

Hendry, Jackie PREM:EX

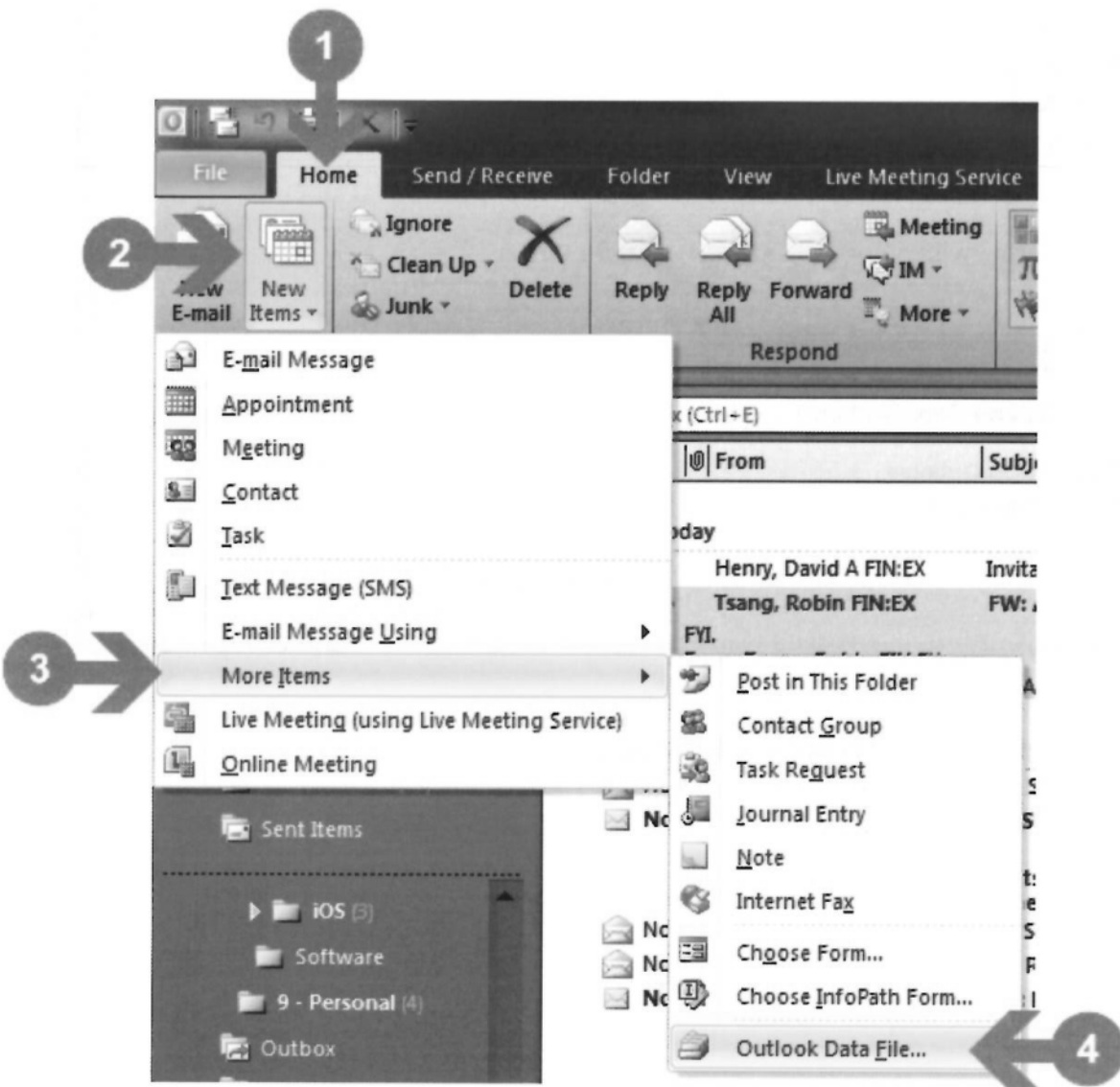
From: Henry, David A FIN:EX
Sent: Friday, June 30, 2017 11:00 AM
To: Leamy, Michelle T PREM:EX
Subject: .PST Outlook folders for storing email/calendar/contacts etc.

