

Page 01 to/à Page 11

Withheld pursuant to/removed as

s.14

**From:** [Curtis, David FIN:EX](#)  
**To:** [Biggs, Jackie FIN:EX](#)  
**Subject:** FW: CLIFF ID 359239  
**Date:** Tuesday, October 10, 2017 2:54:50 PM  
**Attachments:** [Additional Advice to DMOs.docx](#)  
[Memo from Premiers Office.docx](#)  
[Memo from Kim Henderson.docx](#)  
[Employee Guide Managing Cabinet Confidences.docx](#)  
[Scan\\_20170623.pdf](#)

---

**From:** Olson, Lianna FIN:EX  
**Sent:** Monday, June 26, 2017 12:38 PM  
**To:** Curtis, David FIN:EX  
**Cc:** Wenezenki-Yolland, Cheryl FIN:EX; Van El, Wendy M FIN:EX; Biggs, Jackie FIN:EX; Gotto, Sarah F FIN:EX; Olson, Lianna FIN:EX  
**Subject:** CLIFF ID 359239

Hi David, this has been approved by Athana and has now been sent up to Kim's office.

Thanks,

Lianna

---

**From:** Gotto, Sarah F FIN:EX  
**Sent:** Friday, June 23, 2017 9:49 AM  
**To:** MacLean, Shelley FIN:EX  
**Cc:** Nicholson, Riley FIN:EX; Olson, Lianna FIN:EX; Van El, Wendy M FIN:EX  
**Subject:** FOR ACTION - Approve/Not Approve CLIFF ID 359239

Good morning.

Shelley, attached is the package in which I believe Cheryl mentioned to you this morning that she was walking into Athana for review and sign off. Cheryl has left the hard copy (including the sign off sheet) with Athana to review.

I have cliffed the package over to DMO and have embedded the documents within cliff.

I understand this will need to go over to Kim once Athana has reviewed. Will this be something the DMO does or my responsibility?

Thank you.

Sarah

---

**From:** Olson, Lianna FIN:EX  
**Sent:** Friday, June 23, 2017 9:08 AM  
**To:** Gotto, Sarah F FIN:EX  
**Cc:** Van El, Wendy M FIN:EX  
**Subject:** Approve/Not Approve CLIFF ID 359239

Hi Sarah,

Update this morning on this one: Cheryl has approved and is taking it directly into Athana this morning. Please cliff this package over to DMO for Athana's approval. I have updated the "employee guide managing cabinet confidences" document to take out the two comments. (Wendy, please take note of this update)

Thanks,

Lianna

# **Deputy Ministers' Offices: Additional Guidance on Managing Confidential Records during and after Government Transition**

This document supplements the “**Guide to Managing Confidential Records during and after Government Transition**” by providing additional procedural guidance to Deputy Ministers' Offices with respect to the handling of confidential information during and after a government transition.

## **Overview: Protecting Confidential Information in Government's Custody or under its Control**

This guide provides direction on managing confidential records in the event of a transition in government. It builds upon and clarifies the direction provided in the guide [Managing Records During an Election](#).

Government information received, created and used by Cabinet Ministers, their staff, and Ministry employees is a valuable public asset and must be managed in a manner consistent with legislation, policy, information schedules and the Standards of Conduct, as well as established Constitutional conventions.

Government is the steward of a considerable amount of confidential information, including Cabinet records, Cabinet-related records and personal information. It is vital that this information be protected at a level that is commensurate with its sensitivity and value.

Compliance with legislation, policy, information schedules and the Standards of Conduct is subject to review and audit by the Chief Records Officer and may, in some cases, be investigated by the Information and Privacy Commissioner or other independent officers of the Legislature.

The following requirements apply **at all times**:

### **Requirements for Retention of Government Information**

The [Information Management Act](#) (IMA) requires all government information to be held, transferred, archived or disposed of only in accordance with an approved information schedule.

### **Requirements for Protecting All Confidential Information**

The [Appropriate Use Policy](#) sets out the requirements for employees to follow in order to ensure that the confidential information they are working with is protected. This includes restricting access to confidential information to employees who require it to carry out their duties, and only disclosing confidential information to those who are authorized to view it.

## Requirements for Protecting Personal Information

The *Freedom of Information and Protection of Privacy Act* (FOIPPA) sets out the legal requirements for protecting personal information. Ministries may only collect, use, and disclose personal information if authorized by FOIPPA. The unauthorized disclosure of personal information is an offence under FOIPPA. Other enactments may also apply that further limit the collection, use and disclosure of certain types of information.

The following additional requirements apply **in the period following a general election**<sup>1</sup>.

