

**Ministry of Finance**  
**BRIEFING DOCUMENT**

**To:** Honourable Michael de Jong, Q.C.      **Date:** March 1, 2016  
Minister of Finance

**Initiated by:** Tara Richards  
Assistant Deputy Minister/Executive Financial Officer  
Corporate Services Division  
Ministry of Finance

**Ministry  
Contact:** Steve Klak  
Chief Financial Officer  
Ministry of Finance

**Phone Number:** (250)-356-1387  
**Email:** [Steve.Klak@gov.bc.ca](mailto:Steve.Klak@gov.bc.ca)

**Cliff #:**      **349775**

---

**TITLE:**      Proactive Release of Receipted Expenses for Ministers

---

**PURPOSE:**  
**(X) FOR DECISION**

---

---

---

Executive Director approval: \_\_\_\_\_

ADM approval: \_\_\_\_\_

DM approval: \_\_\_\_\_

**DATE PREPARED:** March 1, 2016

**TITLE:** Proactive Release of Receipted Expenses for Ministers

**ISSUE:** Implementation considerations for posting Ministers' expenditure receipts.

**BACKGROUND:**

At the end of March 2015, the receipted expenses for the Members of the Legislative Assembly, after redaction following FOIPPA guidelines, were posted on the Assembly's website for public viewing for the first time.

The Minister has publicly committed to pursue a similar posting of receipted travel expenses for Ministers. The process would require scanning and redaction of receipts prior to website posting for public release.

Currently, monthly summaries (that include totals for In Province flights, Other Travel in Province, Out of Province Travel and Out of Country Travel) of Ministers' travel expenses are posted by all Ministries on the Open Information website.

The Capital City Allowance (CCA), which consists of daily per diems and living allowances, are not disclosed through the Open Information process. The Legislative Assembly posts the total CCA costs quarterly for all Members including Ministers.

**DISCUSSION:**

The timing of the disclosures can either align with the posting of MLA receipted travel expenses on the Legislative Assembly website or follow a separate timeline. The Legislative Assembly currently posts receipts on a quarterly basis with a one quarter lag (e.g. Quarter 1 receipts are posted by end of Quarter 2).

A monthly reporting process with a one month lag could also be adopted for the posting of Ministers' travel receipts and this would supplement the current summaries.

For consistency, government may wish to also disclose receipted expenses for MLAs and parliamentary secretaries travelling on behalf of Executive Council.

The adopted disclosure would also include redacted receipts for CCA.

**OPTIONS:**

1. Ministers' Office Support Services (MOSS) in the Ministry of Finance scans, redacts, and posts all receipts on the Open Information website on a monthly basis. Starting with April 2016, receipts would be posted to the Open Information website by the end of June 2016, cross referenced to the Legislative Assembly website. There

*Quarterly*

afterward, receipts for a month would be posted by the end of the following month. An approval process involving Ministers' Office staff will be developed.

#### Pros

- MOSS is able to leverage existing Open Information infrastructure and the expertise of the Corporate Information and Records Management Office (CIRMO) for training and oversight.
- MOSS is a subject matter expert on Ministers' travel and would be best able to respond to questions that might arise once information is posted.
- Minimizes touch-points to one branch, thereby minimizing potential delays.
- The processing and posting of minister's receipts by core government aligns with government's vote structure and the accountabilities performed by Ministers as leaders of core government.
- Faster recurrence in timing of postings of Minister's receipts.

#### Cons

- Anticipate that up to two new FTEs will be needed to address the related workload, including related payments to suppliers (e.g. airline companies).
- MOSS staff will need to learn how to redact documents.
- The timing of the disclosure and the Open Information website would not be integrated with information released by the Legislative Assembly, but a link cross referencing the Legislative Assembly website would be included.

### 2. MOSS scans receipts and CIRMO redacts and posts receipts.

#### Pros

- CIRMO has the tools and expertise to perform the redaction.
- Consistent redaction practices.

#### Cons

- Multiple touch points may result in delays and inefficiencies.
- Adds to existing backlog within CIRMO.

### 3. Legislative Assembly assumes all responsibility for scanning, redacting and posting travel receipts.

#### Pros


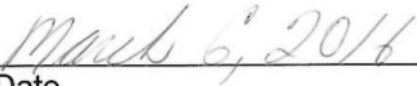
- Legislative Assembly has already developed a framework for redaction and has the experience.
- The timing of postings for all MLAs is aligned.
- Consolidation of all related functions in one organization minimizes the number of touch points, which may result in time savings and efficiencies.

## Cons

- Processes for information sharing and approvals will need to be addressed as the Legislative Assembly is an independent office and uses its own network with restricted access.
- Based on experience with Members of the Legislative Assembly, the Legislative Assembly estimates that up to two additional staff would be required to perform the responsibilities.
- Does not align with government's vote structure.

**RECOMMENDATION:**

Option 1. Ministers' Office Support Services (MOSS) in the Ministry of Finance scans, redacts, and posts all receipts onto the Open Information website. Starting with April 2016, receipts would be posted by June 30, 2016 and on a monthly basis afterwards.

  
\_\_\_\_\_  
Michael de Jong, Q.C.  
Ministry of Finance  
\_\_\_\_\_  
Date



Government Submission  
to the Special Committee to Review the  
*Freedom of Information and  
Protection of Privacy Act*

March 16, 2016



## Table of Contents

<b>Foreword.....</b>	<b>1</b>
<b>Introduction.....</b>	<b>2</b>
Background.....	2
Governance and Administration of FOIPPA .....	3
Recent Events Impacting Information Management .....	4
Government's Action Plan.....	4
<b>Improving Access to Information.....</b>	<b>6</b>
Improving the FOI Service Experience for Applicants .....	6
Increasing Proactive Disclosure of Government Information .....	10
<b>Privacy Protection: Managing Information Assets like Financial Assets.....</b>	<b>13</b>
Solidifying British Columbia's Leading Privacy Practices .....	13
Enhancing Privacy through Better Management and Accountability.....	15
<b>Increasing Oversight and Compliance.....</b>	<b>17</b>
Information Management in Context.....	17
An Integrated and Disciplined Approach .....	19
Increasing Oversight.....	20
<b>Improving Records Management Practices and Advancing the Duty to Document .....</b>	<b>23</b>
The Information Explosion and the Impact on Records Management in Government .....	23
Documenting and Retaining Valuable Information .....	24
<b>Other Considerations.....</b>	<b>26</b>
Clarifying Privacy Impact Assessment (PIA) Requirements.....	26
Streamlining and Clarifying the Commissioner's Powers.....	26
Frequency of Legislative Reviews.....	27
<b>Conclusion .....</b>	<b>28</b>
<b>Summary of Recommendations.....</b>	<b>28</b>
<b>Appendix 1: David Loukidelis' Recommendations.....</b>	<b>30</b>





## Foreword

On November 18, 2015, the Government Chief Information Officer made a presentation to this committee, on behalf of the government. At that time, former Information and Privacy Commissioner David Loukidelis was preparing a report for government on actions it could take to address recommendations made by the current Information and Privacy Commissioner in her investigation report, "Access Denied: Record Retention and Disposal Practices of the Government of British Columbia".

Government offered to provide a follow up briefing after it received the Loukidelis report and to provide a written submission that took into account its recommendations. This submission sets out how government is taking action on the Loukidelis recommendations and reiterates several key themes presented previously to the Committee.

It should also be noted that since the time of government's previous presentation, there has been a significant change in roles and responsibilities for information management. On December 16, 2015, responsibility for government's information management practices, policies and legislation was transferred to the Ministry of Finance. A new Corporate Information and Records Management Office (CIRMO) was established to integrate and align information access, records management, and privacy governance under the leadership of the province's first Chief Records Officer.

By bringing these important disciplines together, government is better positioned to provide corporate oversight, guidance and training to all ministries on the importance of good record keeping and privacy management practices and how these practices facilitate improved access to information. The move to the Ministry of Finance has also enabled better alignment with the Public Service Agency (PSA), the central agency responsible for government's human resources management. Improving information management practices will involve new training, compliance and culture change strategies and closer alignment with the PSA will significantly advance this work.

This strategic realignment of government's information management accountabilities is the first step in improving our access to information and records management practices, including those practice improvements recommended by David Loukidelis in his December 2015 report to government.<sup>1</sup> It is a significant first step and sends a strong message that government is committed to making real and meaningful change. Under the leadership of the Minister of Finance, government is advancing the proactive disclosure of information and a revitalized service culture to improve access to information, accountability and transparency. Information on these and other initiatives are set out in this submission for consideration by the Committee in conducting its legislative review of the *Freedom of Information and Protection of Privacy Act*.

---

<sup>1</sup> See Appendix 1 for a full list of Mr. Loukidelis' recommendations.

# Introduction

## Background

The *Freedom of Information and Protection of Privacy Act* (FOIPPA) came into force on May 22, 1992. The purpose of the Act is twofold:

1. To promote accountability by providing a right of access to records and information of public bodies; and
2. To protect personal information by prohibiting the unauthorized collection, use, disclosure, access or storage of personal information by public bodies.

FOIPPA outlines the rules and requirements respecting citizens' access to information rights and how to exercise them, and their right to privacy including what personal information can be collected, used, disclosed and retained by public bodies, when, why and how.

The Act has been amended a number of times over the years, both in response to previous Special Committee reviews and in response to other reviews and developments.

### 2004 Data Residency Provisions

In 2004, data residency provisions were added to FOIPPA in response to the *USA Patriot Act*. This statute authorized US law enforcement and anti-terrorism authorities to obtain an order requiring any person or US-owned organization to disclose any type of record, including those containing personal information about BC residents. This statute also stipulated that any demand for such disclosure must remain confidential.

The data residency provisions added to FOIPPA restrict the trans-border data flow of British Columbians' personal information by requiring personal information to be stored and accessed only within Canada, except in limited circumstances.

### 2011 Amendments

Significant amendments to FOIPPA were also made in 2011, including:

- The addition of proactive disclosure provisions, providing the Minister responsible for the Act with the authority to establish categories of records that must be proactively disclosed;
- The addition of data linking requirements for public bodies and increased oversight by the Information and Privacy Commissioner;
- The addition of provisions governing the collection, use and disclosure of personal identity information; and,
- Remedies to recover personal information in the custody of an unauthorized person or entity.

## Governance and Administration of FOIPPA

The effective functioning and implementation of FOIPPA is dependent upon the ability, capacity and good faith actions of public bodies to carry out their duties and obligations under the Act. The responsible Minister, currently the Minister of Finance, is responsible for the administration of the Act and has specific regulatory and direction-making authority.

Government's Chief Records Officer (CRO), as head of the Corporate Information and Records Management Office (CIRMO) in the Ministry of Finance, provides access and privacy leadership, advice and support to public bodies and manages the legislative change process for FOIPPA. This is as part of a broader mandate that also includes oversight over other information management legislation such as the *Document Disposal Act* (soon to be replaced by the *Information Management Act*) as well as policies, procedures, and operations related to access to information, privacy, and records management.

The Information and Privacy Commissioner, an independent Officer of the Legislature, has broad responsibility for overseeing and monitoring how FOIPPA is administered and for ensuring that its purposes are achieved.

### Administration of Access to Information (FOI) Requests

FOI requests are processed by CIRMO's Information Access Operations (IAO), on behalf of government. The general process is as follows:

1. IAO, as the central agency responsible for coordination, receives a request and forwards it to the ministry (or ministries) identified in the request (an applicant may identify one or several ministries from whom they are seeking records).
2. IAO is the primary contact with the applicant and has been responsible for assisting applicants, where necessary, with the clarification of requests.<sup>2</sup>
3. The ministry conducts a search for records and provides any responsive records back to IAO.
4. IAO reviews the records in consultation with the ministry, redacts any information that may be exempted from disclosure under the FOIPPA, and prepares a response for the applicant.
5. The Deputy Minister (or delegate) of the applicable ministry is responsible for final decisions on disclosure and approves the response package, before IAO releases it to the applicant.

To support and document this process, IAO provides a Standard Call for Records form, which must be completed by the Ministry. It includes guidance on legislated timelines for response, assessing fees, extension criteria, and conducting a record search.

---

<sup>2</sup> This is an area that is currently under review for service improvement. Applicants are likely to receive a better service experience if ministry staff with knowledge of ministry records and business processes assist applicants in clarifying their requests and identifying responsive records.

## **Recent Events Impacting Information Management**

### **Information and Privacy Commissioner Issues Investigation Report F15-03**

On October 22, 2015, the Information and Privacy Commissioner issued Investigation Report F15-03, which examined government's response to three FOI requests. The report found a number of deficiencies in how government had processed these requests and made 11 recommendations for improvement.

In response to the Commissioner's report, government commissioned a report from former Information and Privacy Commissioner David Loukidelis, on how to implement actions in response to the Commissioner's report.

### **David Loukidelis' Report**

On December 15, 2015, government received David Loukidelis' report, which made 27 recommendations for improving processes, policy and training. The report also recommended that government consider legislative amendments to:

- add a "duty to document" (i.e., create records) with the details to be worked out in policy at the ministry or program level;
- increase oversight of the destruction of records; and
- make it an offence to destroy records with the intent to evade an FOI request.

On December 16, 2016, Premier Christy Clark announced that government had accepted all of Loukidelis' recommendations.

## **Government's Action Plan**

Government is committed to making real and meaningful improvements to its information management practices. This submission sets out how government is advancing its action plan, including actions it is taking to address recent recommendations made by the current Information and Privacy Commissioner, Elizabeth Denham and David Loukidelis.

While taking action on these recommendations is a significant first step, government is committed to a larger plan and vision for improvement — one that ingrains an open and service-oriented culture, supported by an information management discipline that values and protects its information assets.

The actions necessary to succeed can be categorized into four main themes:

1. Improving access to information, including:
  - a. Improving the FOI service experience for applicants; and
  - b. Increasing the proactive disclosure of government information.
2. Enhancing privacy protection, including:
  - a. Solidifying British Columbia's leading privacy practices;

- b. Enhancing privacy through better management and accountability; and
  - c. Privacy compliance auditing.
- 3. Increasing oversight and compliance, including:
  - a. Integrating the information management discipline under the leadership and oversight of government's first Chief Records Officer;
  - b. Establishing a comprehensive compliance program; and
  - c. Instituting mandatory information management training.
- 4. Improving records management practices and advancing a duty to document.

In addition to the four key themes outlined above, this submission also includes a number of related matters for the Committee's consideration.

## Improving Access to Information

British Columbia's *Freedom of Information and Protection of Privacy Act* (FOIPPA) provides the broadest privacy and access coverage in Canada. Over 2,900 public bodies are covered under the legislation, and the citizens of British Columbia are very active in exercising their right to access government information — over the past six years ministries alone have processed approximately 8,000 to 10,000 requests per year. In 2013/14 (the last year for which statistics were available from other provinces), B.C. ministries processed approximately twice as many freedom of information (FOI) requests per capita as ministries in Ontario or Alberta.

The Loukidelis report highlighted several areas for improvement in the government FOI process, including:

- Providing guidance to employees on the “duty to assist” applicants, including with respect to interpreting and clarifying requests;
- Conducting and documenting thorough searches for records;
- Providing better explanations to applicants in cases where no records are located in response to a request;
- Designating career public servants to oversee FOI requests directed to Ministers’ offices; and
- Improving training and awareness for staff.

Government accepted all of David Loukidelis’ recommendations and is committed to addressing these service-related matters while at the same time taking additional measures to significantly improve access to information for British Columbians.

Specifically, government is taking a two-pronged approach which is focused on:

1. Improving the FOI service experience for applicants; and
2. Increasing the proactive disclosure of information.

### Improving the FOI Service Experience for Applicants

The “duty to assist” is a legislative positive duty to make every reasonable effort to respond openly, accurately, completely and without delay to a request for access to information under FOIPPA. In government’s view, however, the “duty to assist” goes beyond just meeting the letter of the law; it involves providing an excellent service experience to each applicant.