Good morning Michelle, as discussed.

To create a Personal folder for email (.PST file):

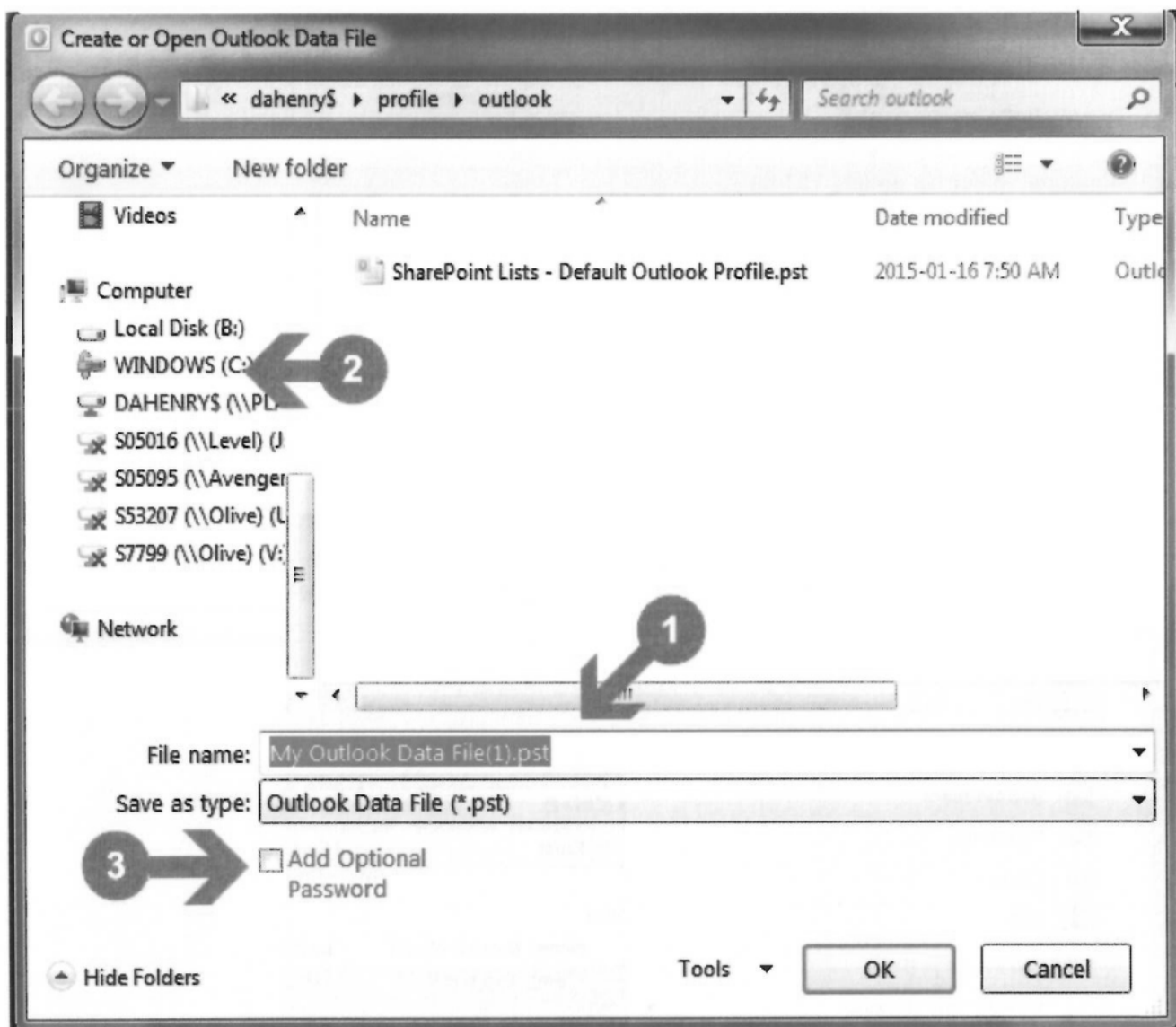
Open Outlook

1. Click <Home>
2. Click <New Items>
3. Click <More Items>
4. Click <Outlook Data file>

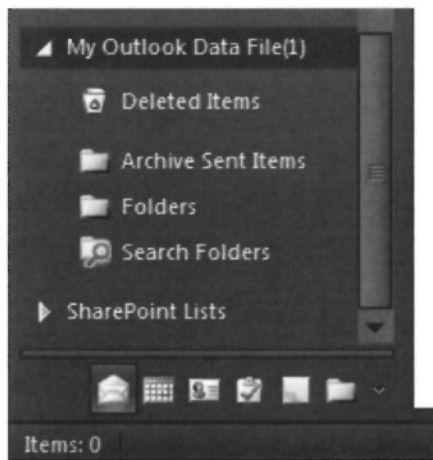


This will create a Personal data file (.PST)

1. Name the file as you wish.
2. Decide where to have it i.e. on network drive best option – H: OR Flashdrive



File will be created. Mine as below is called **My Outlook Data File(1)**



I created a few sub-folders as above.

Any questions let me know.
David

Hendry, Jackie PREM:EX

From: Laidlaw, Susan FIN:EX
Sent: Monday, July 10, 2017 12:33 PM
To: Hendry, Jackie PREM:EX
Subject: FW: Information Management Resource
Attachments: Procedures for Managing Confidential Records during and after Government....docx

Hello Jackie,

I just learned that Cheryl sent out the attached document on Friday to select DMs. s.22 and not involved, I'm afraid. I'm told it is a pared-down version of what Charlotte has previously seen. The timelines were quite tight on Friday (i.e. same day turn-around) and so consultation on this version was minimal. Please let me know if you have any concerns.

The two page document I spoke about on the phone does not reference Cabinet Operations or Cabinet Records. Nonetheless, I will send you a draft copy when its available.

Susan Laidlaw
t: 778-698-2900 c: 778-678-2097

Procedures for Managing Confidential Records during and after Government Transition

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

This document 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.

Under the Standards of Conduct and their oath of employment public service employees are non-partisan and have a duty of loyalty to the government as their employer and must act honestly and in good faith, serving the government of the day to the best of their ability; as such, they must follow these procedures, rules and conventions.

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 election¹.

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, including: 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.

¹ 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 also 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, 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.