## Requirements for Protecting Records that may Reveal the Substance of Deliberations of a Former Cabinet or Cabinet Committees

Established Constitutional convention requires that all records, which may reveal the substance of deliberations of Cabinet or its committees, are treated as privileged information of the government of the day. This means an incoming administration (i.e., incoming Ministers and political staff) does not have access to these documents without the consent of the former administration.

Such records may only be shared with the new Executive Council on an exceptional basis with the express consent of the previous Executive Council, which is sought during and after the transition period from the former Premier or their delegate.

- **Cabinet Records** are those that have been prepared for submission to or circulated for consideration by Cabinet or a Cabinet Committee. Cabinet records can include agendas, minutes, final versions of Cabinet and Cabinet Committee submissions, decision letters of Cabinet and its committees, staff analysis, draft legislation, regulations and Orders in Council circulated for consideration by Cabinet, presentation decks and papers.
- **Cabinet-Related Records** are records held by public bodies that are created or received by the public body, which may reveal the substance of deliberations of Cabinet or a Cabinet Committee, correspondence including email correspondence, briefing notes, drafts of Cabinet or Treasury Board submissions, draft regulations and Orders in Council, financial impact assessments, and memoranda regarding confidential work for the consideration of Cabinet.

**Government information must be retained in accordance with legislation, policy and information schedules. Government information also must be protected using security measures commensurate with its sensitivity and confidential information may be accessed only by those who need the information to perform their duties.**

---

<sup>1</sup> The period following Election Day until a new Cabinet is sworn in is referred to as “transition”.

## Special procedures in the event a Deputy Minister is transferring or departing

In the event that a Deputy Minister is leaving his or her position, the Public Service Agency's recommended practices for any departing employee should be followed.

As in any staff transfer or departure, access to email, systems and facilities by outgoing Deputy Ministers will be halted through termination of IDIR (and reinstated upon relocation to a new Ministry, in the case of a transfer). Deputy Ministers' IDIR accounts are transferred or disabled through a request directed to Ken Prosser, Director, Cybersecurity Intelligence and Investigations.

Former employees should not leave the Public Service with any copies of government information in their possession, with limited exceptions. Transferring or departing employees may, on occasion, be permitted to retain a copy of non-sensitive government records.

Access to a former Deputy Minister's email account for the incoming Deputy Minister or their office may be requested by the responsible Deputy Minister through a request directed to Ken Prosser, Director, Cybersecurity Intelligence and Investigations. Access to these accounts must be controlled by the Deputy Minister's office. Any access to or search of these information holdings must comply with legal, Constitutional, and policy requirements, and be based on the principles of "need-to-know"<sup>2</sup> and "least privilege"<sup>3</sup>, as well as an identified operational need. Access should be granted only to that information that is necessary for an individual to perform the operational task. After the task is completed, the access will be rescinded and any copies of emails destroyed unless there is an ongoing operational need to retain them.

## Special procedures respecting an outgoing Minister's or Minister's Office Staff email account

Cabinet records and Cabinet-related records should have been removed from a Minister's Office's prior to an election. In some cases this may not be possible. For example, because Ministers and their staff were directed by the Premier to retain all sent email effective October 2015, Cabinet and Cabinet-related records may exist in the email accounts of outgoing Ministers and political staff.

Other highly confidential government information may also exist in these accounts. Additionally, confidential information that is not government information may also exist in these accounts, such as the personal information of constituents, or other information confidential to their political or other activities.

---

<sup>2</sup> A principle established in government's "Appropriate Use of Government Information and Information Technology Resources Policy" where access is restricted to authorized employees that require it to carry out their work. Employees are not entitled to access information merely because of status, rank, or office.

<sup>3</sup> A principle established in government's "Appropriate Use of Government Information and Information Technology Resources Policy" requiring that each subject in a system be granted the most restrictive set of privileges (lowest clearance) needed to perform their employment duties. The application of this principle limits the damage that can result from accident, error or unauthorized use.

For this reason, the entire contents of these email accounts should be considered to be **highly confidential**. Accordingly, incoming Ministers and Ministers' Office staff should not be granted access to their predecessor's email accounts. Access to these accounts must be controlled by the Deputy Minister's office. Any access to or search of these information holdings must comply with legal, Constitutional, and policy requirements, and be based on the principles of "need-to-know" and "least privilege", as well as an identified operational need.

By request from the Deputy Minister, the Office of the Chief Information Officer (OCIO) will assist with indexing and searching the information holdings in a former Minister's or Minister's Office staff email account. The Deputy Minister determines whether access should be granted, and if access is granted, to which of the emails in the account, based on the index provided by the OCIO. Access should be granted only to that information that is necessary for an individual to perform the operational task. After the task is completed, the access will be rescinded and any additional copies of emails destroyed unless there is an ongoing operational need to retain them.