Improving the FOI service experience is about supporting members of the public in accessing the information they need to engage meaningfully with government on issues that matter to them. That access is predicated on good service practices, including:

- Making every reasonable effort to assist an applicant and to do so in a timely manner;

- Interpreting and clarifying access requests in a manner that meets the needs of the applicant—which may include engaging knowledgeable program area staff to work directly with the applicant to help identify records responsive to their interests;
- Conducting thorough searches for records and documenting that search effort; and
- Providing better explanations in cases where no records are located and, if applicable, transferring the request to another ministry or public body that has responsive records.

A key element of this approach is clarifying and, where appropriate, resetting roles and responsibilities between ministries and the CIRMO (the central agency responsible for coordinating FOI requests). Deputy Ministers will be responsible for promoting FOI service practices and ensuring that the “duty to assist” is met in responding to every FOI request. Career public servants will also be designated in Deputy Ministers’ offices to oversee all FOI requests directed to Ministers’ offices, ensuring that thorough searches are conducted and documented. Revised policies and procedures will emphasize the importance of the “duty to assist” applicants and clarify associated roles and responsibilities. New guidelines will support employees in clarifying requests and conducting thorough and documented searches for records. These policies, procedures and guidelines will be supported by mandatory training to ensure that all employees understand the requirements and their responsibilities.

There are a number of actions currently underway to drive improvements in these areas:

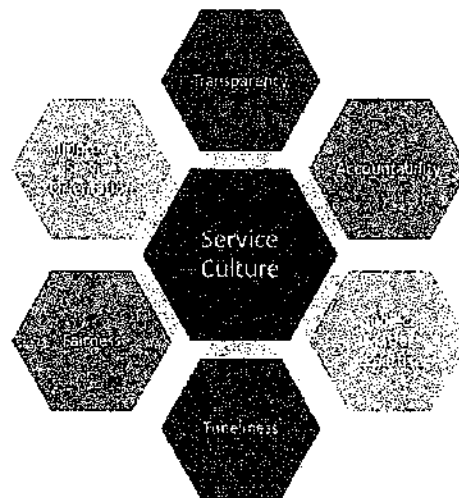
Improving the FOI Service Experience for Applicants	
<b>Enhanced accountability and oversight</b>	<ul style="list-style-type: none"> <li>• Revised policies will clarify roles and responsibilities for ministries and CIRMO, particularly with respect to ensuring that the “duty to assist” is met and the search for records is thorough, well-documented, and clearly articulated to the applicant.</li> <li>• A two-way escalation process will be established between the CIRMO and Deputy Ministers’ Offices to ensure that searches for records are thorough, well-documented, and are carried out in a timely and effective manner.</li> </ul>
<b>Interpreting and clarifying requests in a manner that meets the needs of applicants</b>	<ul style="list-style-type: none"> <li>• Revised policies and procedures will ensure that where necessary, clarification of requests is done: <ul style="list-style-type: none"> <li>○ In a manner that assists the applicant to access the information they want in a timely way; and</li> <li>○ Where appropriate, by an employee with knowledge of the ministry’s records and business.</li> </ul> </li> </ul>
<b>Conducting and documenting a thorough search for records</b>	<ul style="list-style-type: none"> <li>• Revised policies and guidelines will provide specified criteria and processes for conducting and documenting searches.</li> </ul>
<b>Explaining and transferring “no responsive records” responses –</b>  For example, where an explanation may help an applicant understand why the records they are requesting would not typically be held by a Minister’s Office or the Office of the Premier	<ul style="list-style-type: none"> <li>• Revised policies and procedures will require ministries to provide better explanations and information to applicants for why no records may have been located in response to a request.</li> </ul> <p>This was recommended by David Loukidelis as a way to help applicants understand why the records they are requesting would not typically be held by the office to which they directed their request.</p> <ul style="list-style-type: none"> <li>• Revised policies will also require ministries to transfer a request where they know that records responsive to that request are located in another ministry or public body.</li> </ul>

Designating a career public servant responsible for overseeing requests in Ministers' offices	<ul style="list-style-type: none"> <li>Designated career public servants will oversee searches for records in Ministers' offices and be accountable for ensuring that the search and documentation effort is thorough.</li> </ul>
Mandatory training for all staff to ensure a clear understanding of roles and responsibilities	<ul style="list-style-type: none"> <li>All government and political staff will be required to complete comprehensive information management training (including FOI, records management and privacy) with mandatory refresher training every 2 years.</li> </ul>

## Creating a Service Culture in FOI

The above-mentioned actions are only the initial steps towards improving the FOI service experience. Government's long-term vision involves a revitalized service culture where designated government employees are committed to providing excellence in service throughout the FOI request process. Under the oversight of committed senior executive leaders, employees involved in processing requests will be expected to identify and understand an applicant's needs and to make every effort to respond in a manner that best meets those needs — which may include answering questions, redirecting requests, and suggesting better and alternate sources of information.

The principal objectives upon which this service culture will be built are transparency, accountability, subject matter expertise, timeliness, fairness and improved service orientation. These principles support government's view that responding to an FOI request is an important public service.



Government is developing a communications and change management strategy to support this important culture shift. The above principles for service excellence will be incorporated into government policy and ongoing communication and training initiatives.



## **Protecting the Identity of Applicants**

This committee has received submissions recommending legislative amendments to ensure the anonymity of FOI applicants. While government agrees in principle that confidentiality should be respected to the extent reasonable and practicable, it is unclear what value a legislative amendment would add to the protection already afforded by the privacy provisions in the Act, and government's current policy respecting the sharing of an applicant's identity on a "need to know" basis. It is also unclear, and an issue of some concern to government, how a legislative requirement for anonymity would provide the best service to applicants if knowledgeable staff are unable to discuss the request with the applicant.

The privacy provisions in FOIPPA already require government to protect the identities of individual applicants. With respect to the identity of other applicants that represent businesses and organizations, government ensures the appropriate protection of their identity through policy. This policy will be revised to better clarify the circumstances under which it is appropriate to share the identity of an applicant for the purposes of fulfilling his or her FOI request.

While not an exhaustive list, the following situations are ones where the identity of the applicant must be shared with ministry staff involved in the processing of an FOI request:

- Where the identity is necessary to identify responsive records (e.g., applicant is requesting access to his or her own personal information);
- Where the identity is necessary to verify the applicant's claims that they are acting on behalf of another individual or organization (e.g., custodial parent, power of attorney, company president, legal counsel); or
- Where the applicant is requesting a fee waiver and the identity is relevant to verifying the applicant's claim that they cannot afford to pay or is in a position to effectively disseminate information that is deemed to be in the public interest.

There are also situations where discussion with ministry staff, who have detailed knowledge of the ministry's records and business processes, would assist the applicant in identifying the records the applicant wishes to access. These discussions could be of benefit to applicants because in addition to better clarifying requests, they often lead to other or better sources of records and frequently result in reduced fees and a more timely and responsive outcome. They are also a critical part of the new service culture government is establishing where government employees are ready, willing and able to assist applicants in identifying and accessing information which is of interest to them in a timely manner and in the most accessible and useful format.

Legislating a requirement for anonymity could inadvertently and unduly affect government's ability to offer this customized service experience. Policy is a more appropriate mechanism for clarifying these considerations and ensuring that applicants' identities are only shared on a "need to know" basis and for the purpose of assisting them with their access to information needs.

### Recommendation 1:

Current privacy provisions in FOIPPA already protect the identities of individuals who make FOI requests, ensuring that the names of applicants are only shared on a "need to know" basis. Further protection would add little value and could limit public bodies' ability to provide the best service to applicants.

To ensure that knowledgeable employees are able to assist applicants with their requests, specific criteria for the protection and provision of an applicant's identity for the purpose of processing an FOI request should continue to be governed by policy.

## Increasing Proactive Disclosure of Government Information

The most effective way to improve access to information is to make information, which is in the public interest, available to the public without a formal access request. British Columbians increasingly expect to be provided on demand, easy access to information about the issues that are important to them. Government information should be made open for public access unless valid limitations exist in law or policy, so that it can be used for economic and social benefit.

### Leading in Open Information

Since 2011, government has proactively been working to provide citizens with access to the information that matters most to them. Greater proactive disclosure improves awareness, understanding and dialogue and creates opportunities for citizens to better engage with government. The Open Information website provides access to the routinely released public information, based on the kinds of information that is most commonly requested through access to information. This includes responses to General FOI requests<sup>3</sup> and summaries of Ministers' and Deputy Ministers' travel expenses.

**Open Information**

About FAQs Search Contact  
Information Releases Travel Expenses

**Information Releases**  
What's new on? See if the public information you're looking for has already been released.

**Special Information Release**  
PLEASE NOTE: The following documents related to the Review of the Draft Multicultural Strategic Outreach Plan were posted on June 21, 2023:  
Part 1 (PDF - 365KB), Part 2 (PDF - 261KB), Part 3 (PDF - 220KB)

**Travel Expenses**

Minister	Deputy Minister	Released
Hon. Christy Clark		✓
Hon. Suzanne Anson		✓
Hon. Bill Ransford		✓

<sup>3</sup> A "general" FOI request is a request for records of a non-personal nature that potentially could be released, in whole or in part, to anyone.

In addition, over 2,000 datasets are currently available through DataBC's online data catalogue. These datasets represent a broad range of quantitative information about natural resources, the economy, education and many other subjects. Created as a result of running government programs and services, the data also helps develop policy and inform business decisions.

B.C. was the first province to launch an Open Data program in Canada. Citizens can now access thousands of government datasets that are open, machine-readable, searchable and free for anyone to use or repurpose under B.C.'s Open Government License.

### **Use of the Minister's Direction-Making Authority in FOIPPA**

The *Freedom of Information and Protection of Privacy Act* provides the Minister responsible for the Act with the authority to establish categories of records that ministries must make available to the public without an access request. This committee has received submissions related to the fact that the Minister has not used this authority to designate categories of information for proactive disclosure.

While the Minister has not officially issued a direction under section 71.1 of the Act, there are, as noted above, categories of government information currently designated for proactive disclosure by policy.<sup>4</sup> In addition, over 2,000 datasets are available through the DataBC data catalogue under this same policy.

Ministries and other public bodies also routinely release a significant amount of information on their websites. For example, under the *Financial Administration Act*, public bodies across British Columbia are required to disclose executive compensation above \$75,000. Since 2008, under the direction of the Minister of Finance, the Public Sector Employers' Council Secretariat has required public bodies to go above and beyond this legislative requirement and disclose detailed explanations of all the elements that make up the compensation package for chief executive officers and the next four highest paid/ranking executives, where these positions hold an annual base salary of \$125,000 or more. The required details include an explanation of the employer's compensation philosophy, the objectives of the compensation program and what it is designed to reward, and how the payment of salary holdbacks for the top five executives relate to the organization's performance targets. These disclosures happen annually.

While there are many similar examples of routine and proactive release of information that could be cited, government acknowledges that transparency could be enhanced by formalizing these disclosures with a Minister's designation. As government re-initiates its proactive disclosure efforts, and designates new categories of information for proactive disclosure, this committee can expect to see the Minister use his direction-making authority to formalize the requirement to release information on a proactive basis. These directions will be published on government's Open Information site.

### **Exploring New Categories of Information for Proactive Disclosure**

The proactive disclosure of information over the Internet provides the public with one-stop, self-serve, anytime access to government information which is significantly more responsive and convenient than the FOI process.

---

<sup>4</sup> *Open Information and Open Data Policy (July 2011)* [http://www.cio.gov.bc.ca/local/cio/kis/pdfs/open\\_data.pdf](http://www.cio.gov.bc.ca/local/cio/kis/pdfs/open_data.pdf)

While government currently posts responses to general FOI requests and Minister and Deputy Minister travel expense reports on its Open Information site, there are additional categories of information that could be posted.

The Minister of Finance has already announced government's intention to begin the proactive disclosure of receipted travel expenses for Ministers, which will provide more detail than the reports that are currently posted. Government is also considering the proactive disclosure of other categories of information, including those recommended by the Commissioner in her 2013 report on government's Open Information program, such as calendars, direct awards and contract information.<sup>5</sup>

---

<sup>5</sup> *Investigation Report F13-03 Evaluating the Government of British Columbia's Open Government Initiative (January 2013)*  
<https://www.oipc.bc.ca/investigation-reports/1553>

## **Privacy Protection: Managing Information Assets like Financial Assets**

The Commissioner has made the analogy that information assets are like financial assets and should be treated with the same rigour and discipline. Government agrees with this analogy. Protecting personal and confidential information requires a disciplined and principled approach to information management that is similar to existing models for financial management. Financial management is a professional discipline that applies extensive and rigorous controls. The same culture and discipline should be applied to the protection of government information — especially personal and confidential information.

Good information management practices are the foundation of good governance, access rights, and the protection of privacy.

## **Solidifying British Columbia's Leading Privacy Practices**

British Columbia's privacy provisions and practices are bolstered by a strong policy framework and supported by effective training, compliance and investigation programs. B.C.'s data residency provisions — which dictate that personal information must be stored and accessed only within Canada — are the strongest in the country, demonstrating BC's steadfast commitment to robust, responsive privacy protections.

B.C. was the first province in Canada to enshrine a requirement for Privacy Impact Assessments (PIAs) in legislation, and remains one of the only jurisdictions with this type of obligation. PIAs are an effective tool used to ensure that any new enactment, system, project, program or activity conducted by a ministry is reviewed by privacy experts to ensure legislative compliance.

In 2015, the Privacy, Compliance and Training Branch processed over 660 PIAs, representing a 30% increase over the previous year, with the overall trend already indicating another significant increase in the number of PIAs projected to be completed in 2016. Other provinces have begun to follow B.C.'s lead, adopting B.C.'s PIA templates and processes. The Manitoba Ombudsman's Office, the Yukon Government and Citizenship and Immigration Canada, have each acknowledged that B.C.'s PIA framework was used as a model for the creation of their own.

According to the members of a sub-committee of the Public Sector Chief Information Officer Council (PSCIOC), B.C.'s mandatory privacy training for all public service employees and for service providers who collect or create personal information is the farthest-reaching program of its kind in Canada.

B.C. is also among the few jurisdictions that publish summaries of Privacy Impact Assessments, Information Sharing Agreements and Personal Information Banks. These summaries are posted in the Personal Information Directory (PID), which is available on government's DataBC website. The PID is one of DataBC's main drivers of web traffic with nearly 2,000 views in the last year. Publishing these summaries offers a high level of insight into how government manages the personal information in its custody or under its control.

In addition, British Columbia is the only province in Canada that has a central privacy breach response unit for ministries with a 24/7 reporting hotline. This unit is responsible for the containment, investigation and resolution of all privacy breaches.

### **Expanding the Requirement for Mandatory Privacy Breach Notification and Reporting**

The Information and Privacy Commissioner has recommended a legislative requirement for all public bodies to notify affected individuals and report to the Commissioner when a serious privacy breach occurs.

Government ministries are already required by policy to report all actual or suspected privacy breaches to government's central privacy breach response unit, and to notify affected individuals when there is determined to be risk of harm.<sup>6</sup> On behalf of ministries, and in agreement with the Commissioner's Office, the privacy breach response unit reports serious breaches to the Commissioner's Office. In addition, since the beginning of 2015, government has provided a monthly summary to the Commissioner of all actual or suspected privacy breaches.

Some broader public sector agencies may have similar programs in place. However, government has not carried out a comprehensive survey to determine the extent to which this is the case.

Comprehensive consultation should be conducted with impacted public bodies on scope, wording, and timing of any proposed requirement respecting the mandatory notification and reporting of privacy breaches.

#### **Recommendation 2:**

Comprehensive consultation should be conducted with impacted public bodies on the scope, wording and timing of any proposed amendment to FOIPPA that requires the mandatory notification and reporting of privacy breaches.

### **Protecting Personal Privacy through Data Residency Requirements**

Existing data residency requirements in the Act are important for protecting the personal privacy of British Columbians.