In the absence of an express statutory provision or Court Order requiring or prohibiting disclosure, the longstanding constitutional convention is that the former Premier or their designated representatives decide whether or not to disclose Cabinet records and Cabinet-related records prepared when that Premier presided over Cabinet. This convention is recognized among Canadian jurisdictions.

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 immunity² and solicitor client privilege (where applicable). This 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.

² 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.

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.

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.

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. 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. 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 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.

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"³ and "least privilege"⁴, as well as an identified operational need.

³ 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.

⁴ 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.

11. 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.

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.
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.

12. 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.
- 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](#)

Hendry, Jackie PREM:EX

From: Leamy, Michelle T PREM:EX
Sent: Tuesday, July 11, 2017 11:49 AM
To: LP Administrative Coordinators
Subject: FW: iPhone/iPad reset how-to

Please share with your CoS, MA and EA as we need to ensure that they have signed out of iTunes/iCloud before they leave their devices. David has also provided instructions if they wish to wipe their equipment themselves.

David's team will checking each device to ensure all devices are cleared.

thx.

m

From: Henry, David A FIN:EX
Sent: Tuesday, July 11, 2017 11:39 AM
To: Leamy, Michelle T PREM:EX
Cc: VIP Services; Trimble, Brett ISMC:EX
Subject: iPhone/iPad reset how-to

Good morning Michelle, thanks to the team and Brett for compiling this document.