In the case that there is a reasonable belief that the email account contains records responsive to a request for access to information under FOIPPA, the DMO engages the OCIO to carry out a search as described above and, should responsive records be located, they will be processed and severed per the requirements of FOIPPA and standard procedures.

Access to the contents of these email accounts should be requested by the DMO through a request directed to Ken Prosser, Director, Cybersecurity Intelligence and Investigations.

### **Special Procedures when Records responsive to a Request for Access to Information under FOIPPA are Cabinet records or Cabinet-related records of the previous administration**

While FOIPPA prohibits the disclosure of information that would reveal the substance of deliberations of the Executive Council or any of its committees, including any advice, recommendations, policy considerations or draft legislation or regulations submitted or prepared for submission to the Executive Council or any of its committees, there are limited circumstances where this prohibition does not apply:

1. where the record has been in existence for over 15 years;
2. where the information is in a record of a decision made by the Executive Council or any of its committees on an appeal under an Act; and
3. information in a record the purpose of which is to present background explanations or analysis to the Executive Council or any of its committees for its consideration in making a decision if;
  - a. the decision has been made public;
  - b. the decision has been implemented; or
  - c. 5 or more years have passed since the decision was made or considered.

When one of the above exceptions might apply and therefore a decision is required on the potential disclosure of Cabinet confidential information under this section of the *Freedom of Information and Protection of Privacy Act*, and the records are those of a previous administration, the current Deputy Minister is accountable for making the determination, but should consult the former Premier or delegate through the Cabinet Secretary.

## **Special Procedures where Cabinet records or Cabinet-related records of the previous administration are requested for disclosure by a third party or are required to be disclosed to a third party**

In the case of requests to share information from or about Cabinet records or Cabinet-related records of the previous administration with independent officers of the Legislature, there exist standard conventions and government policies, which must be followed (the Ministry responsible for the legislation establishing the function of an Officer of the Legislature can provide copies of agreements entered into with each Officer, as well as details of any government policies and protocols for sharing of information).

Such agreements typically contain provisions with respect to restrictions on copying and dissemination of the records, and disposal of records at the conclusion of the engagement. They also address who may access the records, for what purpose.

Government has a legal obligation to identify relevant documents in the context of legal proceedings or in response to a summons or subpoena. However, these documents may be privileged or protected from disclosure by public interest immunity. The Constitutional convention does not create any special exemption from the requirement to disclose Cabinet records or Cabinet-related records of a prior administration in the context of legal proceedings or when the production of such records is otherwise required at law.

When sharing Cabinet records or Cabinet-related records with third parties, consideration must be given to assertion of public interest immunity<sup>4</sup> and solicitor client privilege (where applicable). This

---

<sup>4</sup> The test to determine if public interest immunity applies to a document is whether the public interest in withholding the document outweighs the public interest in disclosing it. At common law, Cabinet documents are protected in recognition of the fact that democratic governance works best when Cabinet discussions can be conducted with unreserved candour, and any documents revealing the subject of Cabinet deliberations are therefore protected from disclosure. However, the common law also recognizes this protection must be balanced against the public interest in disclosure, for example, preserving the integrity of the justice system or enabling an officer of the legislature to fulfill his or her statutory mandate.

This balancing occurs by the decision maker weighing the public interest in maintaining confidentiality and the specific public interest in disclosing the information (e.g. disclosing documents in particular litigation or allowing the Auditor General to disclose in a report). It is important to note that considerations with respect to the gain or loss of tactical advantage in the context of the particular litigation have no role in this process. If the public interest in maintaining confidentiality outweighs the public interest in disclosure, it is irrelevant whether there are advantages or disadvantages to a party to the litigation in their disclosure.

consideration should include applicable government policy, advice from legal counsel and consultation with Cabinet Operations as appropriate.

Where records of a previous administration have been identified as forming part of the government's disclosure package, convention is for the Cabinet Secretary to request approval from the previous administration (the former Premier or their delegate). This is generally done as part of the decision making process before any final decision is made on disclosure. Care is taken during this process to respect the terms of the Constitutional convention until a final decision on disclosure has been made.

A decision matrix is attached, which sets out various circumstances where Cabinet materials may be shared.

Government's responsibility to respond in a timely manner is essential with respect to responding to requests for information from independent officers of the Legislature.

## **Existing protocols for limited distribution of highly sensitive confidential information where there is a request for Access to Information under FOI**

Existing procedures are in place in all circumstances where the redlined information in an FOI response package is particularly sensitive — for example where the information is about a labour relations issue, a high-profile individual or issue, or is otherwise classified as highly confidential. These files require additional restrictions on access. Information Access Operations will work with the Ministry to ensure the package is designated for limited access and that additional security controls are implemented.