This committee has received submissions from a number of stakeholders, citing some of the challenges they experience in obtaining and delivering services due to the restrictions on trans-border data flow. Many organizations feel that these data residency provisions place significant limitations on the technology solutions they are able to procure, as many leading solutions are built on cloud-based platforms, which store information outside of Canada. As a result, public bodies are at times forced to procure software and technical services, which are more expensive and less effective, to ensure

<sup>6</sup> *Information Incident Management Process*

[http://www.cio.gov.bc.ca/local/cio/information\\_incident/information\\_incident\\_management\\_process.pdf](http://www.cio.gov.bc.ca/local/cio/information_incident/information_incident_management_process.pdf)

compliance. Some stakeholders have called for amendments to the provisions that limit storage, access, and disclosure of personal information outside of Canada.

While government acknowledges these challenges and is open to modernizing the language to ensure it remains relevant and practical in a changing technical environment, we believe that events in Europe and around the world tell us that retention of the data residency provisions is likely the right approach.

The European Court of Justice's recent decision to invalidate the US-EU Safe Harbor Framework is an example that strengthens the case for data-residency in B.C. The Court of Justice focused on the lack of protection of personal information from government surveillance, and ruled that the arrangement, which allowed companies to share information between the US and Europe, was no longer valid. The ruling also permits data regulators in Europe to quash any data-sharing arrangement between a European Union member and an outside jurisdiction if the other jurisdiction is not deemed to have met the "adequacy" provision, which speaks to the protection of data.

### **Recommendation 3:**

Government should continue to monitor changes to privacy laws in other jurisdictions within Canada as well as abroad, especially the European Union General Data Protection Regulations, to ensure that B.C.'s approach remains harmonized. Government should also monitor emerging technology solutions to ensure that the data residency requirements remain relevant and practical in a changing technical environment.

## **Enhancing Privacy through Better Management and Accountability**

In February 2016, government launched its new comprehensive privacy management policy, which is the first of its kind in Canada. The launch of this comprehensive and unified privacy management program for government represents a significant step forward in improving how public bodies manage the personal information in their care. The Privacy Management and Accountability Policy (PMAP) is an overarching privacy framework created to enhance ministry accountability and improve privacy practices. The PMAP provides ministries with corporate direction from the Chief Records Officer on the following privacy elements:

- accountability for privacy management;
- education and awareness;
- privacy impact assessments;
- agreements involving the sharing of personal information;
- personal information inventories and directories;
- privacy breach and information incident management;
- foreign demands for disclosure;
- service provider management; and
- compliance reviews and audits.

The cornerstone of the PMAP is the required designation of a Ministry Privacy Officer for each ministry. Every ministry has named a Privacy Officer on a permanent or interim basis, with six net new positions

added to support these responsibilities to date. This surge in available privacy resources will dramatically change the information management compliance landscape.

Another key element of government's privacy management program is the creation of a multi-faceted compliance monitoring, review and audit program. Unique among other jurisdictions in Canada, this program includes baseline assessments of each ministry, ad hoc reviews where deemed necessary and an annual self-audit to promote maintenance and growth. The program was established in response to the Information and Privacy Commissioner's January 2015 audit report.<sup>7</sup>

### **Expanding the Requirement for Privacy Management Programs**

The Commissioner has recommended a mandatory legislative requirement for all public bodies to implement a privacy management program that includes components such as training, complaint handling and the designation of one or more individuals to be responsible for ensuring compliance.

Currently, government has mandated privacy management programs for ministries through policy (PMAP), and these programs go significantly beyond the Commissioner's recommendations. Best practices from other jurisdictions and information prepared by the Commissioner were considered in the development of this policy. Additionally, the Commissioner was briefed on the policy before it was finalized.

Most broader public sector agencies will have some privacy policies and some level of a privacy management program in place, but at varying levels of maturity. Smaller public bodies are more likely to have limited or less mature privacy management programs.

For this reason, government would recommend comprehensive consultation be carried out with impacted public bodies on scope, wording, and timing of any proposed requirement respecting the implementation of a privacy management program.

While the implementation of such a program is undoubtedly a positive measure, a specific and detailed standard may be too inflexible — the approach should be adaptable to different public bodies' size, organizational structure and business processes.

#### **Recommendation 4:**

Comprehensive consultation should be conducted with impacted public bodies on the implications of a legislated requirement to implement a privacy management program. In particular, consideration should be given to the level of specificity of the amendment. A higher-level requirement that permits different implementation options may be preferable to a one-size fits all approach.

<sup>7</sup> *An Examination of BC Government's Privacy Breach Management (January 2015)* <https://www.oipc.bc.ca/special-reports/1749>

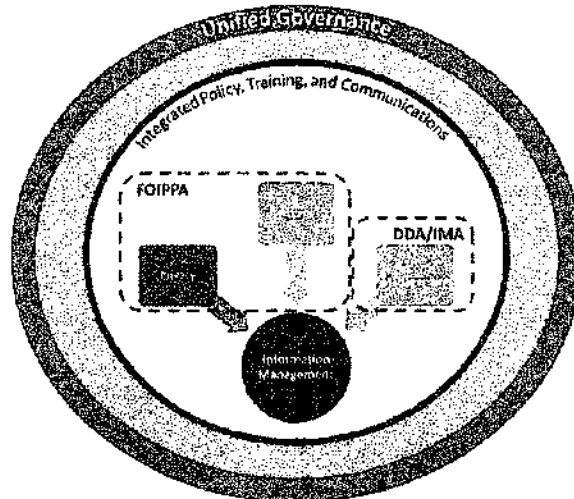


## Increasing Oversight and Compliance

Several of the Loukidelis recommendations relate to increased oversight and compliance, not only over government's access to information practices, but over its records management policies and practices. In several of his recommendations relating to improved training, policies and guidelines, he also recommended improved integration between the two. As government's records management policies and practices are governed under a separate legislative framework, some context setting is beneficial to understanding the actions government is taking to improve and integrate these practices.

## Information Management in Context

To set this discussion in context, it is essential to understand B.C.'s information management governance structure.



## What is Information Management?

Information management is an integrated discipline that includes the domains of privacy, access to information, and records management. In the public sector in British Columbia, this discipline is governed by an integrated and complementary suite of legislation and policy, including:

- The *Freedom of Information and Protection of Privacy Act* (FOIPPA);
- The *Document Disposal Act* (DDA), to be replaced by the *Information Management Act* (IMA);
- Government Core Policy and Procedures on Information Management; and
- Supplemental privacy policy (PMAP) and records management policy.

While the three domains of privacy, access to information, and records management are distinct areas of practice with discrete objectives and expertise, alignment between them is important, and there are many

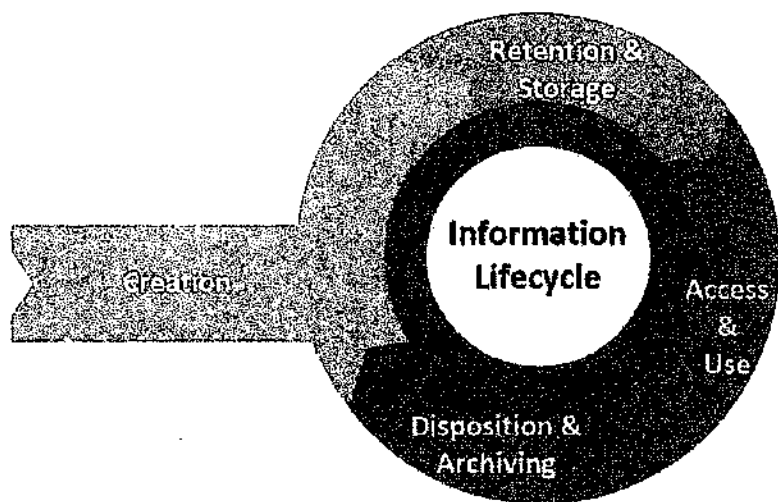
intersections and commonalities between them. They must be considered as an integrated whole and the relationships between them cannot be understated. In order to improve and streamline information management across government, the B.C. government has recently integrated these key information management disciplines under one comprehensive corporate governance program. This program is led by government's first Chief Records Officer.

### **Information Management Act (IMA)**

The information lifecycle is governed under the *Information Management Act (IMA)*, which received Royal Assent in May 2015 and will be brought into force by Order in Council this spring. When it comes into force, the IMA will:

- Repeal and replace the *Document Disposal Act*;
- Establish the role and mandate of the Chief Records Officer;
- Establish government's Digital Archives; and
- Support a modernized approach to information management with an emphasis on digital records and digital information practices.

The IMA lays the foundation for transforming how government manages and enables access to information. The Act also provides a framework for modern, digital information practices, which will increase worker productivity, provide timelier services to citizens, and improve access to information.



Creation	Retention and Storage	Access and Use	Disposition and Archiving
<ol style="list-style-type: none"> <li>1. Government information is created/collected in accordance with program specific legislation/policy and to support the operations of government.</li> <li>2. Personal information is collected in compliance with FOIPPA.</li> </ol>	<ol style="list-style-type: none"> <li>1. Government information is:               <ol style="list-style-type: none"> <li>a) retained in accordance with retention schedules under the IMA;</li> <li>b) classified for easy retrieval; and</li> <li>c) stored in, and accessible from, protected government systems.</li> </ol> </li> <li>2. Personal and confidential information is adequately protected.</li> <li>3. Transitory information is easily identified and is not retained longer than necessary.</li> <li>4. Government information is stored and retained in a digital form in accordance with the IMA.</li> </ol>	<ol style="list-style-type: none"> <li>1. Government information is available:               <ol style="list-style-type: none"> <li>a) to support government operations;</li> <li>b) to the public, subject to limited exceptions, under Open Information and FOI; and</li> <li>c) for authorized research purposes.</li> </ol> </li> <li>2. Personal information is used and disclosed in compliance with FOIPPA.</li> </ol>	<ol style="list-style-type: none"> <li>1. Government information is:               <ol style="list-style-type: none"> <li>a) disposed of, transferred or archived in accordance with retention schedules under the IMA; and</li> <li>b) disposed of securely in compliance with FOIPPA and security policy.</li> </ol> </li> <li>2. Transitory information is properly identified and deleted or disposed of as authorized by retention schedules approved under the IMA.</li> <li>3. Government information is archived digitally in accordance with the IMA.</li> </ol>

## An Integrated and Disciplined Approach

Government is committed to addressing the Loukidelis recommendations in an effective way. For this reason, we have integrated the information management discipline to reflect the interdependencies between the three domains (records management, access to information, and privacy) and to permit a more cohesive and comprehensive approach to addressing the gaps and challenges identified by both the Commissioner and Loukidelis.

Once the IMA is brought into effect, government will have a solid legislative framework upon which to build integrated policies and training, establishing a single set of requirements covering all three domains. This will be supported by a comprehensive compliance review program that evaluates performance in all three domains. Good information management practices are essential for enabling accountability, transparency and improved service delivery for citizens. This involves valuing information as an important and strategic asset and managing and protecting it throughout its lifecycle. Integrated, modernized and adaptable policies and a solid legislative framework are integral because there are important privacy, access to information, and records management considerations at each stage of the information lifecycle.

## Government's first Chief Records Officer

The integration of the information management domains has been formalized in a new Corporate Information and Records Management Office under the senior leadership of government's first Chief Records Officer (CRO).

The CRO leads a team of professional and experienced records managers, archivists, and privacy and access professionals. The amalgamation of all of government's information management related functions under the Ministry of Finance and the leadership of the CRO has:

- Assigned clear accountability for government's information management functions to a senior executive position; and
- Enabled the alignment and integration of information management policy development and training that was a central theme in Loukidelis' report.

## The Most Comprehensive Information Management Oversight in Canada

In other Canadian jurisdictions, oversight over information management is provided by a Provincial Archivist or by a Records Management Committee responsible for advising a Minister. This oversight is typically limited to records management and the archiving of information of historical value.

The powers and authority of British Columbia's Chief Records Officer are the broadest in Canada, with a strategic mandate that includes overseeing not only the management of information throughout its lifecycle, but also ensuring the protection of personal privacy and enabling access to government information.

## Increasing Oversight

The Chief Records Officer is responsible for promoting the preservation of valuable information and best practices in access to information and privacy. Once the IMA comes into effect, new integrated information management policies and best practices will be established to support this mandate, including the establishment of a compliance program to review information management systems and practices.

Next Steps	Oversight Objective
Bring the IMA into effect.	Establishes the legislative mandate of the Chief Records Officer.
Develop policies with clear roles and responsibilities for the Chief Records Officer, executive and employees.	Clarifies requirements, roles and responsibilities and establishes accountability.
Develop an escalation process for FOI issues related to the processing of requests.	Ensures that searches for records are thorough, well-documented are carried out in a timely and effective manner.
Deliver mandatory, integrated information management training to all employees.	Provides a comprehensive and integrated view of information management requirements.

Next Steps	Oversight Objective
Establish an advisory committee to provide recommendations to the Chief Records Officer on the approval of information retention schedules.	Ensures decisions are informed by expert advice from a multi-disciplinary committee including legal, financial, archiving, audit and technology experts.
Establish a comprehensive information management compliance review program based on the privacy compliance program.	Identifies areas of noncompliance, adopting a holistic view of information management, and ensures action is taken to address them. Leverages existing processes and resources.

## Establishing a Comprehensive Compliance Program

The current privacy compliance monitoring, review and audit program is being expanded to address all aspects of information management. In addition to the privacy elements, the new program will incorporate key evaluation criteria for access to information and records management so that a fully integrated assessment of how ministries manage and protect the information they hold can be conducted.

## Implementing Mandatory Training

By integrating FOI and records management training with mandatory privacy training, and taking an information lifecycle approach, this program will go further than the David Loukidellis recommendations.

The program will be developed in modules applicable to different roles in government. It will be delivered through multiple learning channels, and will include a one-stop resource repository and toolkit for all employees.

Mandatory information management training will begin in April 2016, with all employees trained by the end of March 2017. This training will be mandatory, participation will be monitored, and employees will be required to complete mandatory refresher training every 2 years.

## Increasing Oversight over Disposal of Government Information

The destruction of records is currently governed by the *Document Disposal Act*, and going forward will be covered by the *Information Management Act* (IMA). As described above, government is expanding its existing compliance program and implementing strong oversight through policy and practice improvement. The oversight authority of the CRO is already broader than the authority of her provincial counterparts and increased authority in the IMA could be considered as part of a future amendment package.

This committee has received recommendations respecting the oversight of the destruction of records, including the addition of oversight provisions in FOIPPA. However, such an amendment could create confusion and potential conflict, as it would result in two officers responsible for overseeing different or overlapping aspects of information management. Oversight of the destruction of records fits better in the IMA, which governs the entire lifecycle of information, including its eventual destruction.

### Recommendation 5:

To avoid overlapping or conflicting jurisdiction, oversight of the appropriate destruction of records should remain with the *Information Management Act*.

### Penalties and Sanctions

Enhanced employee training, guidelines, and a comprehensive compliance program are all underway with the goal of increasing awareness of, and compliance with, legislative and policy requirements respecting information management practices.

The *Appropriate Use of Government Information and Information Technology Policy* sets out the requirements for employees while collecting, using, disclosing and disposing of government information.<sup>8</sup> Employees are required to handle information in a manner that meets the requirements of FOIPPA, the DDA, and — when in force — the IMA.

Employees who fail to comply with these standards may be subject to disciplinary action up to and including dismissal. This includes employees who wilfully destroy government information that should not be destroyed (whether or not the information is the subject of an FOI request).

This policy is supported by the Standards of Conduct, which requires employees to conduct themselves in a manner that will instill confidence and trust and not bring the B.C. Public Service into disrepute.<sup>9</sup>

Furthermore, the expanded training program will reinforce information management requirements and ensure that all employees are aware of their responsibilities. The compliance review program will identify noncompliance and ensure swift action is taken where warranted, including employee disciplinary action. This will ensure that any inappropriate use, disclosure, and destruction of government information is appropriately and effectively addressed.

