policy. See also the Recorded Information Management (Recorded Information Management) Manual, policy pol02-04: Disposition of Government Records and ARCS Online: How to Use ARCS.

12.3.3 III (a) iii. Components of a Recorded Information Management Program

Recorded Information Management programs help to ensure that ministries administer, control, document, preserve and protect government information in their legal custody and control. Each ministry is responsible and accountable for establishing and implementing a Recorded Information Management program to manage its records. Components of a Recorded Information Management program include policies and procedures to ensure that ministries accomplish the following:

- Meet legislated requirements for managing government records, including those provided in the *Document Disposal Act* and the *Freedom of Information and Protection of Privacy Act* (FOIPP Act).
- Create and retain sufficient records to provide evidence of organizational activity and administrative decisions and to meet legal, evidential and accountability requirements.
- Support organizational efficiency and economy through sound recorded information management practices.
- Manage government records so that they remain authentic, reliable, and accessible throughout their lifecycle, and are available to support decision making and to meet information access requests.
- Protect and safeguard government records until authorized to apply approved final disposition schedules.
- Preserve records of enduring value while destroying records of lesser value in accordance with approved final disposition schedules, in a timely, secure and environmentally sound manner.
- Provide adequate resources to manage the program.

12.3.3 III (a) iv. Ministry Records Officer

A Records Officer or equivalent must be appointed for each ministry or agency covered by the *Document Disposal Act*. This official is responsible for administration of the recorded information management program within their ministry.

12.3.3 III (a) v. Forms Management Program

Ministries must manage government forms in accordance with government legislation, policies and standards. Components of a forms management program include policies and procedures to ensure that ministries:

- Set guidelines for determining if a form is necessary to meet ministry or agency operational needs (e.g., a statutory requirement).
- Develop forms that collect only the information needed to meet ministry or agency purposes and adhere to the requirements of the *Freedom of Information and Protection of Privacy Act* and the *Document Disposal Act*.
- Work to control the proliferation of ministry forms by eliminating forms that are inefficient, ineffective or redundant.
- Comply with government design standards.

For policies related to financial forms, refer to the Core Policy and Procedures Manual, Section 18.3.6.

12.3.3 III (a) vi. Storage and Preservation of Government Records

Records are preserved most effectively and economically when preservation best practices are used throughout the entire records lifecycle. Government records must be handled and stored in a manner that ensures that they remain accessible, authentic and reliable for as long as they are required to support government business and accountability needs.

Ministries must ensure that records of long-term, enduring or archival value are retained in formats and media appropriate for the entire records lifecycle. These include government records that have been scheduled for transfer to the government archives, but are still in the physical and legal custody of a ministry or agency.

The Information Access Operations Records Management Branch provides cost-effective, environmentally controlled and secure offsite storage, retrieval and final disposition services for ministries' semi-active and inactive records.

12.3.3 III (a) vii. Financial Records

Policies related to the management of financial records (see the Core Policy and Procedures Manual, Section 18.3.5) are supported by the Administrative Records Classification System (ARCS) and ministry-/agency-specific Operational Records Classification System (ORCS).

a) Administrative Financial Documents

- Ministries are responsible for financial documents generated at the ministry level and are accountable for the retention and retrieval of paper financial documents.
- Ministry Senior Financial Officers are responsible for original paper financial documents, under the functional control of the Ministry Records Officer (MRO). The Senior Financial Officer is accountable for the proper storage, preservation, access, retrieval and disposition of original paper financial documents of the ministry.
- The office of the Senior Financial Officer must be the Office of Primary Responsibility for original paper financial documents, unless this function is delegated and the Office of Primary Responsibility is designated to some other office(s) of the ministry.

DRAFT – CHAPTER 12 SUPPLEMENTAL

- Ministries affected by a program transfer or split must identify the specific time at which responsibility for the retention of paper financial documents for the program must also be transferred. The ministry formerly responsible for a program must normally continue to administer documents created prior to the transfer and must provide the successor ministry with financial documents upon request. The successor ministry must respond to inquiries under the *Freedom of Information and Protection of Privacy Act*.

b) Storage

- Ministries may use their own storage facilities or those of private sector firms during the active storage period. For semi-active records, ministries must use facilities administered by the GCIO.
- Ministries must use facilities administered by the Information Access Operations Records Management Branch.
- Paper financial documents on facsimile paper other than plain bonded paper must be photocopied for purposes of retention.

c) Access and Retrieval

- Access and retrieval practices, including retrieval times from onsite and offsite storage facilities, for paper financial documents must conform to standards established by the CIMB.
- Original paper financial documents must not leave the control of the ministry except for requests from the following:
 - Office of the Comptroller General
 - Office of the Auditor General
 - Office of the Ombudsman
 - Office of the Information and Privacy Commissioner
 - Public Accounts Committee of the Legislative Assembly
 - Courts of law.

These entities must be responsible for original documents in their possession and must obtain copies or view originals at the ministry's premises where practicable. Requests from the Public Accounts Committee must be made through the Office of the Comptroller General. The ministry must provide all other users with copies unless an original is required by law.

- Ministries must retrieve and deliver paper financial documents stored in onsite facilities within the following time periods of receiving a request:
 - Where the document and the requester are located in the same city:
 - Regular: 24 hours
 - Emergency: 4 hours
 - Otherwise:
 - Regular: 48 hours
 - Emergency: 24 hours
- Ministries must retrieve and deliver paper financial documents stored in offsite facilities within the following time periods of receiving a request:

DRAFT – CHAPTER 12 SUPPLEMENTAL

- Where the document and the requester are located in the same city:
- Regular: 24 hours
- Emergency: 4 hours
- Otherwise:
- Regular: 72 hours
- Emergency: 24 hours

12.3.3 III (a) viii. Access to Information by the Office of the Auditor General

The Auditor General is an Officer of the Legislature, independent from government, with authority to obtain information to carry out the mandate of the office. The Auditor General is directly entitled to access to information under Section 16 of the *Auditor General Act*. Any concern about access to personal information by the Auditor General needs to be directed to a ministry director/manager of Information and Privacy. The disclosure of personal information that may be contained in the requested records is authorized under Section 33.2 (f) of the *Freedom of Information and Protection of Privacy Act*.

If a ministry in possession of information requested by the Auditor General is unsure whether or not public interest immunity or solicitor-client privilege applies to that information, the ministry should consult with the Office of the Government CIO and obtain legal advice from Legal Services Branch, Ministry of Attorney General.

If information requested by the Auditor General is subject to public interest immunity or solicitor-client privilege, refer to specific guidance in Section 18.4.2 of the Core Policy and Procedures Manual.

Standards:

ISO 15489-1:2001 Records Management – Part 1: General

ISO/TR 15489-2:2001 Records Management – Part 2: Guidelines.

Guidelines:

Guide to the Freedom of Information and Protection of Privacy Act

Exemptions:

- Government records that are not covered by the provisions of the *Document Disposal Act* include:
 - Operational records of the Officers of the Legislature including the Auditor General, the Ombudsman, the Information and Privacy Commissioner, and the Conflict of Interest Commissioner. The administrative records of these Officers, and their offices, fall under the provisions of the *Freedom of Information and Protection of Privacy Act* (FOIPP Act).
 - Records created or accumulated by agencies established under legislation that specifically exempts them from the provisions of the Document Disposal Act.
 - Records created or accumulated by agencies that are deemed to be outside the *Document Disposal Act*'s definition of a "ministerial office".
- Non-government records include records created or accumulated by Members of the Legislative Assembly (MLAs) acting in that capacity, or in their capacity as members of

DRAFT – CHAPTER 12 SUPPLEMENTAL

a political party. These records are not subject to the provisions of the Document Disposal Act or the *Freedom of Information and Protection of Privacy Act*. These records must always be managed separately from government records.

To determine whether an agency is covered by the Document Disposal Act, contact the Ministry Records Officer or the Information Access Operations Records Management Branch.

Contact:

Ministry Records Officers

Information Access Operations Records Management Branch

Metrics and Enforcement:

None identified at this time.