Thanks,
David

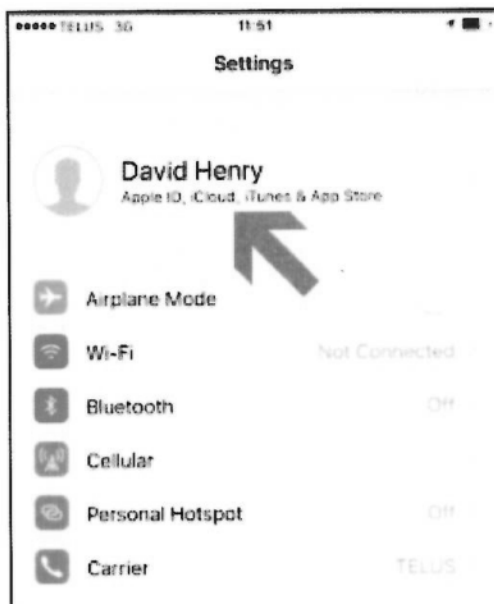
Sign out of iTunes/iCloud on iPhone/iPad



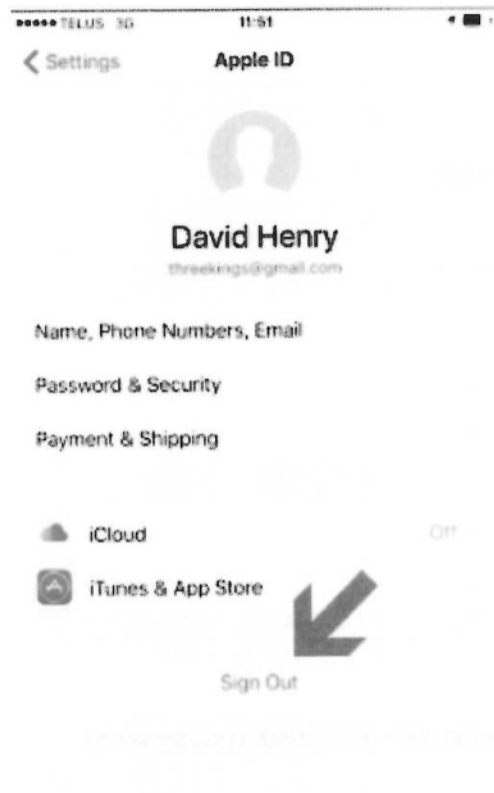
On device got to Settings:

You should see at the top of the screen your account listed. (**Older version devices and operating system:** scroll down to look for **iCloud**)

- Tap on the Account name.



Tap on Sign Out



Older version devices and operating systems tap on **iCloud**:

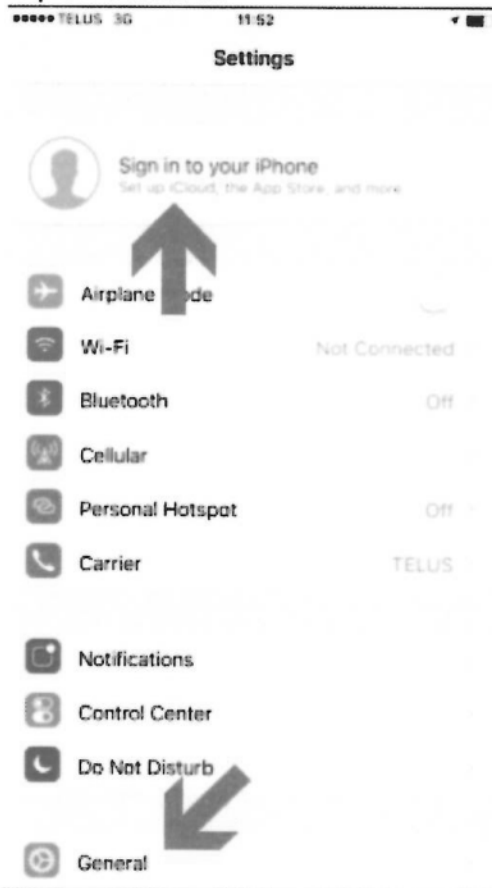


a **Delete Account** option.. choose that)

You should now see no account signed in.
DONE.