As part of its practice review and improvement program, government will monitor and evaluate the efficacy of the existing training and compliance program, including consequences for noncompliance. Government will consider whether increased oversight and penalties are needed, including adding increased oversight authority and penalties to the IMA.

### Recommendation 6:

Government should monitor and evaluate the efficacy of existing training and compliance programs and consider increased oversight and penalties in the *Information Management Act* if needed.

<sup>8</sup> *Appropriate Use of Government Information and Information Technology Policy* [http://www.cio.gov.bc.ca/local/cio/appropriate\\_use/policy.pdf](http://www.cio.gov.bc.ca/local/cio/appropriate_use/policy.pdf)

<sup>9</sup> *Standards of Conduct* [http://www2.gov.bc.ca/local/myhr/documents/jobs\\_hiring/standards\\_of\\_conduct\\_printable\\_version.pdf](http://www2.gov.bc.ca/local/myhr/documents/jobs_hiring/standards_of_conduct_printable_version.pdf)

# Improving Records Management Practices and Advancing the Duty to Document

## The Information Explosion and the Impact on Records Management in Government

The advancement of technologies in the digital age has made it easier than ever before to create and retain records. Daily use of email, instant messaging and social media has resulted in an information explosion over the last two decades. Government's record-keeping practices need to be modernized to keep pace. Advancements in technology have also allowed for greater storage and retention of information, much of which has no ongoing value. Conservative estimates indicate that approximately 50% of the records that are being retained are of little or no value.

In addition, the ease with which electronic records are created and shared has led to duplicate versions of the same record being held in multiple offices. This results in inefficiencies and reduced productivity for employees who need to identify, retrieve and utilize the best information for service delivery, decision-making and research/innovation purposes. The multitude of low-value and duplicate records also increases the cost and effort to respond to freedom of information requests and litigation searches.

David Loukidelis notes that over 350 million emails are sent and received by the provincial public service every year, requiring over 53 terabytes of storage annually. To put that in perspective, every two years government sends and receives about the same amount of data by email alone that the Hubble Space Telescope has collected and sent back to earth in over 25 years of data collection (100 terabytes). This explosion of information has significantly challenged government's record keeping practices and the appropriate solution is not to keep every single record that is generated. As Loukidelis states in his report:

*"At all costs, the provincial government should not entertain any notion that all electronic records must, regardless of their value, be retained. This would be completely contrary to modern records and information management principles. It would also be damaging to both public administration and, perversely, freedom of information and privacy."*

Loukidelis also notes that employees are uncertain as to what records are transitory, and that government's records schedules and guidance documents are out of date and need to be modernized. Government is updating its guidance documents and establishing a mandatory training program for all employees, including those in Ministers' Offices. When the IMA comes into effect, the CRO, with the support of the Information Management Advisory Committee, will update and approve outdated records schedules, to ensure that guidance to employees is clear, consistent and relevant.

## **Documenting and Retaining Valuable Information**

There are also concerns that government's policies are not clear enough on what records need to be created and retained to support and account for government's operations. In Investigation Report F13-01, Commissioner Denham called for a legislative "duty to document". David Loukidelis recommended that government seriously consider the Commissioner's recommendation. Furthermore, in January 2016, Commissioner Denham, along with her counterparts across Canada called on their respective governments to: "Create a legislated duty requiring all public entities to document matters related to their deliberations, actions and decisions."

The IMA requires ministries to retain all information they create or receive which documents key decisions; or which documents or supports a ministry's organization, policies, procedures, transactions and operations. Government Core Policy also reinforces the value of good records management, including the creation of records. One stated objective of the policy is to "create and retain a full and accurate record documenting decisions and actions".

In revising its records management policies, government will further emphasize "duty to document" principles, recognizing that understanding which records need to be created and retained sets the context for what records need not be retained. Government is also considering, as recommended by David Loukidelis, formalizing the "duty to document" requirement in legislation.

### **Legislative "Duty to Document"**

Government has accepted the Loukidelis recommendations, including the recommendation to consider a broadly-stated, legislative "duty to document", with the details to be set out in policy. We will start by developing the policy framework. This framework will give employees a better understanding of the records that they need to create and retain and the records that they can dispose of as a good records management practice.

Currently, 80% of the statutes in British Columbia contain some kind of authority for creating a record, and many program specific policies also set out documentation requirements. Any blanket "duty to document" requirement would need to take all of these authorities into account and address potential overlap and conflict.

Loukidelis noted this challenge and advised that a specific duty to document would not be appropriate at a legislative level. Instead, he recommended a broad duty to document with the details to be implemented through policy. Government agrees that this is a more workable model, and one that would permit incremental implementation, starting with the development of the policy framework.

### **"Duty to Document" in Other Jurisdictions**

Legislating a "duty to document" would make British Columbia the first province in Canada to legislate such a duty. New Zealand, the USA, and four of the six Australian states have legislated some form of a "duty to document". These legislative duties are all broadly stated and rely on supporting policies and procedures to interpret and operationalize.



While no other jurisdiction in Canada has legislated a “duty to document”, several of them are considering the matter. In our discussions with them, most have indicated that should they proceed to implement a legislative solution, the appropriate place for such a duty would be in their information management legislation, rather than their access to information legislation. Of the jurisdictions outside of Canada that have legislated a “duty to document”, all have done so in their information management legislation, not their access to information acts. This approach recognizes that creating records is the first step in the information lifecycle and integrates this requirement with other records management requirements, subject to the same oversight and policies.

Government is considering the implications of adding a broadly-stated, legislative “duty to document” in addition to the existing policy requirements and other legislative requirements to create records.

Given the direction other jurisdictions in Canada and globally have taken around implementing a “duty to document”, FOIPPA may not be the appropriate legislation in which to add such a duty. It may be more appropriate and consistent to add this duty to information management legislation.

#### **Recommendation 7:**

Consider adding a broadly-worded, legislated “duty to document” to the *Information Management Act*, with the details to be implemented through policy.

## Other Considerations

### Clarifying Privacy Impact Assessment (PIA) Requirements

The completion of a Privacy Impact Assessment (PIA) is an internationally-accepted best practice for evaluating and mitigating risks during the early development process of any public program or system. It ensures that all privacy risks are identified and addressed or mitigated before an initiative is launched. In British Columbia, PIAs are required by law to be completed during the implementation phase on all initiatives — ranging from new and amended legislation, to technical systems and government programs and policies. Ensuring that the appropriate safeguards are in place to protect personal information also reduces the likelihood of a privacy breach.

Given the significant value a PIA provides, it is important that the scope and requirements for completing a PIA are clear.

There are some areas where the current language is ambiguous or overlapping. While government has clarified these issues in policy, the legislation could be amended to clarify:

- The Minister responsible for the Act's authority to direct ministries to carry out and submit PIAs;
- The requirement for ministries to complete PIAs on current enactments, systems, projects, programs and activities where directed by the Minister;
- The requirement for ministries to complete PIAs on all changes to these initiatives, including the expansion of data-linking initiatives; and
- That only one PIA need be completed where several public bodies are jointly involved in a data-linking initiative.

Legislative amendments could address these issues, providing clearer authority for the Minister to direct ministries to carry out and submit PIAs in appropriate circumstances, and to address any lack of clarity in the legislation.

#### **Recommendation 8:**

Amend section 69 of the Act to clarify when and how a Privacy Impact Assessment (PIA) must be completed and to provide clearer authority for the Minister to issue directions on conducting and submitting PIAs.

### Streamlining and Clarifying the Commissioner's Powers

Government is supportive of amendments proposed by past committees to streamline and clarify the Commissioner's review and complaint handling processes. Parts 4 and 5 of FOIPPA set out the Commissioner's duties, powers and functions, which include the powers to investigate complaints and review the decisions of the heads of public bodies on requests for information under FOIPPA.

Specifically, Part 4 sets out a process for the Commissioner to investigate complaints from individuals about how public bodies handled access requests and about the personal information practices of public bodies. Part 5 sets out a separate process for the Commissioner to conduct formal reviews of the same.

The current processes are rigid and the terminology for dealing with complaints and reviews is confusing, overlapping and inconsistent. In addition, some provisions lack clarity as to the Commissioner's authority. Amending the Commissioner's processes to unify and streamline them will provide greater clarity and accessibility for the public and allow for operational efficiencies for the Commissioner's office. The amendments would also create consistency between FOIPPA and B.C.'s private sector privacy legislation, the *Personal Information Protection Act* (PIPA), and provide greater flexibility with respect to applying dispute resolution methods best suited to a particular case.

#### **Recommendation 9:**

Amend Parts 4 and 5 of the Act to streamline and clarify the Commissioner's review and complaint handling processes and to ensure consistency with the *Personal Information Protection Act*.

## **Frequency of Legislative Reviews**

The committee heard a proposal from the Commissioner that it consider an amendment to section 80 (1) of FOIPPA to change the review cycle from six years to every three to four years.

Legislative amendments typically take a year or more from policy development to introduction in the House. Government's legislative planning is done on a three-year cycle. Requiring a formal review of the Act every three to four years would allow little opportunity for public bodies to effectively implement past legislative changes. Some stability is required to allow the 2,900 public bodies covered by the Act to remain compliant with legislative requirements.

Shortening the legislative review cycle would also result in new recommendations being added before past recommendations could be implemented. This would present significant challenges for government in determining the potential impacts of recommended amendments and identifying the appropriate legislative solutions.

#### **Recommendation 10:**

In considering the length of time between legislative reviews, the Committee should take into account the time required for government to develop, consult on and implement legislative proposals and the time for public bodies to effectively implement new legislative requirements.

---

## Conclusion

---

David Loukidelis provided a roadmap for improving government's FOI and records management practices, which has been incorporated into the action plan presented in this submission. Government believes that this action plan will result in significant service improvement and increased access to information, and trusts that this information will be helpful to the committee in preparing its report.

In addition, government has made a number of recommendations for the committee's further consideration, which are summarized below.

---

## Summary of Recommendations

---

### **Recommendation 1:**

Current privacy provisions in FOIPPA already protect the identities of individuals who make FOI requests, ensuring that the names of applicants are only shared on a "need to know" basis. Further protection would add little value and could limit public bodies' ability to provide the best service to applicants.

To ensure that knowledgeable employees are able to assist applicants with their requests, specific criteria for the protection and provision of an applicant's identity for the purpose of processing an FOI request should continue to be governed by policy.

### **Recommendation 2:**

Comprehensive consultation should be conducted with impacted public bodies on the scope, wording and timing of any proposed amendment to FOIPPA that requires the mandatory notification and reporting of privacy breaches.

### **Recommendation 3:**

Government should continue to monitor changes to privacy laws in other jurisdictions within Canada as well as abroad, especially the European Union General Data Protection Regulations, to ensure that B.C.'s approach remains harmonized. Government should also monitor emerging technology solutions to ensure that the data residency requirements remain relevant and practical in a changing technical environment.

### **Recommendation 4:**

Comprehensive consultation should be conducted with impacted public bodies on the implications of a legislated requirement to implement a privacy management program. In particular, consideration should be given to the level of specificity of the amendment. A higher-level requirement that permits different implementation options may be preferable to a one-size fits all approach.

### **Recommendation 5:**

To avoid overlapping or conflicting jurisdiction, oversight of the appropriate destruction of records should remain with the *Information Management Act*.

### **Recommendation 6:**

Government should monitor and evaluate the efficacy of existing training and compliance programs and consider increased oversight and penalties to the *Information Management Act* if needed.

### **Recommendation 7:**

Government should consider adding a broadly-worded, legislated “duty to document” to the *Information Management Act*, with the details to be implemented through policy.

### **Recommendation 8:**

Amend section 69 of the Act to clarify when and how a Privacy Impact Assessment (PIA) must be completed and to provide clearer authority for the Minister to issue directions on conducting and submitting PIAs.

### **Recommendation 9:**

Amend Parts 4 and 5 of the Act to streamline and clarify the Commissioner’s review and complaint handling processes and to ensure consistency with the *Personal Information Protection Act*.

### **Recommendation 10:**

In considering the length of time between legislative reviews, the Committee should take into account the time required for government to develop, consult on and implement legislative proposals and the time for public bodies to effectively implement new legislative requirements.

## Appendix 1: David Loukidelis' Recommendations

*The following recommendations were provided to government by former Information and Privacy Commissioner, David Loukidelis, in his December 2015 report, Implementing Investigation Report F15-03: Recommendations to the Government of British Columbia.<sup>10</sup>*

1. Government should devise, and implement, a plan to ensure that during any future data migrations, email accounts are backed up as recommended by Commissioner Denham.
2. It is recommended in the strongest possible terms that government resist any notion that all emails should be kept, or that they should all be kept in order to be vetted by archivists or records managers, who would decide which to keep. The prudent approach is to ensure that government's transitory records policy is appropriate, understood by all, and implemented by all.
3. Government needs to ensure that all ministries have the expert resources in-house necessary to ensure every reasonable effort is made to locate records in response to access requests.
4. Government should improve its training materials, and guidance resources, to provide better education and support for front-line staff searching for records. The materials and guidance should inform all staff about the policy objectives of the duty to assist, the test for search efforts expected of public bodies, and practical steps they can take to help meet the duty. Employees should be given guidance on typical steps for finding records, such as tips on how to search their email accounts. These materials should also underscore the importance of documenting all steps taken to search for records, with specific guidance on what is expected in terms of documentation.
5. IAO should ensure it continues to watch for cases where it has reason to believe records should exist, yet none are produced to it. In such instances, IAO should rapidly escalate the matter to obtain appropriate direction. This should ideally come from the deputy minister for the ministry involved (or her or his immediate delegate). Government should create policy to govern such cases.
6. Where an executive branch office does not have responsive records due to ordinary-course records management, IAO should explain why that is so. It should confirm that the ministry's records were searched and any responsive records are included in the release package. Government also should enhance public understanding by publishing information about how records management is handled as between ministries, ministers' offices and the Premier's office.
7. Government should issue a rule prohibiting anyone from triple deleting emails. It should also configure its email system so that the contents of the recover deleted items folders in all mailboxes are, as recommended by Commissioner Denham, retained for 31 days, not 14 days. Government also should dedicate effort and resources to the other associated policy and practice changes recommended elsewhere in this report.

