Cabinet Operations Information Destruction Authorization – Decentralized Model

Introduction

Cabinet Operations, as an office within the Office of the Premier, is following a decentralized model to authorize on-site destruction of information/records.

The scope of this Information Destruction Authorization (IDA) procedure covers paper and electronic records following an approved schedule, and adequate documentation of decisions to destroy government information.

Outside the scope of this document are routine practices to manage transitory records.

These procedures are intended to demonstrate a consistent, repeatable, defensible, and documented procedure to record ministry authorizations for destructions which prevents the unauthorized or premature destruction of records.

Roles and Responsibilities

Cabinet Operations' roles and responsibilities to implement the IDA are primarily with the Records Management Office (RMO) with support from the Branch Administrator.

IDAs are approved by the Manager of Cabinet Operations and/or the ADM/Deputy Cabinet Secretary.[1]

The RMO is responsible for leading the tasks in preparation for approvals to destroy records and information. The Branch Administrator may assist with identifying eligible records, preparing file lists and documentation, and completing destruction tasks.

[1] Most IDAs will be approved by the Manager of Cabinet Operations, who may use discretion to request authorization from the ADM/Deputy Cabinet Secretary based on program area knowledge. For example, destruction authorization for administrative, financial, FOI case files, past employee files would typically be approved by the Manager. Candidates for ADM/Deputy Cabinet Secretary approval might include litigation search files and Auditor General files.

Procedure

Preparer/Coordinator Roles	Responsibility
Identify and list records eligible for destruction using GRS file list template, ensuring all required information for destruction (DE) authorization is documented.	RMO/Br Admin
Assign and log destruction number. Open ARCS file 432-30 on LAN and file: – IDA form (ARS518) – File list (ARS661)	RMO RMO/Br Admin
Verify records are eligible for destruction in accordance with approved information schedules: – SO (Superseded or Obsolete) criteria are met, – No related litigation, legal action, FOIPPA requests or investigations require the records to be retained. Consult with subject matter experts to confirm eligibility if required. Ensure documentation is accurate and complete.	RMO
Forward completed IDA	RMO
Complete destruction following approvals. Update the Destruction Log.	RMO/Br Admin RMO
Approver Role	**Responsibility**
Verify the destruction is appropriate based on program area knowledge.	Manager
Confirm the records are not needed to meet operational and administrative requirements, related litigation, legal action, requests made under FOIPPA, or investigations that are underway or anticipated.	Manager / ADM* *see Roles & Responsibilities
Ensure records are only destroyed in accordance with approved information schedules.	Manager / ADM* *see Roles & Responsibilities

Systems/Application Roles

- s. 13
-

Defensible Destruction Documentation

The Cabinet Operations Destruction Log and a copy of the current (2022) Destruction File List (ARS661) are filed on the LAN under the ARCS classification 432-30 Destruction Case Files – Authorized Internally. (CY + 30y nil DE). The file provides evidence of defensible destruction and long-term reference for future accountability.

The log and associated file lists are retained in a searchable format (Optical Character Recognition or OCR, or in .pdf), and are saved here:

J:_ARCS (100-1999)\100-499 ADMINISTRATION\432 Records Management\432-30 Destruction Case Files - Decentralized authorization

File lists are created and saved using the prescribed template supported by Government Records Service (ARS661). The Government Records Service intranet site should be referenced to ensure the most recent version of the template is used each time a new records culling project is undertaken.

Information Destruction Log Naming Conventions

Cabinet Operations' Information Destruction Log uses the following naming conventions:

DEYY-###-PREM-CabOps

- YY = Two-digit calendar year, consistent with the retention schedule covering the log (CY+30y nil DE).
- ### = Unique, sequential information destruction number, starting at 001.

Destruction Method

On-site paper records are securely destroyed using Shred It bins under the Corporate Supply Arrangement.

Redundant Source Information (RSI) Destructions

Cabinet Operations has 1 approved Redundant Source Information application (RSIS-0159) covering Conflict of Information disclosure forms, and Confidentiality Agreements related to external guests attending a Cabinet or Cabinet Committee meeting.