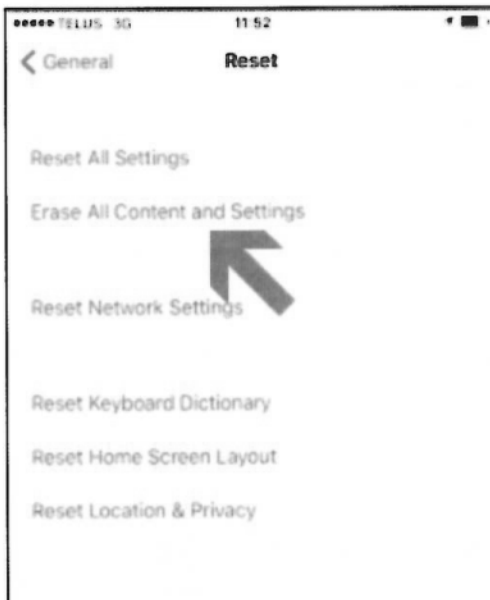
To WIPE the device

Tap on **General**



Scroll down to **Reset**

Tap on **Erase All Content and Settings**



You will be prompted for unlock code and asked if you are sure. Follow prompts.



Once done the device will wipe itself and reset.
Done!

Any questions/issues or assistance required don't hesitate to contact.

David Henry
VIP Services
 TEL #: 250-953-5151
 Email: VIP.Services@gov.bc.ca

Hendry, Jackie PREM:EX

From: Gibbs, Chantal FIN:EX
Sent: Tuesday, July 4, 2017 4:34 PM
To: Leamy, Michelle T PREM:EX
Subject: FW: Minister's email account - archiving old emails

Hi Michelle

David mentions documents below that may be useful to me. I'm going to archive Minister of Finance emails and want to ensure it is done correctly.

Thanks,

Chantal Gibbs

Correspondence Unit | Deputy Minister's Office
Ministry of Finance [Correspondence intranet page](#)
(778) 698-3882

From: Henry, David A FIN:EX
Sent: Tuesday, July 4, 2017 1:23 PM
To: Gibbs, Chantal FIN:EX
Cc: VIP Services
Subject: RE: Minister's email account - archiving old emails

Hi Chantal,

The folder .PST archive you suggest works. Once the and all archives are created, they should be moved to your shared J: drive.

Perhaps in a folder named as appropriate. Then have a note in the folder as well with details.

Pre 2008, records one would hope would have been archived as appropriate. If you don't have them then it is not up to you to deal with?

There was a meeting this AM, with some folks from records and FOI offices that would have good knowledge on best practices. I don't have the contact names, I think Michelle Leamy does.

From our IT perspective, saving archives of emails to the J: drive in a folder structure would be best. Any and all records in electronic format is best.

Give me a call if you like and we can discuss more.

David
250-888-8803

From: Gibbs, Chantal FIN:EX
Sent: July 4, 2017 12:22 PM
To: VIP Services
Subject: FW: Minister's email account - archiving old emails

Hi Gordon,

I'd like to clean up our Minister's email inbox to archive old emails from 2008 and up.

I would like to keep the past 2 years of emails in the inbox (2016/17), should MO staff require these.

I would like to ensure the new MO staff are aware that the old emails (2008-2015) are archived and where these are kept (we propose the DMO's LAN but perhaps you can suggest something else?). I was wondering if creating a folder entitled **2008-2015 emails** & having a note in there indicating the location and DMO contact for retrieval of old emails might be a good idea (transparency & accessibility)?

We have no idea where emails pre-2008 are located. Some of the 2008-2017 emails from the Minister's email are already with the OPR and filed (program areas) but many were handled by the MO directly or not at all and may not have been filed in another location.

Perhaps there are process documents already that provide some guidelines to inform the new MO staff (and DMO during caretaker mode) re: records management requirements for Minister's emails?

Please let me know what I need to do to have my staff archive the Minister's old emails.