<sup>10</sup> A full copy of the report can be found here: <http://www2.gov.bc.ca/assets/gov/british-columbians-and-our-governments/services-policies-for-government/information-management/david-loukidelis-report.pdf>

8. Government should work with Commissioner Denham and with Microsoft to ensure that all mailbox content, including deleted emails, is preserved for 13 months for legal purposes. Solutions to this might, subject to technical confirmation, include configuring government's Microsoft Exchange servers to implement a time-based in-place hold on all email mailboxes.
9. Government should change the process for handling access requests in ministers' offices by adopting the following procedures
  - (a) Each minister's office should be required to designate a career public servant as the person in charge of request processing within the office. The position of senior executive assistant is an example. The goal is to ensure that political staff involved in the day-to-day hurly-burly of political work are not in charge of searches for records.
  - (b) Whenever IAO receives a request that requires the records of a ministerial office to be searched, the designated staff person in the minister's office should be responsible for contacting all staff directly, in writing (for example, by email), setting out the wording of the request and directing that staff search for responsive records and respond in a set time.
  - (c) These emails should include clear direction on searching for records (and should underscore the duty to provide a complete and accurate response).
  - (d) Each member of the minister's staff should be required to respond directly to the assigned staff member, reporting in writing on the search and sending responsive records directly to the assigned staff member, who will then send them to IAO.
  - (e) If any member of a minister's staff has questions about the scope of a request, or about whether a record is responsive, those questions should be directed in writing to IAO. IAO should have the final say on how the request is to be interpreted.
  - (f) IAO should be required to report any failure by a ministerial staff member to respond or any failure to co-operate with IAO. This report should be made to the Premier's chief of staff and to the deputy minister for the ministry.
  - (g) Each minister's office should be required to ensure that IAO at all times has a current list, with contact particulars, for all staff in the office.
  - (h) IAO should be authorized to, where it considers it necessary in a given case or on an ad hoc basis, have access without notice to ministerial office files for the purpose of ensuring that all responsive records have been identified and produced to IAO. This includes the government email accounts, but not personal emails in them, of ministerial staff.
  - (i) Rules will be needed to ensure there is no collection of constituency records of a minister (as opposed to ministerial records, i.e., records of the ministry as a public body).
10. Government should take the following measures to enhance training for political staff in ministers' offices:

- (a) Training should be mandatory for all new ministerial staff. Each time someone is hired, that individual should be required, during orientation, to take access and privacy training.
  - (b) The training should be done by IAO on an in-person basis, in groups if necessary.
  - (c) Existing training materials should be significantly enhanced in the areas of the duty to assist and records management (notably regarding transitory records, discussed below).
  - (d) As further described below, the materials should be designed to help ensure that staff understand and comply with the duty to assist. Another goal is to ensure appropriate practices in relation to transitory records. A third goal is to ensure a sufficient understanding of records management rules and practices. This is also important for the proper management of records other than emails.
  - (e) Reference materials, or guidance, on all of these matters should be provided to ministerial staff for their reference.
  - (f) Staff should be made aware of IAO's contact centre number, so they can reach out with any compliance questions.
  - (g) The director of executive operations in the Premier's office should be responsible for ensuring that training is performed and for keeping records of this.
  - (h) Ministerial staff should be required to take refresher training periodically, at least every two years.
11. Regarding the guidance materials for ministerial staff on interpreting requests and searching for records, new materials should be created to ensure that existing (and new) ministerial staff have a proper understanding of what is expected of them. This guidance material can align with the guidance material recommended below for public servants. The material should also, however, make it clear to ministerial staff that the minister's office is part of the ministry as a public body and is not exempt from FIPPA. The guidance should also address constituency records of the minister in her or his role as a member of the Legislative Assembly, since these are not generally considered to be ministry records for FIPPA purposes. This will help staff understand where the lines are drawn. Last, the guidance should help staff understand that personal email accounts are not to be used for government business and, if they nonetheless are, that these records are not excluded from FIPPA and must be produced for request-processing purposes.
  12. The recommendations for training for ministerial staff should also apply to staff in the Premier's office. On this point, as noted at the outset of this report, the terms of reference contemplate providing training to staff in both ministers' offices and the Premier's office as early as practicable in 2016. This should be done after the enhanced training materials are prepared, which should be done as soon as practicable.
  13. Political staff who are employed in ministers' offices are appointed under the Public Service Act. This means they are subject to government policies on acceptable use of technology and on records management. They are also subject to a code of conduct for political staff. They should be required



to certify in writing that they are aware of their responsibilities under FIPPA, including the duty to assist, and are aware of applicable records management policies and rules, particularly those relating to transitory records.

14. Regarding searches for records within the Premier's office, the above recommendations about IAO authority and access to records in a minister's office should be implemented in relation to the Premier's office. So should the recommendations about FIPPA and records management training for political staff in the Premier's office, and their agreement to be bound by records management rules.
15. Government should significantly update and enhance its transitory records policy, notably in relation to emails, in light of the detailed recommendations made above in this respect. This should include a purpose statement recognizing the need for government to create records of key activities and decisions and retain them in accordance with its records management system.
16. Guidance on transitory records policy will have to be updated to support the new transitory records policy. The Government Records Service should also regularly review and update guidance to keep abreast of new issues, new types of information and new information systems in government. Updates should be informed by users' experience, through an effective feedback loop to inform guidance on transitory records.
17. Government should give serious consideration to introducing legislation, consistent with s. 53 of the Alberta Freedom of Information and Protection of Privacy Act, that would give the Information and Privacy Commissioner authority to investigate alleged unauthorized destruction of records.
18. Government should make such policy and practice changes as are necessary to ensure that any employee appointed under the Public Service Act who destroys a record, or directs or assists anyone else in doing so, with the intent to evade a request for access to the record is subject to discipline up to and including dismissal for cause. Second, government should also give serious consideration to introducing legislation, consistent with s. 92(1) of the Alberta Freedom of Information and Protection of Privacy Act, that would make it an offence to wilfully destroy a record, or direct or assist anyone else in doing so, with the intent to evade a request for access to the record.
19. Government should give the most serious consideration to Commissioner Denham's recommendation that a duty to document be created, specifically, it should seriously consider introducing legislation\* creating such a duty (with the details being worked out in policy at a ministry, even program, level). Government should consider adopting a risk-based approach, with the nature and significance of decisions, actions and transactions being used to determine which records have to be documented and in what manner.
  - \* It is recognized that government could achieve the policy objectives of such a duty through policy, not legislation. Government policy already requires the creation and retention of a full and accurate record documenting decisions and actions. Further policy could be developed ministry by ministry.
20. As regards respondent practice review and improvement, government should ensure that the information management advisory committee established under the Information Management Act has an advisory mandate to ensure that government information management policies and practices

continue to meet accepted good practice, and improve over time, as technologies and government programs evolve. To help ensure public confidence in the committee's work, government should ensure that it includes experts from outside government who have expertise in records management, archives and government administration.

21. Government also should ensure that the chief records officer under the Information Management Act establishes guidance on information management systems in order to assist ministries in achieving early compliance with their Information Management Act duties. Guidance should also be established on the steps heads should take to ensure compliance with information schedules.
22. Further, government should ensure that GRS establishes a program of regular (and spot) review of information management practices in individual ministries. GRS staff would examine the practices of a ministry and make any necessary recommendations for improvement. Each report should be provided to the information management advisory committee for review and any recommendations. The committee should also be mandated to ensure that these practice reviews inform ongoing practice improvement.
23. It is also recommended that the committee have a web presence through GRS. Practice review reports, and committee input, should be published. The committee should be required to report annually to the minister, who should make each report publicly available, such as by tabling it in the Legislative Assembly.
24. There is a clear need for interim guidance to all public servants on records management and freedom of information issues addressed in the investigation report. As soon as practicable, therefore, all public servants should be reminded of, and given specific guidance on, the duty to assist in searching for records and in interpreting access requests. The same recommendation applies for transitory records policy. It would be desirable for the head of the public service to deliver this guidance, although the Deputy Attorney General, as the deputy of the chief law officer to the Crown, could do this. Whoever does this, government should at the earliest opportunity broadcast to all public servants a written reminder, and supportive guidance, on these two issues.
25. Not all employees need to be records managers, but some level of records management training should be mandatory. A key focus should be on transitory records policy, with practical guidance on the topic. Essential areas for training are management of email and draft records. The Government Records Service has a number of useful guides on email management and draft records on its website and these could be incorporated into the training materials. This is also, nonetheless, an opportune time for the Government Records Service to revamp existing materials in light of the Information Management Act. This training should be an online orientation module for new employees. Existing employees should also be required to complete the module.
26. It is recommended that a single set of materials be prepared for freedom of information training courses and the duty to assist and transitory records portions should be substantially improved. The duty to assist portion should relate to searches for records and also interpretation of requests.

27. All ministerial staff should be required to have access and privacy training, along with a records management aspect. The training should use the integrated records management and freedom of information module recommended above. The Premier's office should be responsible for ensuring that all staff complete the training in a timely way. Staff should be required to repeat the training at least every two years.



## Summary of OIPC Recommendations and Status of Government's Response

Document	OIPC Recommendation	OIPC current appraisal and concerns	Government's Response
<b>DATA-LINKING</b>	<p>An error in the drafting of the definition for data linking has resulted in very few initiatives being subject to OIPC oversight. The definition should be broadened to include the type of initiatives that were originally intended to be covered by the 2011 FOIPPA amendments.</p> <p>As acknowledged by Deputy Minister Kim Henderson in her April 11, 2013 letter to the Commissioner, the data linking provisions as currently drafted do not achieve their intended policy objectives and this matter should be addressed at the earliest opportunity.</p>	s.13	
<b>INVESTIGATION REPORTS</b>			
<b>F11-02 – BC FERRIES (MAY 2011)</b>	Minimum delay of 24 hours between the applicant's receipt of the response and the time the response is publicly posted.		
<b>F13-01 – INCREASE IN NO RESPONSIVE RECORDS (MARCH 2013)</b>	IAO communicate to an applicant when it is aware that the records the applicant is seeking exist within a different ministry than from where the applicant has originally requested the records.		
	IAO should be reasonably confident that before narrowing a request, the result will not deprive		

## Summary of OIPC Recommendations and Status of Government's Response

	applicants of records they would otherwise receive, unless IAO informs the applicant that this may be the case. s.13
	IAO ensure that it interprets requests broadly enough to assist the applicants in obtaining the records he or she is seeking.
	Where government does not have records responsive to an access request, IAO provide an explanation to the applicant as to why this is the case.
	IAO develop a classification system that more accurately reflects where an individual who has made the same request to multiple ministries ultimately receives the records they were seeking, irrespective of how many ministries respond that they do not have records.
	Government create a legislative duty to document key decisions as a clear indication that it does not endorse "oral government" and that it is committed to be accountable to citizens by creating an accurate record of its actions.
<b>F13-03: Evaluating the Government of BC's Open Government Initiative (July 25<sup>th</sup>, 2013)</b>	<ul style="list-style-type: none"> <li>All ministries should implement s. 71 of FOIPPA without further delay and establish categories of records for disclosure on a proactive basis. These obligations should be made part of letters</li> </ul>

## Summary of OIPC Recommendations and Status of Government's Response

	of expectation for ministers and deputy ministers.	s.13
	<ul style="list-style-type: none"> <li>The minister responsible for FOIPPA should direct ministries to proactively disclose the travel and hospitality expenses of ministers, deputy ministers and assistant deputy ministers or their equivalent by purpose or event. The disclosed information should include the date of the event, destination, and expenses relating to flight, other transportation, accommodations, meals and incidentals, and the total amount spent for that particular purpose or event. This information should be published and searchable in an open data format.</li> </ul>	
	<ul style="list-style-type: none"> <li>The minister responsible for FOIPPA should direct ministries to proactively disclose calendar information of ministers, deputy ministers and senior executives or equivalent. This release should contain the names of participants, the subject and date of external meetings and be published, at minimum, on a monthly basis.</li> </ul>	
	<ul style="list-style-type: none"> <li>The minister responsible for FOIPPA should direct ministries to proactively disclose</li> </ul>	

## Summary of OIPC Recommendations and Status of Government's Response

	information relating to its contracts that are worth more than \$10,000 on (at minimum) a quarterly basis. Contract information should include with whom the government is contracting, the purpose, value and duration of that contract, and information about the procurement process for the award of the contract.	s.13
	<ul style="list-style-type: none"> <li>The minister responsible for FOIPPA should direct ministries to proactively disclose any final report or audit on the performance or efficiency of their policies, programs or activities.</li> </ul>	
	<ul style="list-style-type: none"> <li>The minister responsible for FOIPPA should direct ministries to proactively disclose the records enumerated in s. 13(2) of FIPPA on a routine basis within a set timeline.</li> </ul>	
	<ul style="list-style-type: none"> <li>The Open Information website should be used as an online library to make information that must be disclosed across government more easily accessible by providing links to that information or a search function.</li> </ul>	
	<ul style="list-style-type: none"> <li>Government should create a separate category for records that are not published on the</li> </ul>	



## Summary of OIPC Recommendations and Status of Government's Response

	disclosure log due to concerns about copyright. s.13
	<ul style="list-style-type: none"> <li>Government should review its policy regarding the disclosure of copyright material to determine whether it is permissible to publish copyright material in response to an access request. Where it is determined that records may not be published due to copyright, government should publish a severed version of the record.</li> </ul>
	<ul style="list-style-type: none"> <li>Government should include information on the Open Information website and in the annual report of the Minister of Technology, Innovation and Citizens' Services regarding responses to general access requests where there have been no responsive records.</li> </ul>
	<ul style="list-style-type: none"> <li>Government should improve the ability to search the disclosure log to allow users to find specific content more easily.</li> </ul>
	<ul style="list-style-type: none"> <li>Government should identify high value data sets for publication, particularly those that will increase the transparency and accountability of</li> </ul>

## Summary of OIPC Recommendations and Status of Government's Response

	government and work towards releasing all identified high value data sets as soon as practicable.	s.13
	<ul style="list-style-type: none"> <li>Government should commit to signing and implementing the G8 Open Data Charter as a sub-national.</li> </ul>	
	<ul style="list-style-type: none"> <li>Government should develop a single de-identification approach for ministries that includes procedures on de-identifying datasets and assessing the risk of re-identification in the context of open data.</li> <li>Government should also develop policies for reviewing data released as open data on a regular basis to assess the risk of re-identification.</li> </ul>	
	<ul style="list-style-type: none"> <li>Government should continue to collaborate with stakeholders to increase data literacy and data literacy should be considered a measure of success for the open data program.</li> </ul>	

## Summary of OIPC Recommendations and Status of Government's Response

	s.13
	<ul style="list-style-type: none"> <li>Government should incorporate access by design principles into its information management practices.</li> </ul>
	<ul style="list-style-type: none"> <li>Government should establish an external advisory board on open government comprised of users of open information and open data, as well as, data and privacy experts to inform future developments in open government.</li> </ul>
	<ul style="list-style-type: none"> <li>The Document Disposal Act should be replaced with a modern archives and records management statute.</li> <li>The government also should act now to develop an archiving policy for its Open Information website, to enable citizens to continue to access records that have been removed from the active site. Indices of archives and the policy should be posted on the Open Information website.</li> </ul>
<b>F13-04 – Sharing of Personal Information as part of the Draft Multicultural Strategic</b>	<ul style="list-style-type: none"> <li>Government should provide training for its employees regarding the use of personal email accounts.</li> </ul>

## Summary of OIPC Recommendations and Status of Government's Response

Outreach Plan (August 2013)		s.13
	<ul style="list-style-type: none"> <li>Government should ensure that copies of all records created by its employees that relate to government business are located in government-controlled information management systems</li> </ul>	
	<ul style="list-style-type: none"> <li>Government should provide its employees with sufficient technical resources to ensure that they do not have a reason to use personal email accounts in the performance of their government duties.</li> </ul>	
	<ul style="list-style-type: none"> <li>Government should ensure that employees with roles that are closely tied to the governing party participate in mandatory training sessions regarding the need to keep personal information obtained in their government role separate from personal information obtained in any role they might have with the political party.</li> </ul>	
Investigation Report F13-05: Public Body Disclosure of Information Under Section 25 of the <i>Freedom of Information and Protection of Privacy Act</i>	<p>Public bodies should develop policies that provide guidance to employees and officers about the public body's obligations under s. 25 of FIPPA.</p> <ul style="list-style-type: none"> <li></li> </ul>	

## Summary of OIPC Recommendations and Status of Government's Response

(Dec. 2, 2013)		s.13
	Public bodies should ensure that its employees and officers understand the public body's obligations under s. 25 of FIPPA and are provided with adequate training to ensure compliance with these obligations	
	Government should amend s. 25(1)(b) of FOIPPA to remove the requirement of temporal urgency so that there is a mandatory obligation for public bodies to disclose all information that is clearly in the public interest to disclose.	
<b>F14-01: Use of Police Information Checks in British Columbia (Apr. 15, 2014)</b>	<ul style="list-style-type: none"> <li>Government and municipal police boards should immediately mandate that police apprehensions collected under the authority of s. 28 of the Mental Health Act should never be included in a police information check.</li> </ul>	
	<ul style="list-style-type: none"> <li>Government should legislatively mandate that</li> </ul>	

## Summary of OIPC Recommendations and Status of Government's Response

	<p>non-conviction information cannot be used in record checks outside of the vulnerable sector.</p>	s.13
	<ul style="list-style-type: none"> <li>At the direction of government and municipal police boards, police agencies should implement a model for conducting record checks that will allow individuals to request only relevant conviction information for record checks for positions outside of the vulnerable sector.</li> </ul>	
	<ul style="list-style-type: none"> <li>Government should legislatively mandate that the centralized office in place under the CRRA should conduct all vulnerable sector checks in British Columbia. The current process for mandatory checks under the CRRA for provincially-funded employers would remain the same. Where an employer or volunteer agency</li> </ul>	