Annual Review

This procedure will be reviewed concurrently with reviews and updates to the Cabinet Operations Manual, or when the Government Records Service (CITZ) publishes updates to the *Defensible Information Destruction Guide* .

Resources

Additional resources available from Government Records Service including role-based learning, guides and forms are available here:

DID - Learning (gov.bc.ca)

07/18/2022

Approved by: Amy Miller, ADM/Deputy Cabinet Secretary

Date

From: Barwise, Lisa A CITZ:EX(Lisa.Barwise@gov.bc.ca)

To: Elliott, Genevieve IGRS:EX (Genevieve.Elliott@gov.bc.ca); Peterson, Melanie IGRS:EX (Melanie.Peterson@gov.bc.ca)

To: Barwise, Lisa A CITZ:EX (Lisa.Barwise@gov.bc.ca)

Subject: CRMS Conversion Project for OOP: Final Charter and Timeline

Sent: 01/07/2021 17:06:30

Attachments: OOP CRMS Migration Project Charter on a page.PDF, OOP timeline v2.PDF

Good morning, attached are copies of the Charter and Timeline for your records.

Thank you,
Lisa

------< Content Manager record Information >------

Record Number:D4144321A
Title:OOP CRMS Migration Project Charter on a page

------< Content Manager record Information >------

Record Number:D2130321A
Title:OOP timeline v2

From: van Marum, Karen IGRS:EX(Karen.vanMarum@gov.bc.ca)
To: Milne, Karen IGRS:EX (Karen.Milne@gov.bc.ca)
Subject: FW: Offsite Records Access - Policy
Sent: 12/08/2023 22:48:14

From: Westgate, Rachael IGRS:EX <Rachael.Westgate@gov.bc.ca>
Sent: Tuesday, January 18, 2022 1:16 PM
To: Dawes, Sandra IGRS:EX <Sandra.Dawes@gov.bc.ca>; Francis, Darren IGRS:EX <Darren.Francis@gov.bc.ca>; van Marum, Karen IGRS:EX <Karen.vanMarum@gov.bc.ca>
Subject: Offsite Records Access - Policy

Hello all,

Please note that you have been added as an approved IGRS contact to retrieve records from BC archives on the policy side as required (Genevieve and the protocol assistants have access for their branch's files). I have added each of your names to all accessions IGRS policy has sent to archives, so if there is ever a need, you now have that ability 😊

The process for requesting documents from BC archives is as follows (full procedures manual available on the LAN):

To request a file from offsite storage, you need to know:

- The file number and/or title, accession number and box number of the file

(If the person requesting the file does not know, you may have to search the Accessions Database and the related Accession case files to find the file. When searching the Accessions Database, check to see whether the box the file is in has been deleted. If the file was sent offsite or destroyed using the CRMS process, information about the status and location of the file will be in CRMS but remember that CRMS was only used since 2005.)

- Location of the file (Access or File Tech) (from the Accessions Database)
- Name(s) of person(s) authorized to access the file (from the Accessions Database)

The Off-site Storage Records Retrieval Form is here: http://www.for.gov.bc.ca/isb/forms/lib/ars626.pdf

- Pick the appropriate location
- Rush service is available for an extra fee. Only use when you need the file urgently. Usually the files come the day you request them or the next day so choose Regular.
- Print the form and fax it to the relevant facility

NOTE – When the box(es) or file(s) come a delivery slip will accompany your order. It is a good idea to keep the slips because sometimes the offsite warehouses lose track of whether you ordered or returned some items.

If any questions, don't hesitate to reach out.

Thanks!

Rachael Westgate
(She/Her)
Manager of Executive Operations
Intergovernmental Relations Secretariat | Office of the Premier
O: 778-974-5461
I respectfully acknowledge the Lekwungen People, known today as the Esquimalt and Songhees Nations, and all the Indigenous Peoples of British Columbia. I am grateful to be able to live, work and play in their territories.