## **Additional Information**

If you have any questions or require further clarification please contact Cheryl Wenezenki-Yolland, Associate Deputy Minister and Chief Records Officer, Ministry of Finance at (250) 387-8499.

---

When balancing the interests, the decision maker must also consider where there are any appropriate conditions or restrictions that would result in disclosure being in the public interest. As an example, sometimes the public interest supports disclosing Cabinet records in litigation as long as there is a court order setting out appropriate confidentiality terms. The Legal Services Branch assists with negotiating and drafting any confidentiality terms.

It is important to note that this balancing may take place at different times for different types of disclosure. In the litigation context, the balancing occurs prior to any production of documents, but for the Office of the Auditor General, the balancing occurs when the OAG provides government with notice that it intends to include information from such documents in a public report.



## Process for Disclosure of Cabinet Records and Cabinet-Related Records Created for the Former Executive Council

Situation Where Instructions May be Required for Disclosure of Records Created for the Former Executive Council	Who Will Collect Documents	Who reviews/makes recommendations on disclosure	Who makes decision re disclosure	Notes
<b>Litigation</b>	Ministry, assisted by Justice	Deputy Attorney General (for solicitor-client privilege content);; Treasury Board staff (for Treasury Board documents) and Cabinet Operations.	Former Premier or delegate or, alternatively, another member of the former Executive Council, in consultation with Cab Ops, applying the principles of public interest immunity.	<ul style="list-style-type: none"> <li>- generally production is made subject to confidentiality orders</li> <li>- may be existing approvals for release on current matters</li> <li>- where disclosure is required, generally government seeks and order that production is made subject to confidentiality requirements</li> <li>- government must comply with an order of the court even if the former government does not consent to disclosure i.e. court order prevails over convention</li> </ul>
<b>FOIPPA -where Cabinet materials are severed</b>	Ministry	DM in consultation with Cabinet Operations and/or Treasury Board Staff as appropriate	n/a	- access determined by s. 12 FOIPPA; final decision to withhold the record is made by the DM
<b>FOIPPA -where Cabinet records are within s. 12 exceptions</b>	Ministry	DM in consultation with the Former Premier or delegate or, alternatively, another member of the former Executive Council. .	DM	- a document is in the public domain when it is older than 15 years or relates to background information for Cabinet if the decision has been made public, has been implemented, or more than 5 years has passed since the decision was considered

<b>Situation Where Instructions May be Required for Disclosure of Records Created for the Former Executive Council</b>	<b>Who Will Collect Documents</b>	<b>Who reviews/makes recommendations on disclosure</b>	<b>Who makes decision re disclosure</b>	<b>Notes</b>
<b>Officers of Legislature - access only</b>	Ministry	Ministry has primary responsibility for this with assistance from LSB, Treasury Board staff, the Comptroller General, the Deputy Attorney General (if solicitor-client privilege also triggered) and Cabinet Operations.	Former Premier or delegate or, alternatively, another member of the former Executive Council, in consultation with current DM, applying the principles of public interest immunity.	-access determined by mandate and legislative powers of officer - may be existing approvals for release on current matters
<b>Officers of the Legislature - use in public reports</b>	Ministry, assisted by Justice	Ministry has primary responsibility for this with assistance from LSB, Treasury Board staff, the Comptroller General, the Deputy Attorney General (if solicitor-client privilege also triggered) and Cabinet Operations.	Former Premier or delegate or, alternatively, another member of the former Executive Council, in consultation with current DM, applying the principles of public interest immunity.	-access determined by mandate and legislative powers of officer
<b>Access to materials required by incoming Executive Council for administrative continuity<sup>5</sup></b>	Ministry	Deputy Minister responsible for the relevant Cabinet materials.	Former Premier or delegate or, alternatively, another member of the former Executive Council, in consultation with current DM.	

<sup>5</sup> In exceptional circumstances - in most cases, new records will be prepared for the incoming administration, taking care to continue to protect information about the options presented to the Executive Council in making the decision and any information related to the opinions, discussions or deliberations among Ministers at the time of the decision

# Memorandum

Deputy Minister's Office  
Office of the Premier

---

Date: June 20, 2017

To: All Deputy Ministers

Re: Managing Confidential Records during and after Government Transition

---

This memorandum is to give guidance on managing confidential and sensitive records in the event of a transition in government. It builds upon and clarifies the guidance in the March 17, 2017 memorandum on *Management during the Election Interregnum and Transition Periods*.

Accompanying this memorandum is a detailed procedures guide outlining how staff should manage confidential records during and after any government transition.