Thanks,

Chantal Gibbs

Correspondence Unit | Deputy Minister's Office
Ministry of Finance [Correspondence intranet page](#)
(778) 698-3882

From: Youdale, Trevor FIN:EX
Sent: Tuesday, July 4, 2017 11:37 AM
To: Gibbs, Chantal FIN:EX
Subject: RE: Minister's email account - archiving old emails

Chantel, Gordon McLean at VIP services asked that you contact them. They have specific information to support you during transition and to assist in moving Minister Files, Emails and any other electronic documents. The VIP Services email is: FINITS@Victoria1.gov.bc.ca

In general, I support your proposed plan. VIP services may have more specific direction.

From: Gibbs, Chantal FIN:EX
Sent: Tuesday, July 4, 2017 10:26 AM
To: Youdale, Trevor FIN:EX
Subject: Minister's email account - archiving old emails

Hi Trevor – the Minister of Finance's email inbox has old emails from 2008-2017. All emails were kept.

Since I assume email inboxes should not be used for records management purposes, I would like to archive the old emails onto our LAN.

Is there anything that I need to do (document/legislative/procedural) to archive the Minister's inbox emails to our LAN?

Some concerns/questions:

1. I want to ensure the process is transparent for the new MO. I was going to include an email in the Minister's Inbox indicating that old emails can be found at <insert LAN address/contact DMO>.
2. I want to ensure that we follow proper Records Management conventions and rules. Most emails will have been logged in CLIFF & filed at the branch level in many cases. Some, however, was handled by MO and I can't be sure if they followed any records management process as this dates back 10 years and have been handled by multiple staff who may or may not have been privy to government requirements. Does your office have any concerns or requirements re: my archiving emails to the Minister to our DMO LAN?

Thanks for your help (I know much of this is likely covered in the many useful documents your office provides, which I do read...but I've been asked to contact you to ascertain if anything specific is required or if your office would have any concerns with my archiving these old emails.). I will, of course.

Chantal Gibbs

Correspondence Unit | Deputy Minister's Office
Ministry of Finance [Correspondence intranet page](#)
(778) 698-3882

From: Gillies, Jessica FIN:EX
Sent: Friday, June 30, 2017 9:23 AM
To: Gibbs, Chantal FIN:EX
Subject: FW: FIN MIN - archiving & searching

Go ahead. Please work with Trevor and let me know if you need help.

Jessica Gillies

Manager, FOI & Correspondence Unit | Ministry of Finance
[FIN FOI SharePoint site](#) | [Correspondence intranet page](#)
phone 250 387-3513

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

From: MacLean, Shelley FIN:EX
Sent: Friday, June 30, 2017 9:22 AM
To: Gillies, Jessica FIN:EX
Subject: RE: FIN MIN - archiving & searching

Yes thanks

From: Gillies, Jessica FIN:EX
Sent: Friday, June 30, 2017 9:20 AM
To: MacLean, Shelley FIN:EX
Subject: FW: FIN MIN - archiving & searching

I am fine with this. I don't think the FIN Minister mailbox should contain records older than 2015/16; they should be moved to an appropriate location for filing (or be deleted if they have been sent to a program area for filing). When I informally canvassed our counterparts in other ministries, most suggested that they do not keep years' worth of correspondence in the Minister's mailbox.

Are you OK with this if Chantal works with Trevor to ensure the records are managed appropriately?

Jessica Gillies

Manager, FOI & Correspondence Unit | Ministry of Finance

[FIN FOI SharePoint site](#) | [Correspondence intranet page](#)

phone 250 387-3513

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

From: Gibbs, Chantal FIN:EX

Sent: Thursday, June 29, 2017 5:48 PM

To: Gillies, Jessica FIN:EX

Subject: FIN MIN - archiving & searching

Jessica – I'd like to request permission to have our FIN MIN email search extend to only 2015/16 in FIN MIN.

Since a Minister's email account is not an OPR filing area, records should not be permanently kept in there. As you requested, I will request direction from Trevor Youdale re: archiving these records.

Archiving the emails onto our LAN will allow us to access them if a search is ever required as we cannot be certain MO staff since 2008 have properly filed/CLIFF'd. I'd like for Mona to begin this next week as we currently have a window of time within which staff are not swamped.

Might you advise if DMO is ok with our removing/archiving the 2008-2014 records from FIN MIN? This will help ensure that a new MO properly manages the inbox and does not keep records in there permanently. I'd love to clean this up quickly before new MO staff start.