From: van Marum, Karen IGRS:EX(Karen.vanMarum@gov.bc.ca)
To: Milne, Karen IGRS:EX (Karen.Milne@gov.bc.ca)
Subject: FW: Records Destruction support material
Sent: 12/08/2023 22:48:45

From: Lewthwaite, Jennifer IGRS:EX <Jennifer.Lewthwaite@gov.bc.ca>
Sent: Tuesday, March 22, 2022 1:01 PM
To: Peterson, Melanie IGRS:EX <Melanie.Peterson@gov.bc.ca>; van Marum, Karen IGRS:EX <Karen.vanMarum@gov.bc.ca>
Cc: Elliott, Genevieve IGRS:EX <Genevieve.Elliott@gov.bc.ca>
Subject: Records Destruction support material

Good afternoon,

I understand from Rachael that you both have agreed to take on the role of coordinators for your respective teams. We had a call last week with Bev Qualizza (Government Records Officer) and understand that the original timeline of April 1st has been pushed out. She's provided a link to more information and resources on the Defensible Information Destruction process https://www2.gov.bc.ca/gov/content?id=CB23673504C747059D1705238C5944A2.

Do you feel like you have what you need to get started? Any additional training or support needs?

Jen

From: van Marum, Karen IGRS:EX(Karen.vanMarum@gov.bc.ca)
To: Milne, Karen IGRS:EX (Karen.Milne@gov.bc.ca)
Subject: FW: Records Destruction support material
Sent: 12/08/2023 22:49:07
Attachments: Project Plan-Ministry Destruction Authorization Model-20220114.docx

From: Lewthwaite, Jennifer IGRS:EX <Jennifer.Lewthwaite@gov.bc.ca>
Sent: Tuesday, March 22, 2022 2:13 PM
To: Peterson, Melanie IGRS:EX <Melanie.Peterson@gov.bc.ca>; van Marum, Karen IGRS:EX <Karen.vanMarum@gov.bc.ca>
Cc: Elliott, Genevieve IGRS:EX <Genevieve.Elliott@gov.bc.ca>
Subject: RE: Records Destruction support material

Do you mean this one?

From: Peterson, Melanie IGRS:EX <Melanie.Peterson@gov.bc.ca>
Sent: March 22, 2022 2:07 PM
To: Lewthwaite, Jennifer IGRS:EX <Jennifer.Lewthwaite@gov.bc.ca>; van Marum, Karen IGRS:EX <Karen.vanMarum@gov.bc.ca>
Cc: Elliott, Genevieve IGRS:EX <Genevieve.Elliott@gov.bc.ca>
Subject: RE: Records Destruction support material

Hi Jen,

I think I am up to date with the training required but maybe it would be helpful to view the destruction authorization model document to make sure? Admittedly, it's been a while since I've seen it!

Thanks,

Melanie Peterson *(she/her)*
Protocol Assistant
Office of Protocol
Intergovernmental Relations Secretariat
Phone: (250) 356-1105 **Fax:** (250) 356-2814
Email: melanie.peterson@gov.bc.ca

From: Lewthwaite, Jennifer IGRS:EX <Jennifer.Lewthwaite@gov.bc.ca>
Sent: March 22, 2022 1:08 PM
To: van Marum, Karen IGRS:EX <Karen.vanMarum@gov.bc.ca>; Peterson, Melanie IGRS:EX <Melanie.Peterson@gov.bc.ca>
Cc: Elliott, Genevieve IGRS:EX <Genevieve.Elliott@gov.bc.ca>
Subject: RE: Records Destruction support material

Well we have a little more time now as if I recall correctly (Genevieve can correct me if I am wrong 😊) we have till end of the calendar year now…..