## Summary of OIPC Recommendations and Status of Government's Response

	<p>that is not currently subject to the CRRA chooses to require a prospective employee or volunteer in the vulnerable sector to undergo a record check, it would be conducted in the same manner as set out by the CRRA.</p>	s.13
	<ul style="list-style-type: none"> <li>Government and municipal police boards should direct municipal police departments to immediately stop releasing non-conviction information for police information checks not involving the vulnerable sector.</li> </ul>	
<b>F15-02 Review of the Mount Polley Mine Tailings Pond Failure and Public Interest Disclosure by Public Bodies</b>	<ul style="list-style-type: none"> <li>I recommend that the Ministry of Energy and Mines and the Ministry of Environment promptly assess what information in relation to the failure of the Mount Polley tailings pond dam, if any, must be disclosed pursuant to s. 25(1)(b) as being clearly in the public interest.</li> </ul>	

## Summary of OIPC Recommendations and Status of Government's Response

	<ul style="list-style-type: none"> <li>I recommend that all public bodies diligently and promptly assess what information, if any, must be disclosed pursuant to s. 25(1)(b) as being clearly in the public interest.</li> </ul>	s.13
	<ul style="list-style-type: none"> <li>All public bodies must develop policies that provide guidance to employees and officers about the public body's obligations under s. 25 of FIPPA, and update existing policies to reflect the revised interpretation of s. 25(1)(b) described in the investigation report.</li> </ul> <p><i>"I conclude that public bodies must disclose information pursuant to s. 25(1)(b) where a disinterested and reasonable observer, knowing what the information is and knowing all of the circumstances, would conclude that disclosure is plainly and obviously in the public interest. Section 25(1)(b) will no longer be interpreted to require an element of temporal urgency in order to require the disclosure of information that is clearly in the public interest pursuant to s. 25(1)(b)."</i></p>	
<b>F15-03 Access Denied: Record Retention and Disposal Practices of the Government of British Columbia</b>	<ul style="list-style-type: none"> <li>The Ministry of Transportation and Infrastructure should release the 36 pages of records initially identified as responsive to the applicant's access request, with severing as allowed under FIPPA, made on November 19, 2014 for:               <ul style="list-style-type: none"> <li>"... all government records that make reference to the issue of missing women along Highway 16 / the Highway of Tears and specifically including records</li> </ul> </li> </ul>	



## Summary of OIPC Recommendations and Status of Government's Response

	related to meetings held by the ministry on this issue. The time frame for my request is May 15 to November 19, 2014."	s.13
	<ul style="list-style-type: none"> <li>Government should develop a policy for all future data migrations that requires at a minimum:               <ol style="list-style-type: none"> <li>Hourly, daily and monthly backup of data;</li> <li>Written directions to government's service provider with respect to these backups; and</li> <li>Government monitoring of the directions to ensure their compliance.</li> </ol> </li> </ul>	
	<ul style="list-style-type: none"> <li>The Ministry of Advanced Education should release the approximately 20 email records identified as responsive to the applicant's access request, with severing as allowed under FIPPA, made on July 21, 2014 for:               <ul style="list-style-type: none"> <li>"Any emails sent by Nick Facey, Chief of Staff to Minister Amrik Virk. Timeframe is February 1, 2014 to July 16, 2014."</li> <li>The Investigations and Forensics Unit will retrieve the emails and provide them to the Ministry.</li> </ul> </li> </ul>	
	<ul style="list-style-type: none"> <li>The Executive Branch of the Office of the Premier should change its access to information processes to ensure that requests for records are communicated by email in a timely manner and properly documented.</li> </ul>	
	<ul style="list-style-type: none"> <li>Government should clarify access requests with</li> </ul>	

## Summary of OIPC Recommendations and Status of Government's Response

	<p>applicants where necessary to ensure it does not interpret the request too narrowly and to maximize the likelihood of producing records that are responsive to the applicant's request.</p>	s.13
	<ul style="list-style-type: none"> <li>Government should create clear guidance for employees on how to conduct a thorough search for potentially responsive records to an access request. This guidance should be incorporated into government's access to information training and should specifically include that employees should conduct searches from their desktop or laptop and not from mobile devices.</li> </ul>	
	<ul style="list-style-type: none"> <li>Government should provide mandatory records management training to all employees, that includes the identification of transitory and non-transitory records and the process for retaining and destroying records. This training should describe employees' responsibilities for records management and provide the basis for understanding an office's record keeping system.</li> </ul>	
	<ul style="list-style-type: none"> <li>Government should legislate independent oversight of information management requirements, such as the destruction of records, including sanctions when those requirements are not met.</li> </ul>	
	<ul style="list-style-type: none"> <li>Government should configure the settings in Microsoft Outlook to prevent employees from removing items from the Recover Deleted Items folder.</li> </ul>	

## Summary of OIPC Recommendations and Status of Government's Response

	<ul style="list-style-type: none"> <li>Government should configure the settings in Microsoft Outlook so that it preserves items in the Recover Deleted Items folder for just over one month. This would ensure all government emails are captured in monthly backups.</li> </ul>	s.13
	<ul style="list-style-type: none"> <li>Government should create a legislative duty to document within FIPPA as a clear indication that it does not endorse "oral government" and that it is committed to be accountable to citizens by creating an accurate record of its key decisions and actions.</li> </ul>	
<b>Special Reports</b>		
<b>A Failure to Archive – Recommendations to Modernize Government Records Management (July 22, 2014)</b>	<ul style="list-style-type: none"> <li>Government should repatriate the BC Archives into government and fund it on the same basis as other valuable public programs.</li> <li>Alternatively, government should develop a policy or legislative framework where the fees to archive records are set on a basis that is acceptable to both government and the Royal British Columbia Museum rather than the current unilateral process set by the Museum. Ministries should then be provided with sufficient resources to enable the transfer of records to the BC Archives.</li> <li>To address the backlog of 33,000 boxes of records, government should provide funding to the Royal British Columbia Museum from the 2014/15 Estimates – Contingencies in an amount to be determined.</li> </ul>	
	<ul style="list-style-type: none"> <li>The Minister of Technology, Innovation and Citizens' Services should initiate the creation or</li> </ul>	

## Summary of OIPC Recommendations and Status of Government's Response

	<p>procurement of an electronic records archiving infrastructure to ensure the management and archival preservation of government's electronic records.</p> <ul style="list-style-type: none"> <li>• The repository for the electronic archives should be within the Ministry and should be publically funded.</li> </ul>	s.13
	<ul style="list-style-type: none"> <li>• Recognizing changes in information management in the last decade, Government should replace the Document Disposal Act of 1936 with a modern statutory framework to address the needs and realities of the digital age.</li> </ul>	
	<ul style="list-style-type: none"> <li>• Provincial archivist should play a prominent role in decisions around the creation of electronic records as well as the approval of retention schedules.</li> </ul>	
	<ul style="list-style-type: none"> <li>• Process for approval of records schedules should be more efficient and should not require the approval of the Legislature of the Public Accounts Committee.</li> </ul>	

## Summary of OIPC Recommendations and Status of Government's Response

		s.13
	<ul style="list-style-type: none"> <li>• Should provide for oversight of information management requirements and for sanctions when those requirements are not met.</li> </ul>	
<b>A Step Backwards: Report Card on Government's Access to Information Responses April 1, 2013 – March 31, 2014 (Sept. 23, 2014)</b>	<ul style="list-style-type: none"> <li>• Government should define and implement steps to eliminate the backlog of access to information requests and, in the forthcoming budget cycle, should give priority to providing more resources to dealing with the greatly increased volume of access requests.</li> </ul>	
	<ul style="list-style-type: none"> <li>• As recommended in my report entitled A Failure to Archive: Recommendations to Modernize Government Information Management, government should adopt a modern statutory framework to address the needs and realities of the digital age, recognizing the importance for government to effectively track records from</li> </ul>	

## Summary of OIPC Recommendations and Status of Government's Response

	their creation through to their archiving.	s.13
	<ul style="list-style-type: none"> <li>After discussion and agreement between government and the political parties currently making calendar requests, the minister responsible for FOIPPA should develop a system to proactively disclose calendar information of ministers, deputy ministers, assistant deputy ministers, as well as, certain other staff whose calendars are routinely the subject of access to information requests. This release should, at a minimum, contain the names of participants, the subject and date of meetings and be published on a monthly basis.</li> </ul>	
	<ul style="list-style-type: none"> <li>The Ministry of Children and Family Development should give attention on a priority basis to its statutory obligation under FOIPPA to respond to access to information requests within legal timelines. Planned actions should include addressing elements such as printing and retrieving difficulties regarding the ICM system, staff levels related to access to information and providing effective ongoing training to ICM users.</li> </ul>	
	Government should ensure it builds access and privacy into any new information management system at the design stage in order to ensure the system operates from a records management perspective, as well as, from a program perspective.	

## Summary of OIPC Recommendations and Status of Government's Response

		s.13
	Where government does not have records responsive to an access to information request, IAO should provide a brief explanation to the applicant as to why this is the case.	
	Government should implement the Capstone or a similar email management system with respect to senior government officials to document its key decisions. This system should also be adopted by the Office of the Premier and Ministerial offices.	
<b>An Examination of The Government of BC'S Privacy Breach Management (January 2015)</b>	Government establish an ongoing privacy compliance monitoring function within the OCIO that: a.) Reviews processes, policies & training government-wide, to ensure that breaches are promptly reported to the OCIO and that affected individuals are notified without delay; b.) Conducts regular follow-up with ministries to ensure full implementation of prevention strategies and recommendations provided through the breach	

## Summary of OIPC Recommendations and Status of Government's Response

	<p>investigation process;</p> <p>c.) Reviews privacy and security safeguards within ministries and service providers;</p> <p>d.) Conducts regular cross-government analysis of the causes and potential solutions to privacy breaches; and</p> <p>e.) Publicly reports detailed information relating to breaches, bodies, responsibilities, types and causes, and preventative measures annually.</p>	s.13
	<p>Government adopt the following interim breach reporting requirements:</p> <p>a.) Document risk evaluation processes and decisions regarding notification of affected individuals and reporting to the OIPC; and</p> <p>b.) Report all suspected breaches to the OIPC if the suspected breach:</p> <ul style="list-style-type: none"> <li>- Involves personal information; and</li> <li>- Could reasonably be expected to cause injury or harm to the individual and/or involves a large number of individuals.</li> </ul>	
	<p>The OCIO to:</p> <p>a.) Review and amend breach categories and category definitions;</p> <p>b.) Ensure fulsome and accurate collection and documentation of privacy breach incidents;</p> <p>c.) Ensure ministry tracking of the OCIO file number; and</p> <p>d.) Ensure OCIO tracking of the OIPC file number.</p>	
	<p>The OCIO to:</p> <p>a.) Review and amend policy documents relating to</p>	



## Summary of OIPC Recommendations and Status of Government's Response

	<p>privacy breach management; and</p> <p>b.) Provide basic guidance or training for privacy breach investigative staff as well as ministry information and security staff relating to amendments made.</p>	s.13
	<p>Government to:</p> <p>a.) Provide ongoing training and awareness of the importance of protecting personal information and breach management processes; and</p> <p>b.) Increase staff (and service provider, if applicable) participation rates in this training.</p>	
<b>OTHER</b>		
<b>Subsidiary Corporations</b>	We have asked that government amend FIPPA to	

## Summary of OIPC Recommendations and Status of Government's Response

(various letters, including June 11, 2014)	ensure that subsidiary corporations of local public bodies are covered. s.13
<b>Adding PRIMECorp to Schedule 2 (2012)</b>	We asked for PRIMECorp to be added
<b>BC Services Card (Feb. 2013)</b>	We recommended public consultation about the implementation of BC Services Card.
<b>Statement from BC Privacy Commissioner regarding the results of government's public consultation on the BC Services Card (Apr 1, 2014)</b>	The need for public consultation on the BC Services Card is not over. Future public consultations are required as the system is architected and new services are contemplated.
<b>Open Letter to Minister Wilkinson regarding the designation of police associations as public bodies under FOIPPA. (Apr. 2, 2014)</b>	Recommend that the BC Association of Chiefs of Police and the BC Association of Municipal Chiefs of Police be added as public bodies under FOIPPA.

## Summary of OIPC Recommendations and Status of Government's Response

			s.13
--	--	--	------



## **Issue 3:**

## **DUTY TO ASSIST**

### **I. ISSUE**

Options for implementing recommendations respecting the "Duty to Assist".

### **II. BACKGROUND**

The "duty to assist" is a legal obligation on heads of public bodies to make every reasonable effort to respond openly, accurately, completely and without delay to a request for access to information under the *Freedom of Information and Protection of Privacy Act* ("FOI request").

#### ***"Access Denied"***

In her October 2015 investigation report, *"Access Denied"*, the Information and Privacy Commissioner found several deficiencies in the way that government had processed and responded to FOI requests. This included interpreting requests too narrowly, failing to clarify requests with applicants and conducting inadequate and undocumented searches for records.

#### **Loukidelis Recommendations**

In his report, David Loukidelis recommended that government develop guidance and training materials that inform employees of their "duty to assist" applicants who make FOI requests. This should include guidelines on interpreting and clarifying requests, and conducting a thorough and documented search for records. He also recommended that government provide better explanations to applicants when no records are produced in response to their request (including, where applicable, why government business records would not typically be located in a minister's office or the Office of the Premier).

### **III. DISCUSSION**

s.13

Page 070 to/à Page 071

Withheld pursuant to/removed as

s.13

**IV. OPTIONS**

s.13

**V. EVALUATION**

s.13

**VI. RECOMMENDATION**

s.13

**VII. DECISION**

s.13

Presentation to the Special Committee to  
Review the *Freedom of Information and Protection  
of Privacy Act*

---

March 16, 2015

Slide 1 – Cover page

Slide 2 - Opening Remarks

- Good morning;
- Members of the Committee, thank you for inviting me to be here today to contribute to this valuable process.
- My name is Cheryl Wenezenki-Yolland and I am the Government Chief Records Officer and Associate Deputy Minister with the Ministry of Finance.

*Regrets from the Minister*

- Minister De Jong sends his regrets — he would have liked to be here to speak with you about government's commitment to improving access to information and privacy protection in British Columbia.



# CONFIDENTIAL ADVICE:

## Slide 2 - Opening Remarks

### *Introductions*

- With me today are my three colleagues —
  - David Curtis, Assistant Deputy Minister of Corporate Information & Records Management;
  - Charmaine Lowe, Executive Director of Strategic Policy and Projects; and
  - Sharon Plater, Executive Director of Privacy, Compliance and Training.
- We all represent the newly-formed Corporate Information and Records Management Office in the Ministry of Finance.
- Along with our colleagues in Records Management and Access to Information, we are breaking new ground in B.C. by establishing an integrated and comprehensive information management program that recognizes the

## CONFIDENTIAL ADVICE:

significant overlap between the disciplines of privacy, access, and records management.

- Later in this presentation you'll hear much more about the important initiatives we've already launched under this new program.

### Slide 3 – Key Themes

#### *What the Committee will find in the submission*

- We have provided a detailed submission for your consideration.
- The written submission before you sets out government's action plan to improve information management practices in British Columbia. This includes
  1. Sets out government's response to the Loukidelis recommendations;
  2. Describes actions government has taken or is taking to improve access to information and privacy generally;

-

## CONFIDENTIAL ADVICE:

### Slide 3 – Key Themes

3. Reiterates several of the key themes from government's previous presentation;
4. Makes recommendations for your consideration as you prepare your report.

### *What we are going to talk about today*

- While I will touch on material contained in our written submission, my primary focus is the steps government is taking to address the recommendations David Loukidelis made to government on how to improve FOI and records management practices.

I want to express our sincere commitment to changing the way we do information management, including

- Improving the FOI process,
- Protecting privacy, and
- Improving records management practices.