## **Importance of Managing Government Information Appropriately**

Government information received, created, and used by British Columbia's Cabinet ministers, their staff and public service employees is a valuable public asset and must be managed in a manner consistent with policy, information schedules and the Standards of Conduct, as well as established Constitutional conventions.

Government is the steward of a considerable amount of confidential information, including Cabinet Records, Cabinet-related records and personal information. It is vital that this information be protected at a level that is commensurate with its sensitivity and value and that confidential information only be accessed by those who need the information to perform their duties.

Accordingly, it is important that the confidentiality, integrity and availability of all government information is maintained when an employee transfers to another office or leaves the public service. When an employee transfers to another office or leaves government, his or her records must be managed by the originating office and retained according to approved information schedules (i.e. ARCS and ORCS). Managing all digital and physical information appropriately should be part of regular office practice.

## **Key Transition-Related Information Management Practices**

Key practices leading up to a transition in government include:

- Managing government information separately from non-government information.
- Disposing of transitory records.
- Ensuring official records are filed appropriately.
- Saving email records appropriately.
- Managing Cabinet and Cabinet-related records in preparation for the Constitutional convention whereby ministers of an incoming administration may not see the Cabinet records of a former administration.

Key practices following all government transitions will include:

- Following appropriate procedures for transferring or departing employees.
- Continued secured and managed access to Cabinet and Cabinet-related documents.
- Carefully managed access to those records only retained within an email account.
- Following appropriate procedures where information is requested by or required to be disclosed to a third party.
- Where there is a request for Access to Information under FOI, continuing to follow:
  - Constitutional convention respecting Cabinet confidential records, and
  - Policy and legislative requirements with respect to other types of confidential information.

The attached *Guide to Managing Cabinet Confidential Records during and after Government Transition* provides guidelines and procedures for how to implement the key practices listed above in any office. Additional information is referenced in the guide and can be found on the [Government Records Service website](#).

### **Additional Information**

If you have any questions or require further clarification please call me at (250) 356-2206.

With respect to specific questions, you may also wish to contact Cheryl Wenezenki-Yolland, Associate Deputy Minister and Chief Records Officer, Ministry of Finance at (250) 387-8499.

Sincerely,

Kim Henderson  
Deputy Minister to the Premier, Cabinet Secretary  
and Head of the BC Public Service

# Memorandum

**Associate Deputy Minister's  
Office**

Corporate Information and  
Records Management Office

---

Date: June 20, 2017

---

To: Kim Henderson  
Deputy Minister to the Premier, Cabinet Secretary  
and Head of the BC Public Service

---

Re: Managing Confidential Records during and after Government Transition

---

In addition to the direction provided to all staff under the title "Guide to Managing Confidential Records during and after Government Transition," this memorandum and its attachment provide further recommended guidance on specific practices for Deputy Ministers' Offices.

These additional recommended practices include

- Special procedures for handling the IDIR and email accounts of transferring or departing Deputy Ministers.
- Special procedures for Deputy Ministers' Offices as the custodian of a Ministry's Cabinet and Cabinet-related records, in the following circumstances:
  - Cabinet records or Cabinet-related records of the previous administration or other highly confidential information is collected as responsive to a request for access to information under FOIPPA; and
  - Cabinet records or Cabinet-related records of the previous administration are requested for disclosure by a third party or are required to be disclosed to a third party.

# Guide to Managing Confidential Records during and after Government Transition

## Overview: Protecting Confidential Information in Government's Custody or under its Control

This guide provides direction on managing confidential records in the event of a transition in government. It builds upon and clarifies the direction provided in the guide [Managing Records During an Election](#).

Government information received, created and used by Cabinet Ministers, their staff, and Ministry employees is a valuable public asset and must be managed in a manner consistent with legislation, policy, information schedules and the Standards of Conduct, as well as established Constitutional conventions.

Government is the steward of a considerable amount of confidential information, including Cabinet records, Cabinet-related records and personal information. It is vital that this information be protected at a level that is commensurate with its sensitivity and value.

Compliance with legislation, policy, information schedules and the Standards of Conduct is subject to review and audit by the Chief Records Officer and may, in some cases, be investigated by the Information and Privacy Commissioner or other independent officers of the Legislature.

The following requirements apply **at all times**:

### **Requirements for Retention of Government Information**

The [Information Management Act](#) (IMA) requires all government information to be held, transferred, archived or disposed of only in accordance with an approved information schedule.

### **Requirements for Protecting All Confidential Information**

The [Appropriate Use Policy](#) sets out the requirements for employees to follow in order to ensure that the confidential information they are working with is protected. This includes restricting access to confidential information to employees who require it to carry out their duties, and only disclosing confidential information to those who are authorized to view it.