References:

Document Disposal Act

Electronic Transactions Act

Freedom of Information and Protection of Privacy Act

DRAFT – CHAPTER 12 SUPPLEMENTAL

Office of the Chief Information Officer Province of British Columbia	Effective Date: Scheduled Review:
12.3.3 Information Management	
12.3.3 III Managing Information	
12.3.3 III (b) Classification, Scheduling and Maintenance of Government Records	
From Chapter 12, Core Policy and Procedures: <ol style="list-style-type: none">1. Ministries must implement and maintain the government standard records classification and scheduling systems (i.e., ARCS, ORCS, Ongoing Records Schedules).2. Ministries must develop records classification systems for their operational records (ORCS).3. Ministries must use the government standard Enterprise Document and Records Management System when implementing an electronic document and records management system.4. Government records must remain authentic, reliable and accessible after any conversion or migration from one medium, format or system to another.	

Section Contents:

- 12.3.3 III (b) i. Implementing Standard Classification and Scheduling Systems
- 12.3.3 III (b) ii. Developing ORCS
- 12.3.3 III (b) iii. Conversion of Recorded Material

Purpose:

To ensure government records are classified, managed and scheduled in accordance with government standards.

12.3.3 III (b) i. Implementing Standard Classification and Scheduling Systems

Records must be classified and scheduled using the government-wide Administrative Records Classification System (ARCS) and program-specific Operational Records Classification System (ORCS). Some records may be managed under Ongoing Records Schedules (ORS), one-time records schedules, and government-wide special schedules.

The records classification and scheduling systems must be used to manage government records in all media (e.g., paper, electronic, film, tape, CD, PDF, tiff, mpeg). For example, ministry email records and related attachments must be classified and retained in accordance with the retention periods mandated either in ARCS or in the approved ministry ORCS or ORS.

Ministries must establish procedures for implementing ARCS and ORCS and maintaining records in accordance with government standards.

DRAFT – CHAPTER 12 SUPPLEMENTAL

Ministries are responsible for establishing implementation policies and procedures when implementing the standard government Enterprise Document and Records Management System. Examples include the assignment of access privileges, file naming conventions, conversion of existing records to the Enterprise Document and Records Management System, and off-site and disposition procedures for physical and electronic Enterprise Document and Records Management System files.

See the Recorded Information Management (Recorded Information Management) Manual policies pol01-01 Government Records and pol01-04 Distinction between Administrative and Operational Records, and related policies.

See also ARCS Online 'How to Use' and individual ministry ORCS 'How to Use' sections.

12.3.3 III (b) ii. Developing ORCS

The Information Access Operations Records Management Branch establishes government standards for the development, review and maintenance of Operational Records Classification Systems (ORCS). Ministries must keep their ORCS up-to-date to reflect organizational and functional changes, current government and ministry recordkeeping standards, and the evolving nature of modern records.

See Recorded Information Management Manual policy pol02-07 Review and Approval of Records Retention and Disposition Schedules under the Document Disposal Act and Standard ORCS Kit - 2001 (Guidelines).

12.3.3 III (b) iii. Conversion of Recorded Material

Program areas must contact their Ministry Records Officer at the planning phase of the project in order to request revised or new records retention and disposition schedules.

The conversion of records to a different medium must be documented in an approved schedule before the original before the original can be sent for final disposition. Information Access Operations Records Management Branch archivists must establish the final disposition for all converted records of enduring value prior to implementation of the conversion project.

See Recorded Information Management Manual policies: 5-10-02 Microfilm as Documentary Evidence; and 5-06-03 Microform Storage.

See also Standard ORCS Kit - 2001 (Guidelines).

Standards:

Administrative Records Classification System: ARCS Online

Operational Records Classification Systems: Standard ORCS Kit - 2001

Special schedules – ARCS Online: Records Schedules for Special Categories of Records

Government Standard for Enterprise Document and Records Management

Recorded Information Management Manual policy: 5-10-02 Microfilm as Documentary Evidence.

DRAFT – CHAPTER 12 SUPPLEMENTAL

Guidelines:

None identified at this time.

Contact:

Ministry Records Officers

Metrics and Enforcement:

None identified at this time.

References:

None identified at this time.

DRAFT – CHAPTER 12 SUPPLEMENTAL

Office of the Chief Information Officer Province of British Columbia	Effective Date: Scheduled Review:
12.3.3 Information Management	
12.3.3 III Managing Information	
12.3.3 III (c) Storage and Disposition of Government Records	
<p>From Chapter 12, Core Policy and Procedures:</p> <ol style="list-style-type: none">1. Government records must be disposed of securely in accordance with approved records retention and disposition schedules and asset management processes.2. Ministries must establish internal records disposition procedures.3. Government records scheduled for archival retention must be maintained in a manner that preserves their integrity and authenticity up to and throughout transfer to the government archives.4. Government records scheduled for destruction must be destroyed in a method appropriate for the recording media and that maintains the security of the information and the privacy of individuals.	

Section Contents:

- 12.3.3 III (c) i. Authority to Apply Final Disposition to Government Records
- 12.3.3 III (c) ii. Establishing Ministry Disposition Procedures
- 12.3.3 III (c) iii. Preserving Records until Final Disposition
- 12.3.3 III (c) iv. Secure Confidential Destruction of Eligible Government Records

Purpose:

These procedures ensure:

- Final disposition is applied to government records once their active and semi-active retention periods expire;
- Final disposition of government records is authorized and documented in accordance with established standards; and,
- Records eligible for destruction are destroyed in a secure and confidential manner appropriate to the media and information content.

12.3.3 III (c) i. Authority to Apply Final Disposition to Government Records

Final disposition of government records requires the authorized application of an approved record retention and disposition schedule (ARCS, ORCS, ORS, special or one-time schedules).

Final disposition actions cannot take place until the expiration of the approved active and semi-active retention periods.

Records eligible for final disposition must not be disposed of if they are identified as relevant during any of the following:

DRAFT – CHAPTER 12 SUPPLEMENTAL

- a litigation document discovery process;
- an inquiry under the *Inquiry Act*;
- a request for information under the *Freedom of Information and Protection of Privacy Act*; or
- in any other extraordinary situation (e.g., a criminal investigation).

Scheduled final disposition action must be suspended until the recorded information is no longer required for the purposes described above. Records Officers must ensure that disposition holds are applied to all relevant records regardless of where they are stored (e.g., onsite, offsite, electronic information stored on Local Area Networks, Enterprise Document and Records Management Systems or other information systems); their format (e.g., email, word processing documents, electronic images); or the physical media they are stored on (e.g., paper, microfilm, magnetic tape, CD).

See the Recorded Information Management (RIM) Manual policy 02-04, section 4.1.1, for additional information on requesting holds on scheduled final disposition.

See also Recorded Information Management Manual, policy pol02-03 Authority to Apply Records Schedules.

12.3.3 III (c) ii. Establishing Ministry Disposition Procedures

Ministries must establish procedures to authorize, administer and document final disposition actions applied to their records. Disposition procedures must include instructions for all types of government records, regardless of storage media or formats.

See Recorded Information Management Manual policy pol02-04 Disposition of Government Records.

12.3.3 III (c) iii. Preserving Records until Final Disposition

Ministries will retain and appropriately manage government records throughout each record's lifecycle.

Records of enduring value must be retained, preserved and remain accessible until such time as they are transferred to the legal custody of the government archives.

Ministries must put procedures in place to ensure that electronic records of enduring value are preserved and remain accessible throughout the lifecycles of the information, the systems (hardware and software), and media. For example, Ministry A may establish procedures for printing email messages and attachments to paper and filing them in the appropriate hard copy file, while Ministry B requires the transfer of email messages and attachments into an Enterprise Document and Records Management System.

12.3.3 III (c) iv. Secure Confidential Destruction of Eligible Government Records

Government records eligible for destruction must be destroyed using a method that maintains the security and confidentiality of the information. The method of destruction must be appropriate to

DRAFT – CHAPTER 12 SUPPLEMENTAL

the record media, insuring that that the information is completely obliterated and can neither be recreated nor retrieved.

See Recorded Information Management Manual policies pol02-02 Destruction of Government Records; and pol02-04 Disposition of Government Records.

Standards:

None identified at this time.