From: van Marum, Karen IGRS:EX <Karen.vanMarum@gov.bc.ca>
Sent: March 22, 2022 1:02 PM
To: Lewthwaite, Jennifer IGRS:EX <Jennifer.Lewthwaite@gov.bc.ca>; Peterson, Melanie IGRS:EX <Melanie.Peterson@gov.bc.ca>
Cc: Elliott, Genevieve IGRS:EX <Genevieve.Elliott@gov.bc.ca>
Subject: Re: Records Destruction support material

I need time to do all the training (haha!)

Get Outlook for iOS

From: Lewthwaite, Jennifer IGRS:EX <Jennifer.Lewthwaite@gov.bc.ca>
Sent: Tuesday, March 22, 2022 1:01:09 PM
To: Peterson, Melanie IGRS:EX <Melanie.Peterson@gov.bc.ca>; van Marum, Karen IGRS:EX <Karen.vanMarum@gov.bc.ca>
Cc: Elliott, Genevieve IGRS:EX <Genevieve.Elliott@gov.bc.ca>
Subject: Records Destruction support material

Good afternoon,

I understand from Rachael that you both have agreed to take on the role of coordinators for your respective teams. We had a call last week with Bev Qualizza (Government Records Officer) and understand that the original timeline of April 1st has been pushed out. She's provided a link to more information and resources on the Defensible Information Destruction process https://www2.gov.bc.ca/gov/content?id=CB23673504C747059D1705238C5944A2.

Do you feel like you have what you need to get started? Any additional training or support needs?

Jen

From: van Marum, Karen IGRS:EX(Karen.vanMarum@gov.bc.ca)
To: Milne, Karen IGRS:EX (Karen.Milne@gov.bc.ca)
Subject: FW: Records mgmt resources
Sent: 12/08/2023 22:48:29
Attachments: transitory-information-quick-tips.pdf, email_guide_-_20190613_-_current.pdf

From: Westgate, Rachael IGRS:EX <Rachael.Westgate@gov.bc.ca>
Sent: Thursday, January 20, 2022 3:53 PM
To: Longpre, Nicole IGRS:EX <Nicole.Longpre@gov.bc.ca>; Vinette, Nicole IGRS:EX <Nicole.Vinette@gov.bc.ca>; van Marum, Karen IGRS:EX <Karen.vanMarum@gov.bc.ca>
Subject: Records mgmt resources

Hello all,

Thanks for reaching out today to discuss the Policy team's records management strategies. As promised, I've attached a couple of the general CITZ guidelines for transitory documents as well as for email management, should they prove useful. Please feel free to share with the team. The resource hub for records management is a great spot to get some more in-depth information and guidance for things like training, H: drive storage, naming conventions, and a refresher on the retention schedules ARCS and ORCS. The resource hub is located here:
https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/records-management/training

From our discussion I understand that there is an appetite to do a LAN cleanup/reorg. I think this makes sense and would be a good project to take on in tandem with the ORCS redevelopment, as I suspect that may require rejigging the location of some folders anyways. My expectation is that we will not be assigned a developer resource for this work for another few months.

One thing that the team can turn their minds to right away is clearing out **transitory records** from the LAN, personal H: drives, and emails. As discussed, these records do not require a destruction authorization approval, and can be routinely deleted when no longer needed as long as they are not subject to a search for legal purposes, or to an access request made under the *Freedom of Information and Protection of Privacy Act* (*FOIPPA*). You can read up on the transitory records' retention schedule in more detail here.

As an action item from this meeting, I'll commit to connecting in with our ministry records office to see about arranging an info session on best practices for IGRS and/or the policy team. I will also work with Sandra to get some of the corporate quick fact sheets for transitory docs etc. incorporated into the welcome binder. Once your team has pulled together a list of frequently generated records, I'll work to create a quick guide on retention practices for those.

Thanks, and let me know if there's anything else I can do to assist 😊

Rachael Westgate
(She/Her)
Manager of Executive Operations
Intergovernmental Relations Secretariat | Office of the Premier
O: 778-974-5461
I respectfully acknowledge the Lekwungen People, known today as the Esquimalt and Songhees Nations, and all the Indigenous Peoples of British Columbia. I am grateful to be able to live, work and play in their territories.