### **Requirements for Protecting Personal Information**

The [Freedom of Information and Protection of Privacy Act](#) (FOIPPA) sets out the legal requirements for protecting personal information. Ministries may only collect, use, and disclose personal information, if authorized by FOIPPA. The unauthorized disclosure of personal information is an offence under FOIPPA. Other enactments may also apply that further limit the collection, use and disclosure of certain types of information.

The following additional requirements apply **in the period following a general election**<sup>1</sup>.

### **Requirements for Protecting Records that may Reveal the Substance of Deliberations of a Former Cabinet or Cabinet Committees**

Established Constitutional convention requires that all records, which may reveal the substance of deliberations of Cabinet or its committees are treated as privileged information of the government of the day. This means an incoming administration (i.e., incoming Ministers and political staff) does not have access to these documents without the consent of the former administration.

Such records may only be shared with the new Executive Council on an exceptional basis with the express consent of the previous Executive Council, which is sought during and after the transition period from the former Premier or their delegate.

- **Cabinet Records** are those that have been prepared for submission to or circulated for consideration by Cabinet or a Cabinet Committee. Cabinet records can include agendas, minutes, final versions of Cabinet and Cabinet Committee submissions, decision letters of Cabinet and its committees, staff analysis, draft legislation, regulations and Orders in Council circulated for consideration by Cabinet, presentation decks and papers.
- **Cabinet-Related Records** are records held by public bodies that are created or received by the public body, which may reveal the substance of deliberations of Cabinet or a Cabinet Committee, correspondence including email correspondence, briefing notes, drafts of Cabinet or Treasury Board submissions, draft regulations and Orders in Council, financial impact assessments, and memoranda regarding confidential work for the consideration of Cabinet.

**Government information must be retained in accordance with legislation, policy and information schedules. Government information also must be protected using security measures commensurate with its sensitivity and confidential information may be accessed only by those who need the information to perform their duties.**

---

<sup>1</sup> The period following Election Day until a new Cabinet is sworn in is referred to as “transition”.

## Key Practices Prior to Transition

### 1. **Manage government information separately from non-government information.**

Government policy permits the limited personal use of information and technology resources. Therefore, some of the information that government employees receive, create, and retain on the government system for reasons that are not related to their work may be confidential because, for example, it contains their own personal information or the personal information of others. This type of information is not government information. Employees should regularly review their paper files, email and voicemail accounts, and any digital records stored on personal or shared drives, for non-government information such as family photos and personal (i.e., not related to government business) emails. Employees are required by policy to limit the amount of non-government information they store on government systems, and should regularly delete/dispose of this type of information.

### 2. **Dispose of transitory information unless it is responsive to an FOI request or litigation search.**

Employees should regularly review their physical and digital environments (e.g., portable storage devices, filing cabinets, desk drawers, email and employee drives) for transitory information and they should dispose of it as appropriate. Employees should delete, or otherwise securely destroy, redundant copies, working materials no longer needed, ephemeral emails, and other transitory information that may have been retained for reference purposes. For more information, see the [\*Transitory Records Guide\*](#) and the [\*Email Decision Diagram\*](#) available on the [Records Management website](#).

Transitory information that is responsive to an open FOI request or active litigation **must not** be destroyed.

### 3. **Ensure official records are sent to the appropriate responsibility centre or filed appropriately.**

Government information must be retained according to information schedules and continue to be available to serve the ongoing needs of the ministry. Departing employees must not retain copies of government information. Employees must not password-protect individual documents or folders. Ensure records subject to Cabinet confidence are appropriately secured.

### 4. **Save email records appropriately.**

In general, an email inbox should not be used to store government information, other than transitory records, for example, convenience copies of messages. Important emails should be saved in an office recordkeeping system, or the information in the email should be summarized in another document. Employees must not password-protect individual messages or folders. Ensure records subject to Cabinet confidence are appropriately secured.

### 5. **Prepare to follow the Constitutional convention whereby ministers of an incoming Executive Council may not see the Cabinet records and Cabinet-related records of a former Executive Council.**

Procedures for managing Cabinet records and Cabinet-related records during and after the election period respect the Constitutional convention that records prepared for consideration by Cabinet are considered to be privileged information of the Executive Council of the day. With rare exceptions and only following review and consultation, a succeeding Executive Council does not have access to



these records without the consent of the former Premier or their delegate. This protects the confidentiality of the collective decision-making process of parliamentary democracy.