Guidelines:

Information Security Policy – section 6.7 Media handling
Privacy Breach Guidelines

Exemptions:

- Government records that are not covered by the provisions of the *Document Disposal Act* include:
 - Operational records of the Officers of the Legislature including the Auditor General, the Ombudsman, the Information and Privacy Commissioner, and the Conflict of Interest Commissioner. The administrative records of these Officers, and their offices, fall under the provisions of the *Freedom of Information and Protection of Privacy Act* (FOIPP Act).
 - Records created or accumulated by agencies established under legislation that specifically exempts them from the provisions of the Document Disposal Act.
 - Records created or accumulated by agencies that are deemed to be outside the *Document Disposal Act*'s definition of a "ministerial office".
- Non-government records include records created or accumulated by Members of the Legislative Assembly (MLAs) acting in that capacity, or in their capacity as members of a political party. These records are not subject to the provisions of the *Document Disposal Act* or the *Freedom of Information and Protection of Privacy Act*. These records must always be managed separately from government records.

To determine whether an agency is covered by the Document Disposal Act, contact the Ministry Records Officer or the Information Access Operations Records Management Branch.

Contact:

Ministry Records Officers

Information Access Operations Records Management Branch (disposition and off-site storage of government records)

Metrics and Enforcement:

Ministries must monitor and report on serious breaches of recorded information management policy (e.g., damage, theft, misuse, unauthorized disposition) to the Ministry Records Officer, Ministry Security Officer and the Director, Information Access Operations Records Management Branch.

References:

DRAFT – CHAPTER 12 SUPPLEMENTAL

Asset Disposal Handbook

Core Policy and Procedures Manual:

Chapter 6, Section 6.3.4. d. Disposal of Surplus Assets;

Chapter 8, sections 8.2 and 8.3 Asset Management; and,

Chapter 20, Loss Management.

Document Disposal Act

Freedom of Information and Protection of Privacy Act.

KEY RECORDS DEFINITIONS

Personal and MLA Records

Personal records are personal in nature and relate to one's private life and are not received or created as part of one's daily ministry business activities. These would include: personal invitations, communications with family and friends containing no government business, personal photographs.

Member of the Legislative Assembly (MLA) records include records created, accumulated and used by a Minister while acting in that capacity (excluding any records of an MLA's role as a cabinet minister). This includes records of legislative and political activities (i.e., legislative records) and records relating to liaising with constituents or constituency offices (i.e., constituency records).

Examples include:

- Documentation relating to caucus meetings and responsibilities
- Political party communications
- Communications (emails, letters, faxes, reports, submissions, photographs, media contact) from constituents either about a local issue or expressing their concerns or opinions about government direction (provided it does not relate to the Ministerial function)
- Communication with an MLA or cabinet minister regarding a constituent or a constituency issue
- Speeches and meetings with constituents while conducting MLA business

Government Records (non-Cabinet)

Government records are all recorded information regardless of physical format which is created, received, deposited or held by, or in, any Ministry. Government records are subject to the *Document Disposal Act* (RSBC 1996, c. 99), Core Policy and Procedures Manual (chapter 12), and approved records schedules.

Government records relate to the mandate and legislation of the ministry.

Once Cabinet, personal and MLA records have been removed, the records remaining in a minister's office are the records that the minister and minister's staff have accumulated in the course of the daily administration of a ministry.

For information on dealing with government email see the GRS online Email Management Guides: http://www.gov.bc.ca/citz/iao/records_mgmt/guides/email_mngt.html.

GOVERNMENT RECORDS SERVICE GUIDE

Cabinet Records

Cabinet records are a sub-category of government records and are considered privileged information of the government of the day. A succeeding administration of a different political party does not have access to them. This protects the confidentiality of the collective decision-making process of the responsible government.

Cabinet records are government records and are subject to the *Document Disposal Act*, Core Policy, and approved records schedules. Most Cabinet records will be classified under ARCS primaries 201 (Cabinet Submissions), 324 (Speaking notes for Cabinet presentations), and 280 (Briefing notes about Treasury Board or Cabinet submissions). See ARCS for more information: <http://www.gov.bc.ca/citz/iao/arcs/index.html>.

Cabinet records include: memoranda, submissions, reports, recommendations, agendas, minutes, notes, and other confidential papers, audio-visual and presentation material that reflect on the decisions or discussions of Cabinet and its committees, and includes, briefing notes, opinions, and advice to Ministers and correspondence between Ministers expressing their views and opinions and other documents reflecting such views and opinions.

Transitory Records

Transitory records are records of temporary usefulness that are not integral to an administrative or operational record series. Transitory records are not regularly filed within a standard records classification system, and are only needed for a limited period of time for completion of an action or preparation of a document. These records are not required to meet statutory obligations or to sustain administrative or operational functions. Transitory records are covered by special records schedules.

See Special Schedule for Transitory Records 102901:
http://www.gov.bc.ca/citz/iao/records_mgmt/special_schedules/transitory_records.html

For related guidelines on email management, including transitory emails, see:
http://www.gov.bc.ca/citz/iao/records_mgmt/guides/email_mngt.html

For further information see the GRS Website:
http://www.gov.bc.ca/citz/iao/records_mgmt/index.html

TRANSITORY RECORDS

Many records do not need to be retained. The Transitory Records Schedule authorizes you to dispose of records of temporary value as soon as their business use ends. This guide will help you identify these records.

What is a transitory record?

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

As with all records, they can exist in **any format or medium** (paper or electronic), and can be created and shared using a variety of technologies (e.g., email, social media, Live Meeting, SharePoint, wikis).

Transitory records **are not required** for financial, legal, audit or statutory purposes and are not regularly filed in the office recordkeeping system.

They do not need to be filed using the *Administrative Records Classification System (ARCS)* or your office's *Operational Records Classification System (ORCS)*.

Examples of transitory records:

- advertising material
- announcements of social events
- cc copies (unless you are the main staff member responsible for the matter)
- copies created for convenience/reference purposes
- email conveying an attachment (providing it doesn't add value to the attachment)
- meeting arrangements
- personal messages
- simple messages reflecting commonplace interactions (e.g., a request to call someone)
- outlines, calculations, preliminary notes and other rough content used to prepare a final record
- drafts and revisions that are not needed to document decisions and associated approvals
- routine correspondence about drafts and revisions

See the Quick Reference Guide on last page for more examples.

Who can apply this schedule?

You can! You simply need to use your judgment to determine whether a record is, or is not, transitory. The authority to identify transitory records is delegated to each BC government employee.

However: DO NOT destroy any transitory records that are relevant to a FOIPPA request or legal discovery.

GOVERNMENT RECORDS SERVICE GUIDE

TRANSITORY RECORDS

What isn't a transitory record?

A record's content and context determines whether it is transitory, not its format or storage medium. If an email, significant draft, or other record is essential to understanding government business, e.g., how a particular decision was reached, then the record is non-transitory and must be kept.

Non-transitory records need to be filed and saved in accordance with the appropriate government records schedule (i.e., *ARCS/ORCS* classification).

Examples of non-transitory records:

- work unit activities documentation (e.g., work schedules, assignments, etc.)
- useful information that helps explain the history of a relationship, decision or project
- drafts or revisions with information about a decision or associated approvals that is unavailable elsewhere (e.g., directions to change a proposal and recommend a different course of action)
- a final report with recommendations
- formal communication about official business
- policies and directives
- decision records, instructions, and advice
- meeting agendas and minutes
- documentation of a policy matter or how a case was managed
- documentation of initiation, authorization, or completion of business transactions
- documentation that is evidence of a significant action (e.g., verification or approval to proceed)

Why Managing Transitory Records Is Important

By promptly removing transitory records, employees are better able to identify and file key records into their office recordkeeping system, where they can be easily found. As well, government avoids unnecessary costs for storing and processing transitory records.

Additional Information

Contact your [Records Officer](#) or check out the other [RM Guides](#).