This would also allow me to limit my search for Cabinet records to 2015-2016.

Please advise.

Chantal Gibbs

Correspondence Unit | Deputy Minister's Office

Ministry of Finance [Correspondence intranet page](#)

(778) 698-3882

Hendry, Jackie PREM:EX

From: Henry, David A FIN:EX
Sent: Sunday, July 9, 2017 11:06 AM
To: Leamy, Michelle T PREM:EX
Subject: GOV PCs Reimage date

Hi Michelle, here is the email.

So the swearing in for the new Premier is Tuesday July 18th.

I am hoping we can queue up the reimage of all PCs starting later this week? Perhaps by Thursday or Friday? Then we can ensure over the weekend all are ready, and they will be ready for the Monday/Tuesday, final patches and such.

Do we know of any staff whom are staying in the various offices? I was thinking those PCs could stay with them? Will that work?

With the inventory being done today for the LP, we should have an idea of how many PCs in Victoria. With Tuesday, the much smaller # in Vancouver being inventoried.

Thanks,
David

Hendry, Jackie PREM:EX

From: Leamy, Michelle T PREM:EX
Sent: Wednesday, July 12, 2017 2:20 PM
To: LP Administrative Coordinators
Cc: LP Chief of Staff
Subject: Minister Office SharePoint

Good Afternoon All!

Further to our meeting and the distribution of records management materials there is one more area to check . . . The Minister Office SharePoint libraries (<https://fin.gov.bc.ca/cbm/cc/BCMinxxx>) that have been used to send documents to a Minister's iPad require final cleanup.

As SharePoint is a transitory medium please ensure that all files on the SharePoint site are properly saved on your LAN drive as part of the final cleanup in the Minister's office.

The SharePoint Libraries will be deleted on July 18, 2017 after the swearing in of the new Executive Council.

This same procedure was in place for our writ period management of records so you may have already done this!

VIP Services is available to assist if required.

Please contact VIP Services at:

TEL #: 250-953-5151

Email: VIP.Services@gov.bc.ca

Thx.

m

Hendry, Jackie PREM:EX

From: Curtis, David FIN:EX
Sent: Friday, July 14, 2017 2:03 PM
To: Leamy, Michelle T PREM:EX
Subject: Transitional Management of Electronic Information 0.9.2.docx
Attachments: Transitional Management of Electronic Information 0.9.2.docx

Hi Michelle,

Please find the amended version attached. Let me know if you would like to discuss.

Regards,

David

Draft Staff Workflow Concerning Transitional Management of Electronic Information

Note:

- The Deputy Minister to the Premier is identified as the “owner” of all Office of the Premier records noted below.
- The following workflow is specific to transition and does not encompass normal service request processes associated with routine staffing actions.

OFFICE OF THE PREMIER

Activity	Service Delivery Agency	Contact
<p>Retirement of the existing Office of the Premier’s SharePoint site</p> <p>Deletion of the pre-July 18, 2017 SharePoint site, which hosts Ministers Offices’ transitory records libraries (iPad transfers) and all associated content.</p> <p>Information contained within the SharePoint site will be confirmed as exclusively transitory in nature (e.g. duplicate/convenience copies) encompassing records that have been retained within the Office of Primary Responsibility consistent with information schedules and retention policies.</p> <p>Responsible Lead: Michelle Leamy</p>	Information Management Branch (IMB), Ministry of Finance	VIP Services Ministry of Finance (Team Lead: David Henry) 250-953-5151 mailto:VIP.Services@gov.bc.ca
<p>Archiving email accounts for the Premier, Ministers, Political Staff and Office of the Premier’s staff</p> <p>Collection and migration of all pre-July 18, 2017 email folders and associated content.</p> <p>Premier, Ministers, Political Staff and Office of the Premier’s staff email is saved in (.PST) format to a secure network share drive.</p> <p>Responsible Lead: Michelle Leamy</p>	Information Management Branch (IMB), Ministry of Finance	VIP Services Ministry of Finance (Team Lead: David Henry) 250-953-5151 mailto:VIP.Services@gov.bc.ca