# CONFIDENTIAL ADVICE:

## Slide 3 - Key Themes

- The actions government has undertaken to address the Loukidelis recommendations which will be the focus of our discussion today:

### **1.A Revitalized Service Culture**

We have made a commitment to a revitalized service culture in Information Management.

### **2.Improving access to information**

This includes improvements government has made to access to information since receiving the Loukidelis report in December.

### **3.Proactive Disclosure**

It also includes steps we've taken or will take soon to increase proactive disclosure of information.

### **4.Enhancing privacy**

I'll talk about steps we've already taken to enhance privacy, including the recent launch of

## CONFIDENTIAL ADVICE:

### Slide 3 - Key Themes

the *Privacy Management and Accountability Policy*, a roadmap that articulates the policy requirements for a strong privacy management program for ministries.

Alongside this policy, we have established improved procedures, training, and education and awareness measures.

### **5. Increasing oversight and compliance**

I want to tell you about steps we've taken towards increasing oversight and compliance in the information management space, including

- The integrated approach we're taking to privacy, access, and records management in BC to support modern, digital information practices, ultimately improve citizens' access to information.
- We are also in the process of establishing a comprehensive information management Compliance and Audit program.

## CONFIDENTIAL ADVICE:

### Slide 3 - Key Themes

#### **6.Improving records management practices and advancing a duty to document.**

- Finally, I want to talk to you about what Government is doing to ensure that records are being created appropriately — you’ve heard this referred to in other presentations as the “duty to document”

### Slide 4 - Government’s Commitment

- Government is committed to ... (Read Slide)

### Slide 5 - Background and Context

### Slide 6 –Loukidelis Report

- In November, this committee heard from my colleague and Government Chief Information Officer Bette-Jo Hughes about the key challenges, opportunities and priorities government had identified with respect to the *Freedom of Information and Protection of Privacy Act* (which I will refer to as “FOIPPA”).

## CONFIDENTIAL ADVICE:

### Slide 6 –Loukidelis Report

- At that time, Government had engaged former Information and Privacy Commissioner David Loukidelis to prepare an action plan for responding to current Information and Privacy Commissioner's findings in her recent investigation report.
- However, we had not yet received Mr. Loukidelis' report.
- Therefore, we committed to provide a second briefing after the receipt of the Loukidelis report, and to provide a comprehensive written submission, as well.
- In December, we received Mr. Loukidelis' report, which contained 27 recommendations for actioning the recommendations made by the Information and Privacy Commissioner in her recent investigation report.

## **CONFIDENTIAL ADVICE:**

### **Slide 6 –Loukidelis Report**

- We have accepted all of Mr. Loukidelis' recommendations. In many cases, we have committed to go above and beyond what he and the Information and Privacy Commissioner have proposed.

### **Slide 7 – Program Alignment with Finance**

- The Commissioner made the analogy — and we agree — that information assets should be treated with the same diligence and discipline as financial assets.
- The transfer of responsibility for information management to the Ministry of Finance and the integration of the information management disciplines under one cohesive program were important first steps.
- The Ministry of Finance also houses the Public Service Agency — collaboration and alignment with that agency will be key in moving forward



## **CONFIDENTIAL ADVICE:**

with the training and change management that you'll find are key focuses of our approach.

### **Slide 8 - B.C.'s First Chief Records Officer**

- Alignment and integration of FOI, privacy, and records management will enable us to provide streamlined, comprehensive policy controls, training and compliance.
- Importantly, this integration also provides for a broad and comprehensive oversight role by the CRO.
- The CRO's mandate and oversight authority will be formalized when the new Information Management Act comes into force.

### **Slide 9 - Information Management Act**

- B.C.'s current records management legislation is 80 years old this year.

## **CONFIDENTIAL ADVICE:**

### **Slide 9 - Information Management Act**

- The new Information Management Act, which received Royal Assent in May 2015, will be brought into force soon.
- In addition to formalizing my mandate as CRO, it will
  - Streamline approval processes for records schedules; and
  - Permit the establishment of an Information Management Advisory Committee
- This in turn will enable outdated records schedules to be updated and approved much more efficiently.

### **Slide 10 Information Management in Context**

### **Slide 11 What is Information management?**

- I want to give you an overview of information management

## CONFIDENTIAL ADVICE:

### Slide 11 What is Information management?

- The first thing that you need to understand is that information is governed under different legislation
- As is the case in most jurisdictions, privacy and access are governed under freedom of information legislation
- Creation, retention and disposal of information is governed under information management legislation - in British Columbia the new Information Management Act
- While these areas of expertise are discrete, alignment between them is important, as there are many commonalities between them.
- In order to improve and streamline information management across government we have integrated these key disciplines into one comprehensive corporate governance program.

## CONFIDENTIAL ADVICE:

### Slide 12 – Information Lifecycle

- Information must be managed throughout its lifecycle from its creation or collection all the way through to its eventual disposal or permanent preservation.
- There are key considerations that must be considered at each stage of the lifecycle
- For example, information must be retained in accordance with approved records schedules
- Access and use is governed by FOIPPA, but information must also be easily retrievable to support government operations
- Disposal of information can only occur in accordance with an approved records schedule, but also must be done securely to protect personal and confidential information
- It is important to understand the interdependencies and the overlapping nature of

## **CONFIDENTIAL ADVICE:**

FOIPPA and IMA as you consider recommended proposals for change

### **Slide 13 - Improving Access to Information**

- British Columbia's Freedom of Information and Protection of Privacy Act (FOIPPA) provides the broadest privacy and access coverage in Canada.
- Over 2,900 public bodies are covered under the legislation.
- The Loukidelis report highlighted several areas for improvement in the government FOI process.

### **Slide 14 – Revitalized Service Culture**

- To support a revitalized service culture government is developing a communication and change management strategy
- This strategy will incorporate these key principles for service excellence including
  - Transparency,
  - Accountability,

## CONFIDENTIAL ADVICE:

### **Slide 14 – Revitalized Service Culture**

- Subject matter expertise
  - Timeliness
  - Fairness
  - Improved service orientation
- 
- Regular communication and messaging will be integrated into the release of new policies, guidelines, and training programs
  - Supported by senior executive committees
  - I will personally support this strategy with regular communications and bulletins from my office

### **Slide 15 – Focus on Access**

- We want applicants to see a noticeable difference in how the FOI process works.

## CONFIDENTIAL ADVICE:

### Slide 15 – Focus on Access

- We want to support a deep culture where all employees recognize and promote the “Duty to assist”
- We want to ensure that where it is necessary to clarify an FOI request, they are clarified by ministry staff that have the best possible knowledge of the records and business processes.
- We will standardize the requirements for conducting and documenting searches for records
- We are committed to improving both timeliness and responsiveness.
  - This includes providing a clear explanation to applicants when their request results in no records being found.

## CONFIDENTIAL ADVICE:

### **Slide 16 - New FOI Process for Ministers' Offices**

- One of David Loukidelis' recommendations was that the responsibility for responding to FOI requests in Ministers' offices should be assigned to a career public servant
- We have moved forward with this recommendation and have developed a new FOI process for ministers offices.
- A designated contact in a Deputy Minister's office will be responsible for overseeing the requests to a Minister's Office.
- These contacts will receive expedited training and guidance, and, like all staff, will be required to keep their training up-to-date by refreshing it every two years.
- These contacts will be responsible for ensuring search processes are followed, and will be supported in escalating any issues or concerns that may arise about the response to any request.



## CONFIDENTIAL ADVICE:

### Slide 17- Proactive Disclosure

- Since 2011, British Columbia has been a leader in Open Government, proactively working to provide citizens with access to the information that matters most to them.
- Greater proactive disclosure creates opportunities for citizens to participate in government and collaborate on decisions being made; and improves awareness, understanding and dialogue.
- Currently we publish responses to General FOI requests and summaries of Ministers' and Deputy Ministers' travel expenses.
- We are looking at adding many more categories of information, including:
  - Ministers' travel receipts
  - Purchase card information
  - Ministers' and Deputy Ministers' calendars
  - Government contract information
  - Direct award summaries

## CONFIDENTIAL ADVICE:

- I should note that this is in addition to the over 2,000 data sets available on the DataBC website.

### **Slide 18 - Enhancing Privacy Protection**

### **Slide 19 - British Columbia's Leading Privacy Practices**

- B.C.'s data residency provisions — which dictate that personal information must be stored and accessed only within Canada — are the strongest in the country, demonstrating BC's steadfast commitment to robust, responsive privacy protections.
- B.C. was the first province in Canada to enshrine a requirement for Privacy Impact Assessments (PIAs) in legislation, and remains one of the only jurisdictions with this type of obligation.
- B.C.'s mandatory privacy training for all public service employees and for service providers who collect or create personal information is the farthest-reaching program of its kind in Canada.

## CONFIDENTIAL ADVICE:

### Slide 19 - British Columbia's Leading Privacy Practices

- B.C. is also among the few jurisdictions that publish a Personal Information Directory (PID).
- The PID contains summaries of Privacy Impact Assessments, Information Sharing Agreements, and Personal Information Banks.
- These summaries are available on government's DataBC website.
- Publishing these summaries offers a high level of insight into how government manages the personal information in its custody or under its control.
- We are also the only province in Canada with a central privacy breach response unit that is on call 24 hours a day.

## CONFIDENTIAL ADVICE:

### **Slide 20 - Enhancing Privacy Management, Accountability and Oversight**

- In February 2016, we launched the new comprehensive privacy management policy — the first of its kind in Canada.
- This a significant step forward in improving how we manage the personal information in our care.
- The cornerstone of the PMAP is the required designation of a Ministry Privacy Officer for each ministry.
- Another key element of government's privacy management program is the creation of a multi-faceted compliance monitoring, review and audit program.
- Unique among other jurisdictions in Canada, this program includes baseline assessments of each ministry, ad hoc reviews where deemed necessary and an annual self-audit to promote maintenance and growth.

## **CONFIDENTIAL ADVICE:**

### **Slide 21 -Increased oversight and compliance**

### **Slide 22 – Increasing Oversight in Information Management**

- Once the IMA comes into effect, new information management policies and best practices will be established
- A comprehensive information management compliance program will be developed to review information management systems and practices
- This will be supported by our mandatory information management training

### **Slide 23 Mandatory Training**

- Our mandatory information management training will begin in April this year with all employees being trained by the end of March 2017
- The training will be:
  - Mandatory
  - Monitored, and
  - Refreshed every two years

## **CONFIDENTIAL ADVICE:**

### **Slide 24 - Improving Records Management practices and Advancing the Duty to Document**

#### **Slide 25 - Information explosion**

- Advances in technology has made it easier than ever to create and retain records
- Daily use of email and social media, has resulted in an information explosion over the last 2 decades
- Governments record keeping practices need to be modernized
- We are literally drowning in information

#### **Slide 26 - Impact on Records Management**

- DL notes that over 350 million emails are sent and received by government every year
- This results in 53 terabytes of storage annually
- This presents significant challenges to governments records keeping practices

## CONFIDENTIAL ADVICE:

- But the solution is not to keep every record that is generated
- At Loukidelis states in his report (Read Slide)

### **Slide 27 - Documenting and Retaining Valuable Information**

- The IMA requires the retention of all information that documents key decisions
- This is reinforced by governments Core Policy and Procedures
- However, there are concerns that government is not in all cases creating the records that it needs to support government operations and accountability
- As government considers a legislative document we will work on further emphasizing the duty to document principle in the revisions that we are making to our records management policy

## CONFIDENTIAL ADVICE:

- A key consideration is the appropriate enactment for the duty to document

### **Slide 27 - Documenting and Retaining Valuable Information**

- All other jurisdictions that have a legislative duty to document do so in their information management legislation not their access to information legislation
- This approach recognizes that creating records is the first step in the information lifecycle
- Integration of this requirement with other records management requirements is important for clarity and implementation of business processes

### **Slide 28 – Conclusion**

- Government is taking action on all of the Loukidelis Recommendations,



## CONFIDENTIAL ADVICE:

We are also committed in going further by:

- revitalizing the service culture around access to information
  - creating a comprehensive compliance review and training program
  - Making more information available to the public through proactive disclosure
- 
- Thank you for your attention. I would be pleased to take your questions.

# Presentation to the Special Committee to Review the *Freedom of Information* *and Protection of Privacy Act*

March 16, 2016



Ministry  
of Finance

Trusted financial and economic leadership for a prosperous province

# Who We Are

## **Corporate Information and Records Management Office**

- Newly integrated office
- Responsible for information management legislation, policies, and procedures including:
  - Privacy;
  - Access to Information;
  - Records Management; and
  - Proactive Disclosure.

# Key Themes

- **A Revitalized Service Culture**
- **Improving Access to Information**
- **Proactive Disclosure**
- **Enhancing Privacy Protection**
- **Increasing Oversight and Compliance**
- **Improving Records Management and Advancing a “Duty to Document”**

# Government's Commitment

- ✓ Service excellence
- ✓ Improved information and records management practices
- ✓ Enhanced transparency and accountability
- ✓ Strong protection of privacy and security of information

# Background and Context

# The Loukidelis Report

- In November of 2015, the Government Chief Information Officer addressed this Committee
  - David Loukidelis' review of Commissioner's Denham's report was underway at the time
- In December of 2015, David Loukidelis provided his report to government
- Government has accepted all 27 recommendations made by Loukidelis and has committed to going above and beyond the recommendations in many cases

Government is committed to improving access to information for British Columbians

# Program Alignment with Finance

- Change in how we think about information – focus on People, Behaviour and Training, Customer Service (Culture)
- Better alignment with PSA
- Information is a critical asset and we need to work with employees across government to manage it as such – including protecting privacy and applying security controls

We need to exercise the same due diligence with information assets that we do with financial assets



# B.C.'s First Chief Records Officer

- Brings FOI, privacy and records management policy, training and oversight together
- The CRO's mandate and oversight authority will be formalized when the new *Information Management Act* comes into force

Alignment and integration of FOI, privacy, and records management will streamline and enhance policy controls, training and compliance

# *Information Management Act*

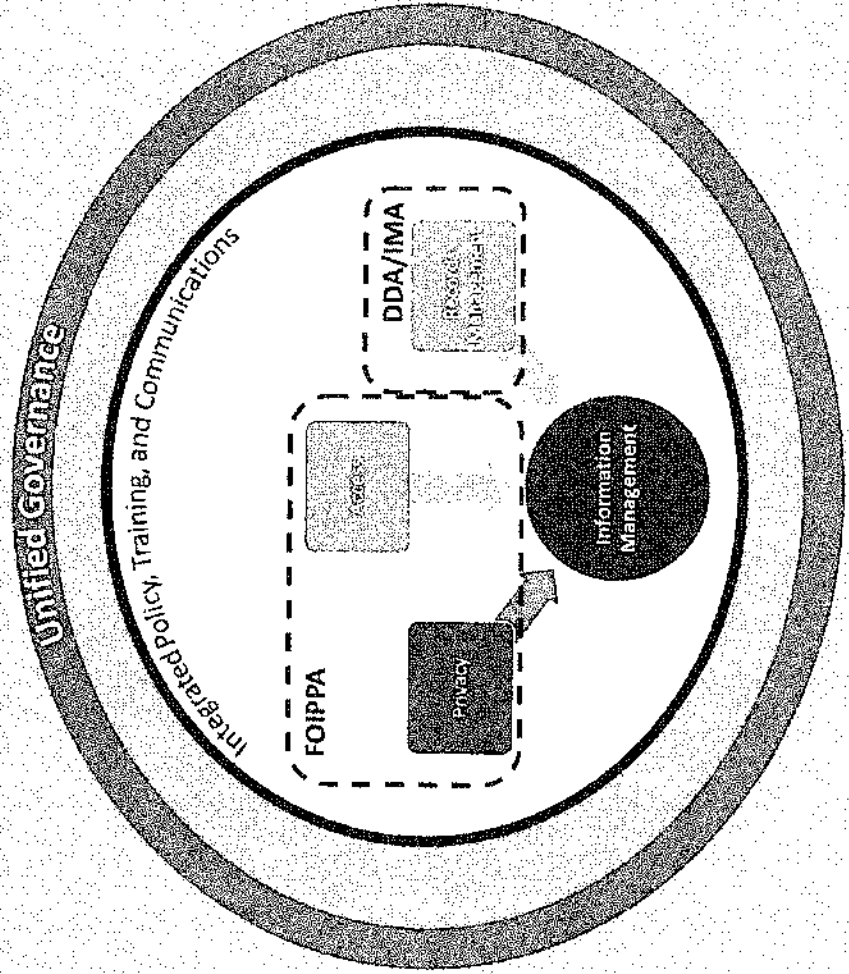
- Current plan is to bring into force this Spring
- Will replace the 80 year old *Document Disposal Act* with a modern and streamlined information management framework
- The traditional practices and tools used to manage electronic records are changing
  - Will establish:
    - The mandate and powers of the Chief Records Officer
    - Streamlined approval processes for records schedules
    - An Information Management Advisory Committee
  - Will enable outdated records schedules to be updated and approved by the CRO