TRANSITORY RECORDS

Quick Reference Guide to Transitory Records

	WHAT	SHORT DEFINITION	EXAMPLES
1.	Records of Short-term Use	Records created or received for informational purposes only; OR convenience copies for reference or ease of use (i.e., the official copy has been filed in the <u>office recordkeeping system</u>)	<ul style="list-style-type: none"> Messages (e.g., email, voicemail, instant messages) that are not required to document a decision, action, or transaction Duplicate copies, partial copies or extracts no longer needed for reference purposes Input source documents no longer required
2.	Working Materials, Drafts, and Revisions	Preliminary versions and supplementary documentation used to prepare a final document, which DO NOT indicate new decisions or provide approvals and are not specified in another records schedule (e.g., <u>ARCS</u> or your <u>ORCS</u>)	<ul style="list-style-type: none"> Drafts and revisions that provide no information on decisions or approvals that cannot be found elsewhere Rough notes, calculations, outlines, lists of ideas or suggestions Newspapers or magazines used for compiling daily 'news clippings' (physical or electronic)
3.	Advertising and Promotional Material from the Private Sector	Advertising and promotional material from businesses or business professionals which DOES NOT relate to a transaction with a private sector provider	<ul style="list-style-type: none"> Company profiles, pamphlets Direct mail/email notices and bulletins Catalogues Free trial CDs and DVDs Course and seminar announcements
4.	Supplies of BC Government Publications and Blank Forms	Stocks of publications and blank forms which have no further usefulness	<ul style="list-style-type: none"> Blank forms, including blank e-forms and e-templates Blank stationary with out-of-date information Out-of-date published material (e.g., pamphlets, brochures, and newsletters)

Dispose of Transitory Records as soon as you are finished with them!

Managing Government Records During Interregnum and Transition

Government Records Service

March 28, 2013

Parliamentary Timelines

- Writ issued – April 16, 2013
- Lieutenant Governor dissolves the Legislative Assembly
- Interregnum period - Government is in a caretaker period
- Ministers continue to hold Cabinet positions until a new Cabinet is sworn in
- Transition period - day after the election until new Cabinet is sworn in

Parliamentary Conventions

- During the interregnum and transition periods, management of Minister's office records must respect the Parliamentary tradition of privilege for all Cabinet Records
- Cabinet records are removed from Minister's office and placed under control of the Deputy Minister

Shared Responsibilities

- Deputy Minister's office – during interregnum and transition periods control Cabinet and Government records of Ministers' offices
- Minister's office – organize and manage according to records management policy and procedures
- Government Records Service – provide policy direction and practical guidance

What is a “Record”

- A record is **any** information recorded by any means, electronic or physical
- This includes all documents and communications such as email, letters, and reports, that are created or received

Transitory Records

- Are records of temporary usefulness not required to document decisions and actions or to support ongoing government business (see handout)
- Should be regularly deleted as their usefulness ends (e.g. transitory emails of no further use can be deleted as you work through the following procedures)
- Does not apply to personal or MLA records

Minister's Office Records

- Categories:
 - Personal and MLA records
 - Cabinet records
 - Government records
- Cabinet and Government records must be retained and managed according to government retention schedules and policies

Personal and MLA Records

- Are to be separated from Cabinet and Government records **PRIOR** to interregnum
- Are not covered by the *Document Disposal Act*
- Are not covered by the Executive Records Schedule

Personal Records

Personal in nature:

- Relate to the MLA's private life
- Not received or created as part of the MLA's daily ministry or constituent business activities
- Examples include: personal invitations, communications with family and friends that contain no government business

MLA Records

MLA records reflect, for example:

- Constituency operations
- Constituency meetings
- Caucus committee meetings
- Committees of the Legislative Assembly

Procedures - Personal and MLA Records

Electronic records:

- If the Minister wishes
 - Print to hard copy, or
 - Copy to CDROM or other removable memory device

Records must be removed from the Minister's office computer libraries and files

Procedures - Personal and MLA Records

Paper Records:

- Minister may provide direction on shipping to a location of the Minister's choice
- Minister may choose to have records stored by Government until the Minister arranges for shipping to an alternate location (handout available)
 - Ask your DMO for assistance
 - After 5 years the Minister may request the records be transferred to the custody and control of the BC Archives

Must be separated from Cabinet and Government records prior to the interregnum.

Definition - Cabinet Records

Anything that reflects the decisions or discussions of Cabinet or its committees

Anything that expresses views or opinions on a Cabinet issue that is communicated to or among Ministers

Examples - Cabinet Records

- Audio visual and presentation materials
- Confidential papers
- Notes
- Opinions
- Advice to Ministers
- Correspondence between Ministers
- Memoranda
- Submissions
- Draft Submissions
- Reports
- Recommendations
- Agendas
- Minutes
- Records of Decision

Not media specific

Procedures - Cabinet Records

Identify all Cabinet documents in Minister's office

All Cabinet documents are placed in a secure location under the control of the Deputy Minister as soon as possible after the writs have been issued and no later than the end of the interregnum

- Paper copies:
 - Isolate all documents
 - Work with your DM office to arrange physical transfer
- Electronic copies:
 - Work with your DM office in removing Minister's office access to the electronic files
 - Access must be restricted to the DM office

Government Records

- Records that the Minister and Minister's staff have accumulated in the course of the daily administration of a ministry
- In other words, the records remaining in a Minister's office, once Cabinet, personal and MLA records have been removed

Examples - Government Records

- Ministerial correspondence
- Copies of incoming/
outgoing MRLs
- Meeting minutes with
ministry Executive and staff
- Meeting minutes re ministry
business with a stakeholder
- Policy decisions
- Briefing notes
- Ministerial invites & regrets
- Ministerial presentations &
speeches
- Financial – payables
procurement, travel
- Ministerial meetings
- Outlook or other calendars
- Mail logs

Procedures - Government Records

This is the responsibility of the Minister's office:

- All Government records must be managed according to normal records management policies and procedures
- Government records must be classified according to ARCS and ORCS classification systems
- The legislatively approved Executive Records Retention schedule applies
- Minister's calendars, for the duration of the Minister's term, must be output and filed (e.g. printed to hard copy or PDF)

Document Destruction

- During the interregnum period, all commercial document shredding for Ministers' offices within the Legislative Precinct is to be suspended.

Resources - Handouts

- Presentation slides
- Your Records Management Contacts
- Key Records Definitions
- Forms to transfer personal and MLA records to the BC Archives
 - Archival Agreement
 - Archival Deposit Decision

Online Records Management Resources

Government Records Service website:

http://www.gov.bc.ca/citz/iao/records_mgmt/index.html

Records Officers/Teams contacts:

http://www.gov.bc.ca/citz/iao/records_mgmt/rec_officers/

Forms for MLA records transfers:

http://www.gov.bc.ca/citz/iao/records_mgmt/rcs/index.html

Government records schedules (ARCS & ORCS and Special Schedules): http://www.gov.bc.ca/citz/iao/records_mgmt/arcs_orcs/

Definitions:

http://www.gov.bc.ca/citz/iao/records_mgmt/policy_standards/rim_manual/glossary.html

GOVERNMENT RECORDS SERVICE GUIDE

YOUR RECORDS MANAGEMENT CONTACTS

To arrange transfer of member's personal and MLA papers contact: **Alexander Wright**,
Director, Government Records Service (GRS) – Alexander.Wright@gov.bc.ca;
Phone: 250-588-4057

Records Officers/Teams Providing Services to:

Advanced Education, Innovation and Technology

Education

Health

Terrence McKenny – RMHELP.HealthEducation@gov.bc.ca; Phone: 250-387-9811

Citizens' Services and Open Government

Office of the Premier

BC Public Service Agency

Government Communications and Public Engagement

Bea Nacey – RMHELP.CentralAgencyOP5@gov.bc.ca; Phone: 250-387-4594

Community, Sport and Cultural Development

Finance

Jobs, Tourism and Skills Training

Transportation and Infrastructure

Blair Turner – RMHELP.BUSINESS@gov.bc.ca; Phone: 250-356-7507

Justice and Attorney General

Children and Family Development

Social Development

Roxanne Weeds – RMHELP.Justice.Social@gov.bc.ca; Phone: 250-356-5858

Aboriginal Relations and Reconciliation

Agriculture

Energy, Mines and Natural Gas

Environment

Forests, Lands and Natural Resource Operations

Jeff Barber – RMHELP.RESOURCES@gov.bc.ca; Phone: 250-356-9153

Broader Public Sector, Client Relations Specialist

Mike Lauzon – Mike.Lauzon@gov.bc.ca; Phone: 250-356-2503

GRS Website: http://www.gov.bc.ca/citz/iao/records_mgmt/rec_officers/

GOVERNMENT RECORDS SERVICE GUIDE

KEY DEFINITIONS


Personal and MLA Records

Personal records are personal in nature and relate to one's private life and not received or created as part of one's daily ministry business activities. These would include: personal invitations, communications with family and friends containing no government business.