Activity	Service Delivery Agency	Contact
<p>Isolation and distribution of copies of the existing Ministers Offices' LAN Shares to the newly appointed Deputy Ministers with related portfolio responsibilities</p> <p>Isolation of all pre-July 18, 2017 Minister's Offices LAN Shares and any associated content. Access to copies of the drive content will be made available upon request to the newly appointed Deputy Ministers to support specific operational requirements (e.g. program requirements, FOI, or litigation). Given the potential for a reallocation of portfolio responsibilities, individual LAN Shares may have to be disseminated to and/or concurrent access provided to other responsible Deputy Minister(s).</p> <p>Each DM request for materials will identify the purpose for the access. Once accessed and the operational requirement is complete, the copied drive contents must be deleted and notification provided to VIP services that the preceding steps have concluded.</p> <p>Note that the post-July 18, 2017 Ministers Offices' LAN Shares will be established as new LAN Shares.</p> <p>Responsible Lead: Don Wright or alternate</p>	<p>Information Management Branch (IMB), Ministry of Finance</p>	<p>VIP Services Ministry of Finance (Team Lead: David Henry) 250-953-5151 mailto:VIP.Services@gov.bc.ca</p>
<p>Distribution of email accounts for the Premier, Ministers, Political Staff and Office of the Premier's staff to the newly appointed Deputy Ministers with related portfolio responsibilities</p> <p>In response to specific operational requirements, the newly appointed Deputy Ministers may request copies of the pre-July 18, 2017 email accounts of the Premier, Ministers, Political Staff and Office of the Premier's staff saved on the secure network share drive. Given the potential for a reallocation of portfolio responsibilities, individual emails may have to be disseminated to and/or concurrent access provided to other responsible Deputy Minister(s).</p> <p>The Deputy Minister to the Premier will, upon request, have access to emails from the Premier and all Premier's Office staff.</p>	<p>Information Management Branch (IMB), Ministry of Finance</p>	<p>VIP Services Ministry of Finance (Team Lead: David Henry) 250-953-5151 mailto:VIP.Services@gov.bc.ca</p>

As with the LAN drive contents, each DM request for materials will identify the purpose for the access. Once accessed and the operational requirement is complete, the copy email materials must be deleted and notification provided to VIP services that the preceding steps have concluded.		
Responsible Lead: Don Wright or alternate		
Activity	Service Delivery Agency	Contact
New office infrastructure Establishment of new LAN structure and access, iDIR accounts, Email and other SharePoint sites as required. Note that new Ministers Offices' LAN Shares will be established. Responsible Lead: Don Wright or alternate	Information Management Branch (IMB), Ministry of Finance Additional Resource: Government Records Service, Ministry of Finance	VIP Services Ministry of Finance (Team Lead: David Henry) 250-953-5151 mailto:VIP.Services@gov.bc.ca Trevor Youdale 250 356-0845 Trevor.Youdale@gov.bc.ca

DEPUTY MINISTERS' OFFICES

Activity	Service Delivery Agency	Contact
New office infrastructure Establishment of new LAN structure and access, iDIR accounts, Email and other SharePoint sites as required. Responsible Lead: Newly Appointed Deputy Minister or alternate	Ministry of Technology, Innovation and Citizens Services	iStore request as per the standard processes defined within each Ministry.
Access to previous Deputy Ministers Email accounts (as required) This information is retained and may be accessed for operational use only (e.g. program requirements, FOI, or litigation). Incoming Deputy Ministers may request access for themselves and one DMO alternate. Once accessed and the requirement is complete, the copy of the email folders and contents must be deleted.	Information Security Branch, Office of the Chief Information Officer	Ken Prosser 250 387-5931 ken.prosser@gov.bc.ca

<p>Please note given the potential for a reallocation of portfolio responsibilities, individual emails may have to be disseminated to and/or concurrent access provided to other responsible Deputy Minister(s).</p> <p>Responsible Lead: Newly Appointed Deputy Minister or alternate</p>		
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--