Before the transition period, Cabinet records and Cabinet-related records must be identified, labelled and managed to ensure access is limited to those who “need to know”. Prior to the interregnum, the Deputy Minister’s Office (DMO) will ensure that any Cabinet records or Cabinet-related records are removed from their Minister’s Office and placed in a secure location controlled by the DMO. The Deputy Minister’s Office must create an inventory of physical and digital locations where Cabinet and Cabinet-related records are located within the Ministry, including who has access to these locations.

Where the Cabinet record or Cabinet-related record is an integral part of ministry business files, a copy may be retained in the relevant operational/business unit files.

Appropriate security and access measures must be in place for these records, whether in physical or digital storage (e.g., EDRMS, LAN/shared drive, SharePoint, Email, or CLIFF).

For assistance in limiting access to records via TRIM/EDRMS or CLIFF, contact a Ministry Records Officer.

For assistance in limiting access to records in SharePoint, a LAN or shared drive contact [77000@gov.bc.ca](mailto:77000@gov.bc.ca), or dial 7-7000.

## Key Practices Post Transition

### 6. Follow appropriate procedures for transferring or departing employees.

When an employee transitions out of the Public Service, they must not have access to their government email account or any information stored in government systems.

Former employees should not leave the Public Service with any copies of government information in their possession, with limited exceptions. Departing or transferring employees may, on occasion, be permitted to take a copy of non-sensitive government records (e.g., work samples or information relevant to the employee’s knowledge base).

It is important that the confidentiality, integrity and availability of all government information is maintained when an employee transfers to another office or leaves the public service. When an employee leaves government or transfers to another office, his or her records must be managed by the originating office and retained according to approved information schedules (i.e. ARCS and ORCS). Managing all digital and physical records appropriately should be part of regular office practice.

For more information, please refer to Government Records Service’s Departing or Transferring Employees Guide.

**7. Continue to secure and manage access to Cabinet records and Cabinet-related records in accordance with legislation, Constitutional convention, government policy, protocols and good practices.**

After the transition, particular care must be given to protecting Cabinet records and Cabinet-related records.

Cabinet Operations holds the final versions of Cabinet records and Cabinet-related records, other than Treasury Board records, which are held by Treasury Board Staff. The ministry responsibility centre (i.e., the Office of Primary Responsibility [OPR]) is the DMO.

Where the Cabinet record or Cabinet-related record is an integral part of ministry business files, a copy may be retained in the relevant operational/business unit files. The ministry copies of Cabinet submissions and draft submissions must be kept secure to ensure no unauthorized access.

Where records contain information subject to Cabinet Confidence, Constitutional convention requires that those records **not** be shared with the incoming Minister or political staff. These records also must only be accessed by members of the public service on a need-to-know basis.

Although a new administration is precluded from viewing the *records* of a previous administration, it is generally permissible for a new administration to obtain *information* about decisions made by a previous administration, particularly where the information is necessary to ensure that government business will be carried out effectively. For this reason, after a change in administration occurs, in responding to requests of the new government, the proper procedure is to prepare new reports and submissions, rather than simply providing copies of old ones. Previous Cabinet submissions and records used in their preparation may continue to be used as resource documents by Public Service staff preparing new submissions, where authorized by the Deputy Minister. In providing advice to the new Executive Council, where the continuity of administration requires reference to records prepared for previous Executive Councils, it may be appropriate to paraphrase the contents of those materials, provided that the paraphrasing is essential to explain a point of policy affecting the future operations of government.

However, in preparing new records or paraphrasing information about the decisions made by a prior administration, employees must take care to continue to protect information about the options presented to the Executive Council in making the decision and any information related to the opinions, discussions or deliberations among Ministers at the time of the decision.

**8. Continue to follow established legislation, Constitutional Convention, government policies, protocols and good practices when sharing Cabinet records and Cabinet-related records with external parties.**

Policies and procedures are generally in place through the Ministry of Justice and Attorney General's Legal Services Branch to work with Ministry program areas to collect and review relevant documents to determine whether they are subject to disclosure. Where information is requested to be shared with external parties (e.g. broader public sector entities or independent officers of the Legislature), employees should comply with the applicable government policy. In the absence of such a policy, Ministries should ensure there is clear documentation in place that establishes expectations around access to, use, circulation and disposal of the records.

Sharing of any Cabinet records or Cabinet-related records of former administration with third parties, including independent officers of the Legislature, must be approved by the former Premier or their delegate.

In sharing these records, consideration must be given to the assertion of public interest immunity and solicitor client privilege (where applicable). This consideration should include applicable government policy, advice from legal counsel and consultation with Cabinet Operations as appropriate.

Government's responsibility to respond in a timely manner is essential with respect to responding to requests for information from independent officers of the Legislature.