MLA records include records created and accumulated and used by an MLA acting in that capacity. This includes records created by a Minister while acting as an MLA, such as carrying out constituency operations, e.g., liaising with constituents or constituency offices.

Examples include:

- Communications (emails, letters, faxes, reports, submissions, photographs, media contact) from constituents either about a local issue or expressing their concerns or opinions about government direction (provided it does not relate to the Ministerial function.)
- Communication with an MLA or cabinet minister regarding a constituent or a constituency issue.
- Speeches and meetings with constituents while conducting MLA business.



BRITISH COLUMBIA

[Advanced Search](#) | [Help](#) | [Contact Us](#)

Text Size **AA**

[All B.C. Government](#)
[ARCS Online](#)

[News](#) | [The Premier](#) | [Ministries](#) | [Apply for a Job](#) | [Bid on a Contract](#) | [Main Index](#)

[SHARE](#)

[B.C. Home](#) | [Citizens' Services and Open Government](#) | [Information Access Operations](#)

[Printer Version](#)

Ministry of Citizens' Services and Open Government

Government Records Service

Information Access Operations Branch, Government Records Service supports a government-wide framework for the management of recorded information. This framework includes policies, standards and strategic direction for the creation, security, accessibility, retention, disposition and preservation of records.

The branch provides central records management support services to ministries, Crown Corporations and agencies including:

- Advisory services
- Contracted records storage
- Centralized records management training
- Operational Records Classification System (ORCS) development
- Administrative Records Classification System (ARCS) development and maintenance
- Archival appraisal
- Enterprise Document and Records Management System (EDRMS) implementation
- Records management systems administration

ARCS Online

USEFUL LINKS

[Forms](#)

[ORCS](#)

[RIM Glossary](#)

[Special Schedules](#)

[B.C. Home](#)

[Ministry of Citizens' Services and Open Government](#)

[Information Access Operations](#)

[Freedom of Information](#)

[Managers, Information Access](#)

[Records Management](#)

[ARCS/ORCS](#)

[Special Schedules](#)

[Records Officers](#)

[Records Transfer and Storage](#)

[Policy & Standards](#)

[EDRMS/TRIM](#)

[EDRMS Support Desk](#)

[Training](#)

[RM Guides](#)

[CRMS](#)

[ARCS Online](#)

[RELATED LINKS](#)



TRANSFER AGREEMENT

GRS USE ONLY

- Application Number: _____
- Accession Number: _____

This is an Agreement between _____, Member of the Legislative Assembly for the Electoral District of _____ [hereinafter known as the "Member" or the "owner of the records"], of the first part, and Government Records Service (GRS), Information Access Operations, Shared Services BC, Ministry of Citizens' Services, and Open Government of the second part.

This Agreement provides for the orderly transfer, storage and retrieval of the Member's semi-active and inactive records to and from off-site storage during the Member's current term of office, including a grace period of up to thirty days following cessation of membership in the Legislative Assembly. An existing transfer agreement for a Member shall be automatically extended at the beginning of each Parliament, unless GRS is notified in writing by the Member.

The parties agree:

1. ~~that~~ those semi-active or inactive records designated by the Member for transfer to Government Records Service shall receive off-site storage and retrieval services;
2. ~~that~~ these services will continue to be provided until 31 December following the fifth anniversary of the owner's ceasing to be a Member of the Legislative Assembly, with the exception that courier or postal delivery will be provided at cost;
3. ~~that~~ six months prior to the expiry of the time stipulated above, the owner of the records will complete an Archival Deposit Decision indicating one of the following final dispositions for the records:
 - a) ~~transfer~~ to the custody of Archives of the Province for archival appraisal and selective retention under access conditions negotiated between the former Member and the Archives;
 - b) ~~destruction~~ of the records in a secure and confidential manner;
 - c) transfer at the expense of GRS to any British Columbia address designated by the former Member which will terminate any obligation the government may have had towards those records; or,
 - d) ~~transfer~~ to another archival repository as designated by the former member and agreed to by the archival repository.
4. ~~that~~ records designated for transfer to the custody of the Archives of the Province will be reviewed for archival value and that records not selected for archival retention will be returned to the former Member or, with Member's approval, destroyed in a secure and confidential manner;
5. ~~that~~ should a completed Archival Deposit Decision not be received by GRS by 31 December following the fifth anniversary of the owner's ceasing to be a Member of the Legislative Assembly, the records shall be transferred to the legal custody of the Archives of the Province and an archival appraisal and selection shall be made. The selected records shall be held there, closed to public access for a maximum of twenty years after the death of the owner, at which time they will be opened for public access. Access to personal information will be governed by guidelines and regulations for access and individual privacy.

MEMBER SIGNATURE

DATE

MILITARY TRANSFER AGREEMENT / ARCHIVAL DEPOSIT DECISION

AMS 408 / 409

ARCHIVAL DEPOSIT DECISION

ARMY USE ONLY

- Application Number: _____
- Accession Number: _____

_____, formerly Member of the Legislative Assembly for _____

_____, acknowledge that the Transfer Agreement between myself and Government Records Service (GRS) expires on 31 December 20____, and I hereby choose the following final disposition for the records covered by that Agreement.

(Please indicate with a check in the appropriate box the clause of your choice, and sign on the line below.)

☐

- a) Transfer of the records to the custody of the British Columbia Archives, Royal British Columbia Museum (RBCM) for archival appraisal and selective retention under access conditions to be negotiated between myself and RBCM, hereby giving physical ownership of the records and all associated rights (including copyright where owned by me) to RBCM.

I would like any records not selected for archival retention to be (choose one):

- ☐ Destroyed securely and confidentially
☐ Transferred to: _____

☐

- b) Destruction of the records in a secure and confidential manner.

☐

- c) Transfer of the records at the expense of Government Records Service to any British Columbia address designated by me which will terminate any obligation the government may have had towards those records.

I would like the records sent to: _____

☐

- d) Transfer of the records to another archival repository which has agreed to receive them.

I would like the records sent to: _____

I further agree that this archival deposit decision shall come into force on 31 December 20____. Should Government Records Service not receive a reply by that date, the records will, according to the Transfer Agreement, be transferred to the legal custody of the British Columbia Archives, Royal British Columbia Museum.

Questions ??

Logistics and Business Services

RECORDS MANAGEMENT AND FREEDOM OF INFORMATION

Presented April 2015



FREEDOM OF INFORMATION

1. The Act
2. Records Management
3. How the FOI Process Works

PURPOSES OF THE ACT

Accountability

Right of access to
records



Privacy

Prevent unauthorized
collection, use or
disclosure of personal
information

Independent oversight



PURPOSES OF THE ACT

Accountability to the Public

- Legislated right to access all government records - specifying limited exceptions (i.e. make what is commonly referred to as an 'FOI request').
- Independent review of the decisions made under the Act (OIPC).

Protection of Privacy

- Provides a right of access to individuals own personal information.
- Regulates how public bodies collect, use and disclose personal information.
- Right to request correction of personal information.



ENTITIES COVERED BY THE ACT

All provincial ministries, and most provincial agencies, boards, commissions, Crown Corporations and smaller agencies.

Local Public Bodies

- School districts, colleges and universities
- Regional health boards

Self-Governing Professions and Occupations

- Teachers
 - Doctors
 - Nurses
- Government is only responsible for requests to BC government ministries
- NOT MLA offices, Speaker's office, Crowns, etc.



WHAT RECORDS ARE COVERED BY THE ACT

All records in the **custody** or under the **control** of a public body.

What is a Record?