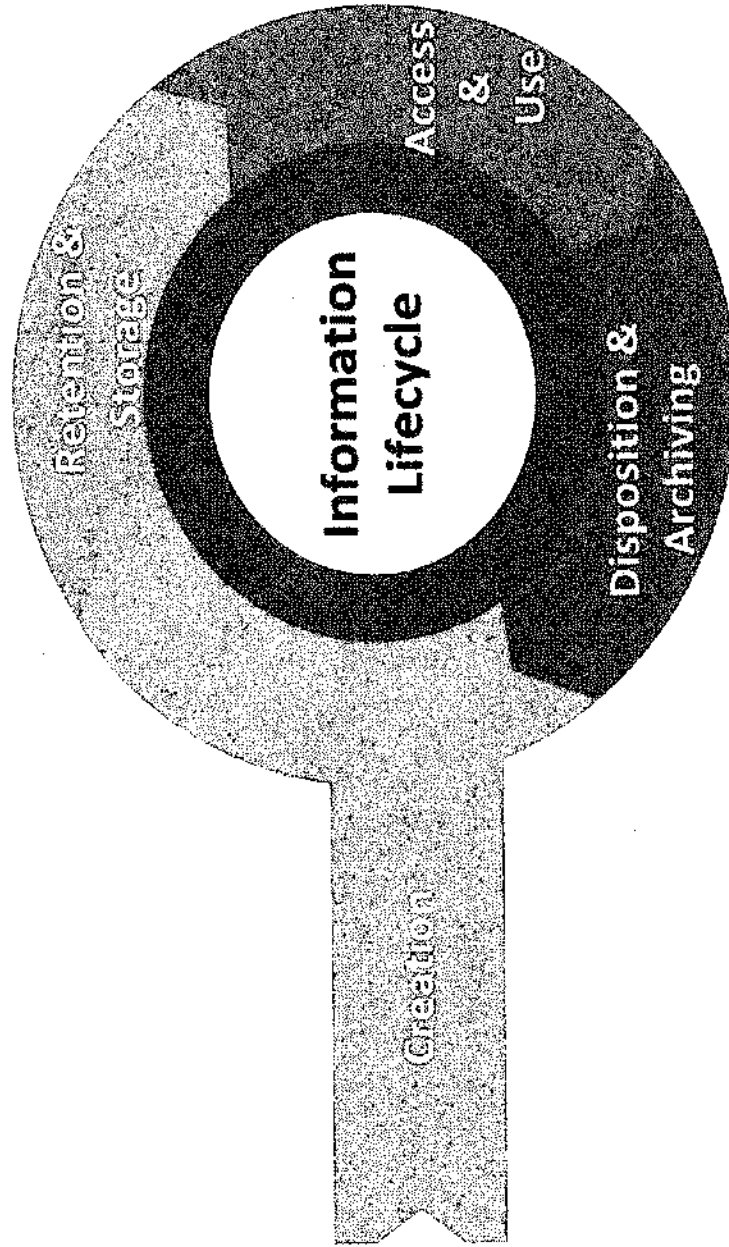
# **Information Management in Context**

# What is Information Management?

## B.C.'s Information Management Governance Structure

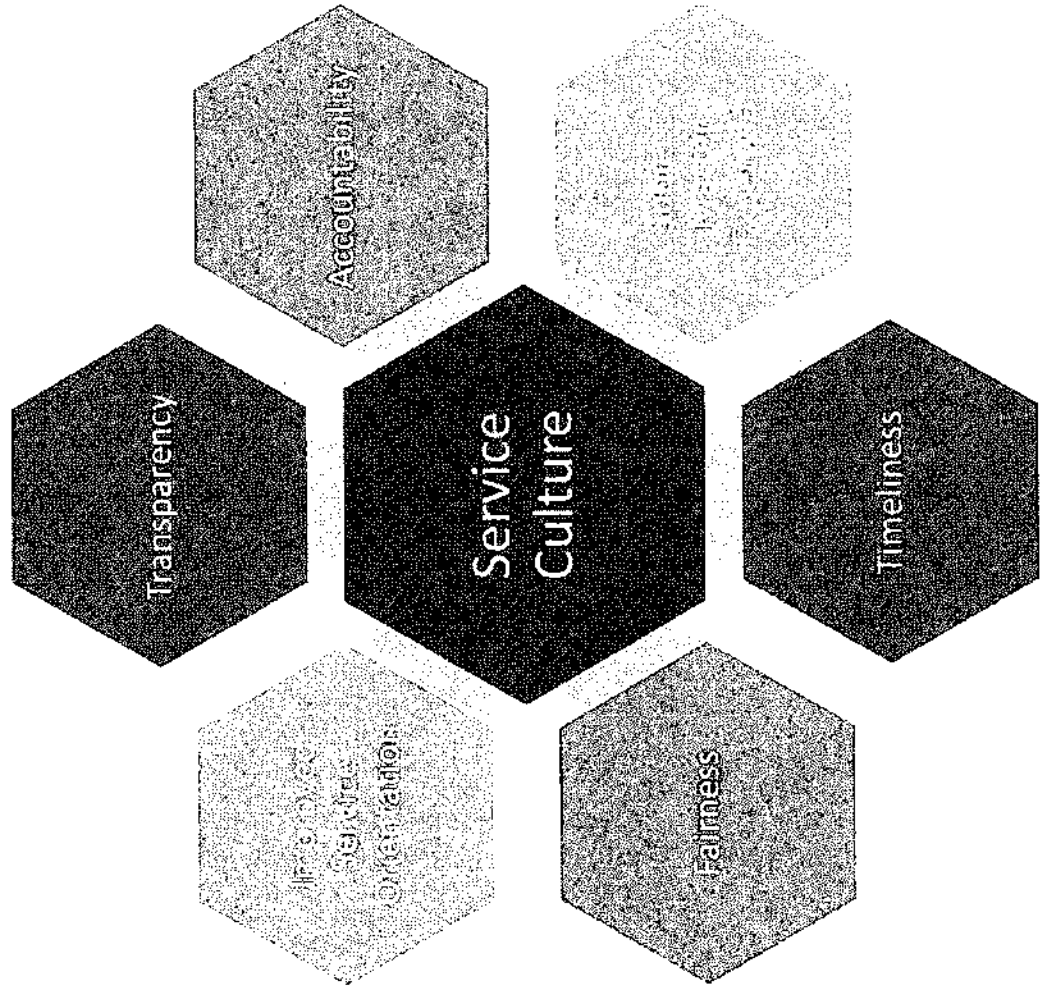


# Information Management Lifecycle



# Improving Access to Information

# Revitalized Service Culture



## Focus on Access

- Commitment to improve customer service experience by:
  - ✓ Improving timeliness
  - ✓ Reducing the number of “no records” responses
  - ✓ Improving on our “duty to assist” applicants
  - ✓ Clarification of FOI requests by ministry staff with better knowledge of records / business processes
  - ✓ Standards for conducting and documenting searches for records in place and followed



# New FOI Process for Ministers' Offices

## 1. Designated contact in DMOs established

- Will coordinate and oversee records searches in Ministers' offices
- Will receive expedited and enhanced training on FOI and records management
- Will provide FOI and records management support to staff in Ministers' offices

## 2. Updated criteria and process for conducting and documenting records searches

- Staff in Ministers' offices will receive updated guidance and training on search criteria and process
- Designated DMO contact will be responsible for ensuring process is followed (will sign off search documentation)

## 3. Escalation process for inadequate searches established

- Two way escalation process in place between the CRO and DMO contacts for situations where records are believed to exist but have not been produced

# Proactive Disclosure

- B.C. is already a leader in the proactive disclosure of information and open data
- Will solidify this position by designating and publishing new categories of information

Already published
<ul style="list-style-type: none"> <li>• Responses to General (non personal) FOI requests</li> <li>• Summary of Ministers' and Deputy Ministers' travel expenses</li> <li>• Over 2,000 data sets, including government's Personal Information Directory</li> </ul>

Underway or Under Consideration
<ul style="list-style-type: none"> <li>• Ministers' travel receipts</li> <li>• Purchase card information</li> <li>• Ministers' and Deputy Ministers' calendars</li> <li>• Government contract information</li> <li>• Direct award summaries</li> </ul>

# Enhancing Privacy Protection

# B.C.'s Leading Privacy Practices

## B.C. is setting the standard across Canada

- **Strongest data residency** protections in Canada
- **Privacy Impact Assessments** – first province to legislate requirements; remains one of the only jurisdictions with this obligation
- **Mandatory privacy training** – farthest reaching program of its kind in Canada
- **Personal Information Directory** available as open data on DataBC
  - Includes summaries of Privacy Impact Assessments, Information Sharing Agreements and Personal Information Banks
- Only province with a **central privacy breach response unit** with a 24/7 reporting hotline

# Enhancing Privacy Management, Accountability and Oversight

- B.C. is building on its leading practices with enhanced privacy management, accountability and oversight

## Privacy Management and Accountability Policy

- Launched February 2016, is the first of its kind in Canada
- Overarching framework to enhance accountability and improve privacy practices
- Requires the designation of a Privacy Officer in every Ministry

## Privacy Compliance Auditing

- The creation of a multi-faceted compliance monitoring, review and audit program is underway
- First of its kind in Canada, includes baseline assessments for each ministry, ad hoc reviews and an annual self-audit

# Increased Oversight and Compliance

# Increasing Oversight in Information Management

Next Steps	Oversight Objective
Bring the IMA into effect.	Establishes the legislative mandate of the Chief Records Officer.
Develop policies with clear roles and responsibilities for the Chief Records Officer, executive and employees.	Clarifies requirements, roles and responsibilities and establishes accountability.
Develop an escalation process for FOI issues related to the processing of requests.	Ensures that searches for records are thorough, well-documented are carried out in a timely and effective manner.
Deliver mandatory, integrated information management training to all employees.	Provides a comprehensive and integrated view of information management requirements.
Establish an advisory committee to provide recommendations to the Chief Records Officer on the approval of information retention schedules.	Ensures decisions are informed by expert advice from a multi-disciplinary committee including legal, financial, archiving, audit and technology experts.
Establish a comprehensive information management compliance review program based on the privacy compliance program.	Identifies areas of noncompliance, adopting a holistic view of information management, and ensures action is taken to address them. Leverages existing processes and resources.

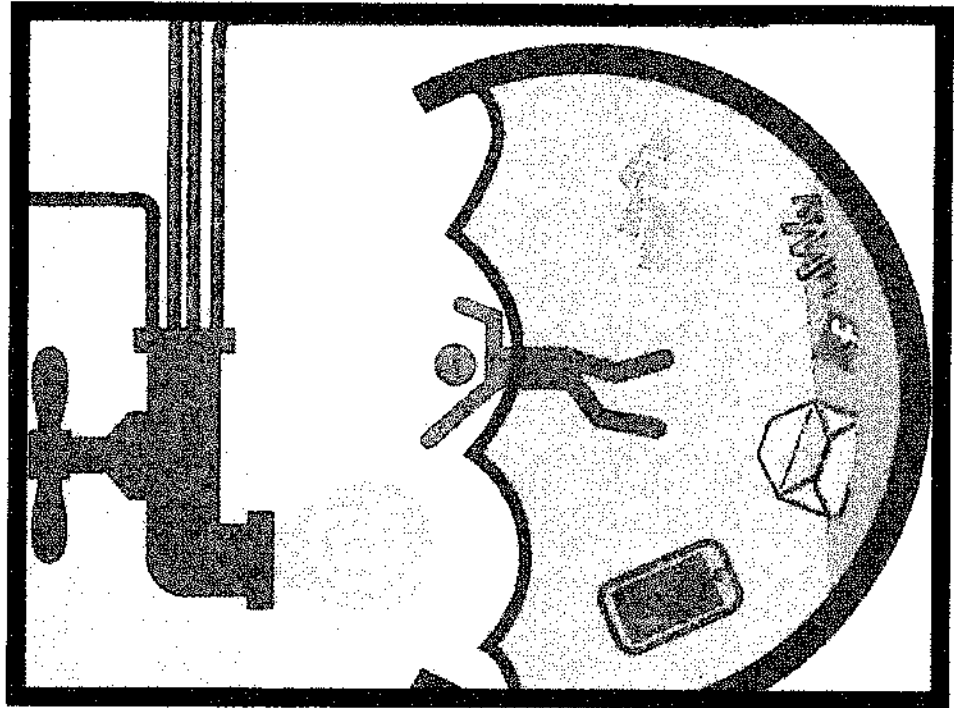
# Mandatory Training

- A robust and integrated training program will be established for all government and political staff and implemented in three phases
- Training will be mandatory and must be repeated every 2 years
- Training of political staff and designated FOI coordinators will proceed on an expedited basis



# **Improving Records Management Practices and Advancing the Duty to Document**

# Information Explosion



## Impact on Records Management

*“At all costs, the provincial government should not entertain any notion that all electronic records must, regardless of their value, be retained. This would be completely contrary to modern records and information management principles. It would also be damaging to both public administration and, perversely, freedom of information and privacy.”*

*David Loukidelis, 2015*

# Documenting and Retaining Valuable Information

## Current State

- IMA requires the retention of all information that documents key decisions
- Government's Core Policy and Procedures reinforces the value of good records management including the creation of records

## Next steps

- Further emphasize duty to document principles in updates to records management policies
- Further consider implications of legislative "duty to document", including the appropriate legislation in which to add such a duty

# Conclusion

- Government is taking action on all of the Loukidelis recommendations
- We are also committed to going further than the recommendations
  - Revitalizing a service culture
  - Proactive disclosure
  - Comprehensive training, policies and compliance
- We look forward to the committee's recommendations

**Thank you!**



## Hudson, Vicki MTIC:EX

---

**From:** Curtis, David FIN:EX  
**Sent:** Monday, February 29, 2016 5:46 PM  
**To:** Williams, Brad M MTIC:EX; Lowe, Charmaine MTIC:EX  
**Subject:** Expense Note  
**Attachments:** 1731516 (3).docx

FYI – Earlier work on the proactive release.



Page 130 to/à Page 134

Withheld pursuant to/removed as

s.13

## Hudson, Vicki MTIC:EX

---

**From:** Hoskins, Chad MTIC:EX  
**Sent:** Tuesday, March 22, 2016 1:31 PM  
**To:** Curtis, David FIN:EX  
**Cc:** Williams, Brad M MTIC:EX  
**Subject:** RE: Special Committee questions

Hi David,

Please see below for some costing rationale.

Let us know if we are on the right track.

Thanks, Chad

---

**From:** Curtis, David FIN:EX  
**Sent:** Wednesday, March 16, 2016 12:08 PM  
**To:** Hoskins, Chad MTIC:EX  
**Cc:** Williams, Brad M MTIC:EX  
**Subject:** Special Committee questions

Hi Chad,

I was hoping to get your help developing a response to a question raised in today's Special Committee.  
s.13,s.17

s.13,s.17

Thanks again and happy to discuss.

David