In the case of requests to share information with independent officers of the Legislature, there exist standard conventions and government policies, which must be followed (e.g., for requests from the Auditor General

see [http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/18\\_Administration.htm#1842](http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/18_Administration.htm#1842)).

Government has a legal obligation to identify relevant documents in the context of legal proceedings or in response to a summons or subpoena. However, these documents may be privileged or protected from disclosure by public interest immunity. The Constitutional convention does not create any special exemption from disclosure for Cabinet records or Cabinet-related records of a prior administration.

Where records of a previous administration have been identified as forming part of the government's disclosure obligations, convention is for the Cabinet Secretary to notify the previous administration (the former Premier or their delegate). Therefore, it is important that employees identify this type of information promptly and that the Ministry notify the Cabinet Secretary of the requested/required disclosure, as soon as possible.

**9. Consider who should have access to those records only retained within an email account.**

By following the practices set out above respecting records management before the transition, key records should be located in the office record keeping system and therefore access to a former staff member's email records should only be necessary in extraordinary circumstances where it was not possible to dispose of transitory records and/or save email records appropriately. In some cases, however, it may be reasonable for incoming staff to access their predecessor's email account for an operational reason, or for Information Access Operations to view records retrieved from a departed staff's email account for the purpose of responding to a request for access to information under FOIPPA.

Since an email account may contain personal and other sensitive information, access to the email account and any individual emails contained therein should be granted only on a "need to know" basis, disclosing only the minimum information that is necessary for an individual to perform the operational task. After the task is completed, the access should be rescinded and any additional copies of emails destroyed unless there is an ongoing operational need to retain them.

**10. FOI: Continue to follow Constitutional convention respecting Cabinet confidential records where there is a request for Access to Information under FOI.**

It is possible that copies of Cabinet records and Cabinet-related records prepared for a former administration will be collected in response to a Freedom of Information (FOI) request. Employees must continue to take care to ensure that the Constitutional convention is followed whereby ministers of an incoming administration may not see, or otherwise obtain information about the contents of the Cabinet records and Cabinet-related records of a former administration.

**11. FOI: Continue to follow policy and legislative requirements with respect to other types of confidential information where there is a request for Access to Information under FOI.**

In addition, when responding to an FOI request, employees are bound by government policy and law to maintain the confidentiality of other types of sensitive information, including personal information and information subject to solicitor-client privilege.

Some recommended best practices for protecting personal and other confidential information in redlined copies of FOI response packages include:

- Identifying who should have access to redlined copies of response packages, based on the principles of “need to know” and “least privilege” as defined in the Appropriate Use Policy;
- Limiting the printing of redlined copies of response packages so that there are not multiple copies to keep track of and account for;
- Providing general briefings without compromising personal information to other employees impacted by an FOI request rather than sharing or distributing redline copies of response packages; and
- Ensuring employees are informed of their responsibilities regarding the protection of personal and other confidential information.

For more information on appropriate records management practices, please see:

- [Managing Records During an Election](#)
- [Departing or Transferring Employees](#)
- [Employee Exit Checklist](#)
- [Managing Minister’s Office Records](#)


# Ministry of Finance SIGN-OFF SHEET

Item: ☐ BN for Information ☐ BN for Decision ☒ Correspondence ☐ OIC  
☐ Other

Issue: Deputy Ministers' Offices: Additional Guidance on Managing Confidential Records during and after Government Transition

CLIFF #: 359239

Date initiated: June 20, 2017 Final Due on:

Approvals Required:	Reviewer	Reviewer Initial	Approval	Date Signed
Drafter	Melissa Sexsmith			
Director	Melissa Sexsmith	MS	<input checked="" type="checkbox"/> Approved <input type="checkbox"/> Approved w/ Changes <input type="checkbox"/> Needs Rewrite	June 22, 2017
ADM	David Curtis	DC	<input checked="" type="checkbox"/> Approved <input type="checkbox"/> Approved w/ Changes <input type="checkbox"/> Needs Rewrite	June 22, 2017
Assoc. DM	Cheryl Wenezenki-Yolland		<input checked="" type="checkbox"/> Approved <input type="checkbox"/> Approved w/ Changes <input type="checkbox"/> Needs Rewrite	Jun 23 2017
DM	Athana Mentzelopoulos		<input type="checkbox"/> Approved <input type="checkbox"/> Approved w/ Changes <input type="checkbox"/> Needs Rewrite	
DM Premier's Office	Kim Henderson		<input type="checkbox"/> Approved <input type="checkbox"/> Approved w/ Changes <input type="checkbox"/> Needs Rewrite	
Notes:				

Included are the following: (check all that apply)

- ☒ Correspondence
- ☐ Incoming
- ☐ Memo
- ☐ OIC
- ☐ Briefing Note