- Any information recorded or stored **by any means whether in hard copy or in electronic format.**
- Regardless of content and subject matter, the following are subject to an FOI request:
 - briefing notes
 - vouchers
 - telephone records
 - notebooks/daybooks
 - contractor records
 - email
 - records on your smart phone
 - transitory records



RECORDS MANAGEMENT

Records created or received while doing Government business must be managed according to legislation, litigation requirements and Government policy and are subject to FOI and Government policy regardless of where they are located.

- Government **email** must be conducted using approved Government email systems, not personal email systems. This is essential for information security, privacy protection and effective management of the information.
- Government records that are **not transitory** should be filed in the office's record-keeping system (e.g., TRIM or LAN) and must not be destroyed without an approved schedule (e.g., ARCS/ORCS) or before the schedule allows.
- Employees must keep Government records separate from material relating to ministers' **constituency matters**, legislative committee involvement and other MLA activities. Those, and personal (e.g., family) records, are not Government records.

RECORDS SCHEDULES

- Executive records schedule includes all government business of ADMs and above, including Ministers' offices.
- Retention period for executive records is typically 10 years after business use has ended.
- ARCS are administrative records common to all program areas (e.g., competition files, financial information) and the retention period is typically around 7 years.
- ORCS are program specific business records with a retention period typically under 10 years.



TRANSITORY RECORDS

- Are records of **temporary usefulness** not required to document decisions and actions or to support ongoing government business.
- Should be **regularly deleted** as their usefulness ends (e.g., transitory emails of no further use or convenience copies of submission or briefing notes can be deleted).
- The Transitory Records Schedule does not apply to personal or MLA records.

BEST PRACTICES FOR EMAIL

- Use government email accounts for government business.
- Keep email inbox up to date.
- Retain records that document government decisions in your office's electronic filing system – email sender is generally responsible for retaining the original.
- Regularly eliminate transitory records (e.g., personal emails, duplicates, working materials or non-substantive drafts).

WHAT HAPPENS WHEN AN FOI REQUEST IS RECEIVED?

Ministry responsibilities include provision of the following information to IAO:

- where search for records was conducted (i.e. TRIM files, databases off-site records);
- duration of search time by ministry program area;
- who conducted the record search;
- potential **harms** could result from disclosure of records gathered;
- **issues** associated with disclosure of records gathered;
- regional locations where records pertaining to this request may reside.

Mandatory Exceptions

Section 12	Cabinet confidence
Section 21	Third party business information
Section 22	Personal information

Discretionary Exceptions

Section 13	Policy advice/recommendations
Section 14	Legal advice
Section 15	Law enforcement
Section 16	Intergovernmental relations
Section 17	Financial or economic interests
Section 18	Heritage sites
Section 19	Personal health or safety
Section 20	Information soon to be published



SECTION 12

- Section 12 is a mandatory section of the Act that enables Cabinet Committees to discuss issues in confidence.
- The head of a public body (e.g. the DM) must refuse to disclose information that would reveal the **substance** of deliberations (implications, options, advice, etc.) of Cabinet Committees.
- Section 12 does not apply to **background explanations** or analysis to Cabinet **if** the decision has been made public, has been implemented, or five or more years have passed since the decision was made or considered. The 'Substance' still remains withheld.



FOI APPROVAL, PUBLICATION & APPEAL

- FOI requests are sent to program areas (ministries) for review and sign-off.
- The DM or delegated head of the public body exercises discretion with respect to disclosure recommendations.
- The DM or designate signs-off the final version of the request before it is released to the applicant.
- Applicant has the right to appeal to OIPC.
- General FOI requests are posted to the Open Information site.
- It is important to consider that broader release gives more people access to the information in the FOI release.



CONTACTS

Wes Boyd, ADM, Logistics and Business Services	250 508-5791
Brad Williams, Executive Director, FOI	250 387-9807
Chad Hoskins, Senior Director, FOI	250 356-7343

FOI Managers:

<i>Sector</i>	<i>Manager</i>	
Justice/Social	<u>Vicki Hudson</u>	250 356-0845
Central Agencies	<u>Cindy Elbahir</u>	250 952-6355
Natural Resources	<u>Kris Ghag</u>	250 356-5702
Business/Infrastructure	<u>Russ Fuller</u>	250 387-4503
Health/Education	<u>Maxine Vanzetta</u>	250 387-9805
Personals	<u>Vivian McDonald</u>	250 356-6266
Intake/Open Information	<u>Cindy Kukucska</u>	250 387-7356

QUESTIONS ?

FY2014-2015 Overview of Training on the *Freedom of Information and Protection of Privacy Act* (FOIPPA)

Privacy and Legislation Branch						Information Access Operations
Topic	FOIPPA Legislation (Privacy and Access)	PIAs	Info Incidents/Privacy Breaches	BC Privacy Professional Certificate program (in development)	Other	Access only
Session details	Full day FOIPPA session (6 hours, offered routinely 4 times per year in Vancouver and Victoria) Voluntary Target: All government and broader public body staff Attendance: Registration tracked	PIA training (3 hours) Voluntary Target: All government and broader public body staff Attendance: Registration tracked	IM111 - Privacy and Information Sharing: Awareness Training (1 hour, online, available anytime) Mandatory Target: All government staff Attendance: tracked by PSA	Privacy Management Programs and Audits (3 hours) – how to develop, follow, and audit a PMP Voluntary Target: Government, broader public sector Attendance: tracked by OCIO	Appropriate Use (1 hour) Voluntary Target: All government staff Attendance: Not tracked	IAO Conference 1 day of workshops 2 days of presentations Offered once per year in Victoria Voluntary Target: government staff Attendance: Registration tracked
	Dedicated FOIPPA training (1, 2 or 3 hours) Voluntary Target: All government and broader public body staff Attendance:	PIA template and directions training (3 hours) Voluntary Target: Government broader public bodies Attendance: Registration tracked	IM500/550 Privacy and Information Sharing: Awareness Training for Executives (1 hour, online or in person, available anytime) Mandatory Target: All government executive Attendance: tracked by PSA	Privacy Tools – incl. PIAs, ISAs, IPAs, RAs and contracts (3 hours) Voluntary Target: Government, broader public sector Attendance: tracked by OCIO	Internet of Things (30 minutes) Voluntary Target: Government, broader public bodies Attendance: Not tracked	Legislature FOI Training (1hr) Delivered as required generally monthly or as new staff are hired. Mandatory Target: New to leg staff Attendance: tracked by OOP
	Privacy training for IDIM (BC Services Card) (3 hours, offered routinely twice per year) Mandatory for IDIM staff, annually Target: All IDIM staff	Condensed PIA training (30 minutes) Voluntary Target: Government, broader public bodies Attendance: Registration tracked	Dedicated ministry/public body breach training (1.5 hours) Voluntary Target: Government, broader public bodies Attendance: Registration tracked	Other in-depth privacy courses, access/records management and security are being developed	Privacy and Information Sharing for Government Contractors (1 hour, online, available anytime for nominal fee) Mandatory Target: All government contractors handling personal information Attendance: tracked by Open Schools BC	FOI Training to Ministry Executive teams. Annual Voluntary Target: At the discretion of the Ministry Executive
			Security Day presentation (30 minutes) Voluntary Target: security professionals Attendance: not tracked			Program Area Specific FOI & Records Management training. Delivered as and when needed Voluntary Target: Min FOI Staff
Total	894 attendees (17 sessions)	572 attendees (12 sessions)	464 attendees (9 sessions)	106 attendees (2 sessions)	400 attendees (4 sessions)	420 attendees (28 sessions)

¹All training sessions are offered face to face or via LiveMeeting unless otherwise noted.