From: van Marum, Karen IGRS:EX(Karen.vanMarum@gov.bc.ca)
To: Milne, Karen IGRS:EX (Karen.Milne@gov.bc.ca)
Subject: FW: for discussion at PNP: Ministry Destruction Authorization Model
Sent: 12/08/2023 22:48:04
Attachments: Project Plan-Ministry Destruction Authorization Model-20220114.docx

---

From: Westgate, Rachael IGRS:EX <Rachael.Westgate@gov.bc.ca>
Sent: Friday, January 14, 2022 2:41 PM
To: Maranda, Pierrette IGRS:EX <Pierrette.Maranda@gov.bc.ca>; Brownsey, Silas IGRS:EX <Silas.Brownsey@gov.bc.ca>; Lobmeier, Lucy S IGRS:EX <Lucy.Lobmeier@gov.bc.ca>; Smith, Grant H IGRS:EX <Grant.H.Smith@gov.bc.ca>; van Marum, Karen IGRS:EX <Karen.vanMarum@gov.bc.ca>; Portal, Vincent IGRS:EX <Vincent.Portal@gov.bc.ca>; Vinette, Nicole IGRS:EX <Nicole.Vinette@gov.bc.ca>
Cc: Elliott, Genevieve IGRS:EX <Genevieve.Elliott@gov.bc.ca>; Francis, Darren IGRS:EX <Darren.Francis@gov.bc.ca>
Subject: for discussion at PNP: Ministry Destruction Authorization Model

Hello all,

In advanced of Monday's PNP meeting, I am attaching a draft project plan for an **IGRS Ministry Destruction Authorization Model**, which Genevieve and I have been working on. This work has been initiated in response to an ask from Government Records Services to bring the administration and approvals for destruction of government records away from CIRMO and into the ministries. Their hope is to have each ministry develop their own team of administrators/approvers to facilitate this process, and (ideally) have them trained and ready by April 1, 2022. The attached project plan gives a high-level overview of the ask, a refresher on IGRS' current process for applying to destroy records, and an overview of the training that would be required of staff responsible for the model.

Our hope on Monday is to discuss possible governance structures for this in-house model, and to identify potential resources within IGRS to take on this work. You will notice that GRS has proposed a series of roles (preparer, approver, coordinator) to fulfill this responsibility, but this is not prescriptive and can be mixed/matched/customized for each ministry. For the purpose of this project, IGRS has been categorized as its own "ministry".

Looking forward to your thoughts on Monday.

Many thanks,

Rachael Westgate
(She/Her)
Manager of Executive Operations
Intergovernmental Relations Secretariat | Office of the Premier
O: 778-974-5461
I respectfully acknowledge the Lekwungen People, known today as the Esquimalt and Songhees Nations, and all the Indigenous Peoples of British Columbia. I am grateful to be able to live, work and play in their territories.

From: van Marum, Karen IGRS:EX(Karen.vanMarum@gov.bc.ca)
To: Milne, Karen IGRS:EX (Karen.Milne@gov.bc.ca)
Subject: FW: records destruction - coordinator training
Sent: 12/08/2023 22:48:32

From: Westgate, Rachael IGRS:EX <Rachael.Westgate@gov.bc.ca>
Sent: Monday, February 28, 2022 12:06 PM
To: van Marum, Karen IGRS:EX <Karen.vanMarum@gov.bc.ca>
Subject: records destruction - coordinator training

No timeline set on these – Suspect you should be in the clear for about 6 months to complete the training and review the docs mentioned. This list was created by GRS, but they did not link to where to find the docs, so I'll do some poking around and see if I can't get them all rounded up for you…I have time with GRS tomorrow to chat records so I'll inquire if they have housed the resources somewhere central. stay tuned for a follow up email.