FY2014-2015 Overview of Records Management Training

Government Records Service					
Topic	Records Management for Administrative Staff with RM responsibilities	Records Management for All Employees	TRIM	CRMS (Corporate Records Management System)	Other
Session details	Orientation to Records management Full day (7 hours, offered monthly in Victoria and 6 – 8 sessions across Province) Voluntary/Highly Recommended Target: All government admin/records management staff Attendance: Registration tracked	Managing Government Records Available on Web (1.5 hours) Voluntary Target: All government and broader public body staff Attendance: Not tracked	TRIM Folder Management Full day (7 hours, offered monthly in Victoria and 6 – 8 sessions across Province) Required for TRIM implemented offices Target: All government admin/records management staff in TRIM implemented offices Attendance: Registration tracked	CRMS Full day (7 hours, offered bi-monthly in Victoria with livemeetings for non-Victoria staff) Voluntary/Highly Recommended Target: Select government admin/records mgmt. staff for offices using CRMS Attendance: Registration tracked	LAN Organization Half day (3.5 hours) offered monthly in Victoria with livemeetings for non-Victoria staff) Voluntary Target: Anyone interested in learning LAN management skills Attendance: Registration tracked
	Records Disposition Processing Full day (7 hours, offered monthly in Victoria and 6 – 8 sessions across Province) Voluntary/Highly Recommended Target: Select government admin/records mgmt. staff in TRIM implemented offices Attendance: Registration tracked	Managing Government Records 1 – 3 hours based on client request Voluntary Target: All government and broader public body staff Attendance: Tracked manually; registration is managed by client	TRIM Disposition Management Full day (6 hours, offered bi-monthly in Victoria and 6 – 8 sessions across Province) Voluntary/Highly Recommended Target: Select government admin/records mgmt. staff in TRIM implemented offices Attendance: Registration tracked		Managing Calendars 2 hours facilitated in Victoria only; offered quarterly or on client demand Voluntary Target: Executive staff Attendance: Registration tracked
		IM110 Managing Government Information 15 Minute online module IM112 Managing Government Records Target: All government staff Attendance: Not tracked	TRIM End User 4 hours (offered monthly and for TRIM implementations in Victoria and across Province for new implementations) Voluntary Target: All offices using TRIM Attendance: Registration tracked		
Total	299 attendees	199 attendees (excludes online web courses)	946 attendees	67 attendees	294 attendees

Office of the Chief Information Officer Policy Directive

DIRECTIVE:	1/14
SUBJECT:	Appropriate Use of Government Information and Information Technology Resources ("Appropriate Use Policy")
AUTHORITY:	Chapter 12 of the Core Policy and Procedures Manual (CPPM)
EFFECTIVE DATE	March 21, 2014

Purpose:

The purpose of this directive is to set out the policy requirements that all government employees must follow when:

- accessing and managing government information (particularly confidential information); and,
- using information technology (IT) resources.

Additional policies and procedures may be established at the ministry level to support employee compliance with, and monitoring of, this directive and/or to augment this directive with policies and procedures specific to that ministry's information holdings or organizational structure.

Compliance with this directive, and supporting ministry policies and procedures, will ensure that government information is appropriately protected while remaining accessible to those who need it and are authorized to access it. Ultimately, appropriate use of government information and IT resources will ensure that government is able to deliver effective and efficient services to citizens while meeting its statutory obligations to protect information.

Application:

This policy applies to all ministries, agencies, boards and commissions reporting or responsible to the Government of British Columbia.

Advice on this Directive:

Advice on this Directive can be obtained from the:

Information Stewardship and Policy Branch
Office of the Chief Information Officer
Ministry of Technology, Innovation and Citizens' Services

Email: im.itpolicy@gov.bc.ca

Version	Date	Changed By	Description of Change
1.0	March 21, 2014	Colleen Rice	
1.1	August 25, 2014	Colleen Rice	Update broken links
1.2	April 21, 2015	Colleen Rice	Update broken links
1.3	September 21, 2015	Colleen Rice	Update broken links

Table of Contents

Definitions:.....	1
Roles and Responsibilities:.....	3
Policy:.....	4
A. General Requirements	4
B. Collection, Access, Use, Disclosure, Storage and Disposal of Government Information.....	5
C. Use and Disposal of Government IT Resources	7
D. Access to and Use of Applications and Software	8
E. Monitoring and Investigations.....	8

Definitions:

The following key terms are defined below and appear in bold font throughout the document.

Confidential Information is a category of **Government Information** with confidentiality requirements. It includes, but is not limited to:

- cabinet confidences (for example, a briefing note to Cabinet);
- government economic or financial information (for example, information about a proposed administrative plan that has not yet been implemented or made public);
- information harmful to intergovernmental relations (for example, information received in confidence from another government);
- third party business information, where its disclosure could harm the third party;
- **Personal Information**;
- legal advice or law enforcement information.

Device: an **IT Resource** that can connect (wired, wireless or cellular) to the government network, including but not limited to computers, laptops, tablets, smartphones, and cellphones.

Employee: an individual working for the Government of British Columbia, including **Service Providers** or volunteers.

Government Information: means all recorded information relating to government business, regardless of format, that is received, created, deposited or held by any ministry, agency, board or commission reporting or responsible to the Government of British Columbia.

Information Incident is a single or a series of unwanted or unexpected events that threaten privacy or information security, including a privacy breach or the collection, use, disclosure, access, disposal, or storage of information, whether accidental or deliberate, that is not authorized by the business owner of that information.

IT Resources: information and communication technologies that include, but are not limited to: information systems, **Devices**, and the government electronic network.

Least Privilege: a principle requiring that each subject in a system be granted the most restrictive set of privileges (lowest clearance) needed to perform their employment duties. The application of this principle limits the damage that can result from accident, error or unauthorized use.

Need-to-know: a principle where access is restricted to authorized **Employees** that require it to carry out their work. Employees are not entitled to access merely because of status, rank, or office.

Personal Information: is recorded information about an identifiable individual other than (business) contact information.

Portable Storage Device: is a portable (or removable) device that is primarily designed to store electronic information, for example an external hard drive or a USB flash drive.

Protected Government System: a computer system in a data centre that has met the approved security requirements for the storage of **Confidential Information** (for example, an **Employee's** network drives). This does not include the hard drives of computers, laptops, tablets, smartphones or other **Devices**.

Record: is anything that is recorded or stored by graphic, electronic, mechanical or other means, including books, documents, maps, drawings, photographs, letters, vouchers, and papers.

Service Provider: means a person retained under contract to perform services for the Government of British Columbia.

Roles and Responsibilities:

Deputy Ministers or Equivalent

Deputy Ministers (or equivalent positions) are responsible for ensuring that ministry specific policy and procedures are developed, where necessary, to support the Appropriate Use Policy.

Government Chief Information Officer

The Government Chief Information Officer is responsible for issuing corporate policy, directives and guidelines on the appropriate use of government **IT Resources** and **Government Information**.

Ministry Chief Information Officers or Equivalent

Ministry Chief Information Officers (or equivalent positions) are responsible for developing ministry-specific policies and procedures, where necessary, to support the Appropriate Use Policy.

In addition, Ministry Chief Information Officers are responsible for providing support to supervisors in their respective ministries to ensure that supervisors have the information and training necessary to fulfill their responsibilities as set out in this policy.

Supervisors

Supervisors are responsible for ensuring that **Employees** are made aware of their responsibilities concerning the appropriate use of **Government Information** and government **IT Resources**.

They are also responsible for ensuring that **Employee** access to **Confidential Information** is based on the principles of **Need-to-Know** and **Least Privilege** and for reviewing that access level annually.

They are responsible for ensuring that **Employees** receive the level of training (including privacy, security and records management training) necessary to perform their duties.

In addition, supervisors are responsible for approving the downloading of applications and software by **Employees**. This includes exercising due diligence to ensure that applications and software that are approved for download meet the requirements of this policy.

Further, supervisors are responsible for approving **Employees'** ability to work outside the workplace with **Confidential Information** and ensuring compliance with the Working Outside the Workplace Policy.

Employees

Employees are responsible for complying with this policy and for seeking direction from their supervisors if they have questions regarding this policy.

Policy:

A. General Requirements

1. **Employees** must comply with the Standards of Conduct for Public Service Employees when:
 - a) collecting, accessing, using, disclosing or disposing of **Government Information**;
 - b) using **IT Resources**, whether that use is directly related to their employment duties or not; and,
 - c) accessing third party hosted sites (e.g. Facebook and Twitter) in a manner that could be perceived as representing government. For more information on the use of Social Media, please see the Social Media Guidelines.
2. Supervisors must ensure that **Employees** are made aware of their responsibilities concerning the appropriate management of **Government Information** and **IT Resources**:
 - a) at the commencement of their employment;
 - b) when a significant change occurs respecting their access to, or authorized use of, **Government Information** or their use of **IT Resources**, including but not limited to:
 - i. the issuance a new **Device**; and
 - ii. access to a new information database.
 - c) when a new or updated version of this directive or similar policy is issued; and
 - d) annually for **Employees** that have access to a significant amount of **Confidential Information**.
3. Supervisors must ensure that **Employees**:
 - a) understand what **Confidential Information** is and the ministry policies and procedures that must be followed when accessing and managing **Confidential Information**; and
 - b) have received training appropriate to their position respecting the management of **Confidential Information** (including privacy, security and records management training) and what to do if an **Information Incident** occurs.

For further information on **Information Incidents** please refer to The Information Incident Management Process.

4. Ministry Chief Information Officers (or equivalent positions) must develop ministry-specific policies and procedures, where necessary, to support **Employee** compliance with, and monitoring of, this policy.

5. Deputy Ministers (or equivalent positions) must ensure that ministry-specific policies and procedures are developed, where necessary, to support **Employee** compliance with, and monitoring of, this policy.

B. Collection, Access, Use, Disclosure, Storage and Disposal of Government Information

6. **Employees** must collect, access, use, disclose and dispose of **Government Information** in accordance with policy and law. For example, disposal of information must be done in accordance with approved records schedules, and collection, access, use and disclosure of **Personal Information** must be in accordance with the Freedom of Information and Protection of Privacy Act and its supporting policies.
7. Supervisors must authorize an **Employee's** access to **Government Information** based on the principles of "Need-to-know" and "Least Privilege". Specifically, an **Employee** should have access to the least amount of **Confidential Information** that is necessary to perform their duties.
8. Supervisors must review an **Employee's** level of access to **Confidential Information** at least once per year to ensure that their access level remains necessary and appropriate for the performance of their duties.
9. **Employees** must not collect, access, use, disclose or dispose of **Confidential Information** unless authorized to do so and it is necessary for the performance of their duties.
10. **Employees** must respect intellectual property rights. For example, **Employees** must not use, reproduce, modify or distribute programs or data if they have not received permission from the intellectual property owner to do so.

For more information on intellectual property rights please contact the Intellectual Property Program.

11. **Employees** must store electronic **Records** that relate to government business in **Protected Government Systems**.
 - a) In extenuating circumstances, an electronic government **Record** may be temporarily stored outside of a **Protected Government System**, as long as the following conditions are met:
 - i. the electronic **Record** is stored on the system or **Device** only as long as is necessary to deal with the extenuating circumstance;
 - ii. at the first available opportunity, the **Record** is transferred to a **Protected Government System**; and
 - iii. duplicate copies of any electronic **Record** containing **Confidential Information** are deleted from the other system or **Device** as soon as possible.

- b) The requirements set out in subsection (a) do not apply to an email **Record** that is automatically stored by government's email system on an **Employee's Device**.

12. **Employees** are responsible for ensuring that the **Confidential Information** they are working with is protected. This includes, but is not limited to:

- a) storing **Confidential Information** in **Protected Government Systems**, as set out in section 11, above;
- b) physically securing **Confidential Information** in their workspace (e.g. locked drawers or cabinets);
- c) only disclosing **Confidential Information** to authorized individuals in a secure manner according to ministry approved processes (e.g. **Portable Storage Devices** should only be used in extenuating circumstances when more secure methods are not available and must be encrypted); and
- d) limiting the amount of **Confidential Information**, particularly **Personal Information** (which is subject to legal restrictions), that is disclosed through email.

For further information on encryption standards, please see the [Cryptographic Standards for Information Protection](#).

13. **Employees** may work outside the workplace with **Confidential Information** provided that they have their supervisor's approval and comply with all the provisions of this directive. In addition, **Employees** must:

- a) protect the information, particularly when working in a public environment (for example, ensuring that information is not viewable or accessible by others);
- b) limit the amount of printed materials that are used outside of the workplace (government **Devices** are more secure because they are protected with government security features); and
- c) follow the [Working Outside the Workplace Policy](#).

14. If an **Information Incident** occurs, **Employees** and supervisors must follow the [Information Incident Management Process](#) which requires the immediate reporting of any suspected or actual **Information Incident** (including a privacy breach) to the Office of the Government Chief Information Officer and to the Ministry Chief Information Officer.

C. Use and Disposal of Government IT Resources

15. Reasonable personal use of government **IT Resources** by **Employees** is permitted. Personal use is reasonable provided that it:
- a) is limited during core business hours and does not interfere with the **Employee's** duties and responsibilities;
 - b) is lawful;
 - c) does not compromise the security of government **IT Resources** or **Government Information**; and
 - d) is not used for personal financial gain.
16. For privacy reasons and to reduce the cost of electronic storage for government, **Employees** must limit the amount of personal **Records** they store on government systems.
17. **Employees** must use their government email accounts when conducting government business. This includes while working outside of the workplace.

In extenuating circumstances, **Employees** may use their personal email or other non-government email, as long as the following conditions are met:

- a) a copy of the email is sent to their government email account, ensuring that the **Government Information** is stored in a **Protected Government System**;
- b) the email is immediately deleted from their personal or non-government email account as soon as possible after dealing with the extenuating circumstance; and
- c) the amount of **Confidential Information** collected, accessed, used or disclosed is limited to the least amount necessary to deal with the extenuating circumstance.

For information on how to access government email accounts from a remote location, please see the [Outlook Web App Guide](#).

18. **Employees** must not divulge, share or compromise their own or another **Employee's** government authentication credentials (e.g., passwords, access cards, etc.). This includes not divulging passwords to technical support.
19. **Employees** must report any lost or stolen **Device** or access card in accordance with [Chapter 20 – Loss Management of the Core Policies and Procedures Manual \(CPPM\)](#) and [Procedure L – Loss Reporting of the CPPM](#).
20. **Employees** must follow the appropriate policies and procedures when disposing of **IT Resources**. For further information, please see the [IT Asset Disposition Site](#).

D. Access to and Use of Applications and Software

21. **Employees** must have their supervisor's permission, and follow the established procedures, to download or use applications or software from the iStore or the Self-Serve Centre.
22. If an **Employee** wishes to download or use applications or software for government business purposes that are available through the iStore or the Self-Serve Centre and are also available from another source, the **Employee** must download or access the application or software from the iStore or the Self-Serve Centre.
23. **Employees** must not download or use applications or software for government business that are not available from the iStore or the Self-Serve Centre without the permission of their supervisor.

Applications and software that are not available from the iStore or the Self-Serve Centre may present privacy or security concerns or could impose terms and conditions, such as indemnification clauses, that are unacceptable to government.

24. Supervisors must not permit an **Employee** to download or use applications or software that:
 - a) are prohibited by the Government Chief Information Officer;
 - b) present unacceptable privacy or security concerns; or
 - c) impose unacceptable terms and conditions.

With respect to section 2(c), supervisors should review their procurement responsibilities in the Core Policy and Procedures Manual - Chapter 6 Procurement before approving an application for download.

E. Monitoring and Investigations

25. Any collection, access, use, transmission, or disposal of **Government Information** or use of government **IT Resources**, whether for personal reasons or not, may be audited, inspected, monitored and/or investigated to:
 - a) maintain, repair and manage **IT Resources** for the efficient operation of business systems;
 - b) meet legal requirements to produce information, including by engaging in e-discovery;
 - c) ensure accessibility of government **IT Resources** for the continuity of work processes;
 - d) improve business processes and manage productivity; and
 - e) ensure compliance with legislative and policy requirements, including the Standards of Conduct.

26. Allegations of inappropriate access, collection, use, disclosure, or disposal of **Government Information** or inappropriate use of government **IT Resources** will be investigated on a case-by-case basis. Investigations may include, but are not limited to, the search and/or seizure of **IT Resources**.
27. **Employees** who inappropriately access, collect, use, disclose or dispose of **Government Information** or inappropriately use **IT Resources** may be subject to disciplinary action, including dismissal, cancellation of contract, and/or other legal remedies.