Training:

1. .IM 117 Information Management: Access, Information Security, Privacy and Records Management (ITEM-652)
2. .IM 112: Records Management Foundations (ITEM-1100)
3. .Records Disposal module within the Records Management: Administrative Practices (ITEM-1161) course
4. .Digital Recordkeeping: Developing Organizational Excellence (ITEM-1395)

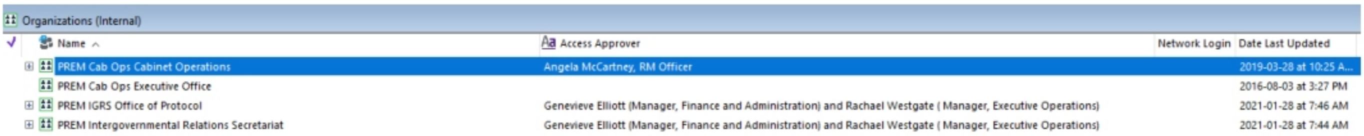
Documents to review:

5. .Appropriate Recordkeeping System (PDF)
6. .Critical Information (PDF)
7. .CRO Directive on Documenting Government Decisions
8. .CRO Guidelines on Documenting Government Decisions
9. .Practitioner's Guide to the Information Management Act
10. .ARCS & ORCS User Guide
11. .Information Schedules
12. .Key to ARCS/ORCS Codes and Acronyms (PDF)
13. .Section 3 of the Recorded Information Management (RIM) Manual
14. .Records Management Community | How to Manage Government Information | Destruction of Onsite Records

Rachael Westgate
(She/Her)
Manager of Executive Operations
Intergovernmental Relations Secretariat | Office of the Premier
O: 778-974-5461
I respectfully acknowledge the Lekwungen People, known today as the Esquimalt and Songhees Nations, and all the Indigenous Peoples of British Columbia. I am grateful to be able to live, work and play in their territories.

From: Larade, Sharon P CITZ:EX(Sharon.Larade@gov.bc.ca)
To: Elliott, Genevieve IGRS:EX (Genevieve.Elliott@gov.bc.ca)
To: Hold - 220321 - Westgate, Rachael IGRS:EX (Rachael.Westgate@gov.bc.ca); Peterson, Melanie IGRS:EX (Melanie.Peterson@gov.bc.ca)
Subject: For approval: Office of the Premier Security Basics for EDRMS
Sent: 02/24/2021 20:37:58
Attachments: Office of the Premier Security Basics final 20210122.DOCX

Hi Genevieve,
Yes, as requested, we have updated the Designated Access Approvers in the system as follows:



Organizations (Internal)

Name	Access Approver	Network Login	Date Last Updated
PREM Cab Ops Cabinet Operations	Angela McCartney, RM Officer		2019-03-28 at 10:25 A...
PREM Cab Ops Executive Office			2016-08-03 at 3:27 PM
PREM IGRS Office of Protocol	Genevieve Elliott (Manager, Finance and Administration) and Rachael Westgate (Manager, Executive Operations)		2021-01-28 at 7:46 AM
PREM Intergovernmental Relations Secretariat	Genevieve Elliott (Manager, Finance and Administration) and Rachael Westgate (Manager, Executive Operations)		2021-01-28 at 7:44 AM

Can you please review the attached Security Basics document, and reply via email with your approval or any other changes?
Thanks

Sharon Larade
Business Services Manager, Enterprise Document and Records Management Systems (EDRMS)
Government Records Service, Corporate Information and Records Management Office
Ministry of Citizens' Services
Office (250) 387-4129; cell (250) 589-1328 Sharon.larade@gov.bc.ca
Records Management Systems   EDRMS Implementations   EDRMS Readiness

---

From: Elliott, Genevieve IGRS:EX <Genevieve.Elliott@gov.bc.ca>
Sent: January 27, 2021 4:04 PM
To: Larade, Sharon P CITZ:EX <Sharon.Larade@gov.bc.ca>
Cc: Westgate, Rachael IGRS:EX <Rachael.Westgate@gov.bc.ca>; Peterson, Melanie IGRS:EX <Melanie.Peterson@gov.bc.ca>
Subject: FW: For approval: Office of the Premier Security Basics

Hi Sharon, can you please make Rachael Westgate & myself the Designated Access Approvers?

From: Larade, Sharon P CITZ:EX <Sharon.Larade@gov.bc.ca>
Sent: January 22, 2021 1:26 PM
To: Elliott, Genevieve IGRS:EX <Genevieve.Elliott@gov.bc.ca>; Peterson, Melanie IGRS:EX <Melanie.Peterson@gov.bc.ca>
Subject: For approval: Office of the Premier Security Basics

Hi Melanie and Genevieve,
Thanks for the discussion this morning; attached is a revised Security Basics for approval; let me know the results of your discussion with Lucie Lobmeier and others on your team.

Please let me know who you would like to be listed in the system as the Designated Access Approver for your area; this can be one or multiple individuals, depending on what you need for backup. These individuals be who we will receive approval from for new user or modify user forms.

Let me know if you have any additional questions or concerns,
Sharon

From: Larade, Sharon P CITZ:EX
Sent: January 15, 2021 2:57 PM
To: Elliott, Genevieve IGRS:EX <Genevieve.Elliott@gov.bc.ca>; Peterson, Melanie IGRS:EX

<Melanie.Peterson@gov.bc.ca>
Cc: Barwise, Lisa A CITZ:EX <Lisa.Barwise@gov.bc.ca>
Subject: Office of the Premier Security Basics draft 20210115

Hi Melanie and Genevieve,
I've drafted the attached Security Basic document to outline your environment in EDRMS.
We can plan some time next week to discuss it together, and answer any questions you may have.

Sharon Larade
Business Services Manager, Enterprise Document and Records Management Systems (EDRMS)
Government Records Service, Corporate Information and Records Management Office
Ministry of Citizens' Services
Office (250) 387-4129; cell (250) 589-1328 Sharon.larade@gov.bc.ca
Records Management Systems   EDRMS Implementations   EDRMS Readiness

------< Content Manager record Information >------

Record Number :   D10538921A
Title   :   Office of the Premier Security Basics draft 20210115

From:	Appleby, Danielle CITZ:EX(Danielle.Appleby@gov.bc.ca)
To:	Elliott, Genevieve IGRS:EX (Genevieve.Elliott@gov.bc.ca); Peterson, Melanie IGRS:EX (Melanie.Peterson@gov.bc.ca)
Subject:	IGRS - Appropriate Information Destruction (AID) procedure
Sent:	03/21/2023 23:09:58
Attachments:	IDA Model Documentation - Final Draft - FIN.docx

Hello Genevieve and Melanie,
I hope this email finds you well, and that you are enjoying the peeks of sunshine we are now getting graced with more frequently.

I wanted to take a moment to check-in with you and see how you were doing with developing an Appropriate Information Destruction (AID) (previously referred to as "DID") procedure for IGRS.
My understanding is that back in December you met with Wendy and Betty, and were going plan a meeting again with them and a couple other people on your team. But that it has not yet happened. I would like to offer you my aid on this project if there is something I could provide assistance with at this time.
Please let me know if you have any questions, and/or would like to set-up a time to meet and review where you are at with your ministry's AID procedure, or guidance on what your next steps should be.

If you require any further assistance or have any additional questions, please let me know.
Regards,

Danielle Appleby (she/her)
Sr Gov't Records Analyst | GRS | CIRMO | CITZ
P: 778-698-9383

General Inquiries: GRS@gov.bc.ca | **Records Management:** Resources & Info | Guides & Training

I acknowledge and respect the Lekwungen peoples, and I am ever so grateful for the privilege to work and live on the traditional territories of the W̱SÁNEĆ Nations.

From: deMontmorency, Wendy CITZ:EX
Sent: December 9, 2022 11:16 AM
To: Elliott, Genevieve IGRS:EX <Genevieve.Elliott@gov.bc.ca>; Peterson, Melanie IGRS:EX <Melanie.Peterson@gov.bc.ca>
Subject: DID procedure

Hello Genevieve and Melanie,

Thank you for meeting with Betty and me today. As promised, please see attached Defensible Information Destruction procedure created by the Ministry of Finance.

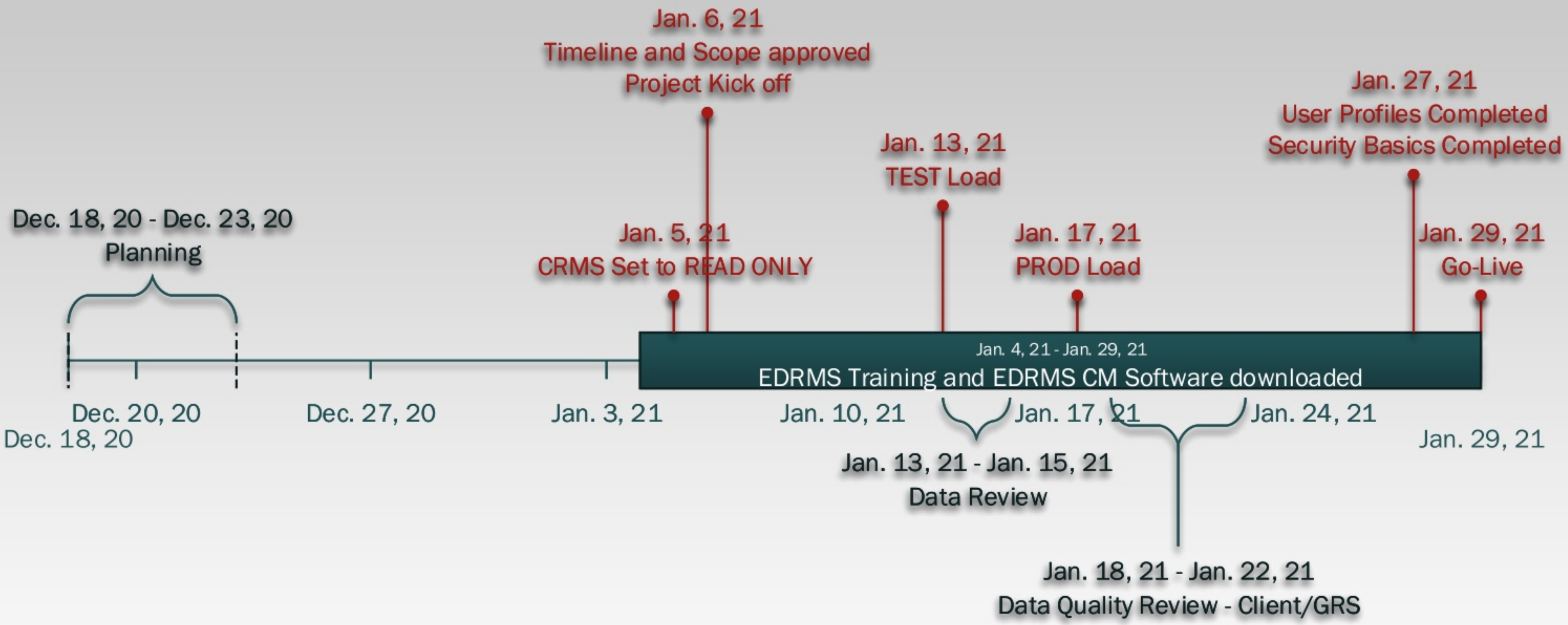
Again, I want to reassure you the destruction process can be paused while you work on the new process and approve it.

If you have any questions, please do not hesitate to contact me.

Regards,

Wendy deMontmorency
Government Records Officer
Government Records Service

Office of the Premier CRMS Migration Timeline



Dec. 18, 20 - Dec. 23, 20
Planning

Jan. 5, 21
CRMS Set to READ ONLY

Jan. 6, 21
Timeline and Scope approved
Project Kick off

Jan. 13, 21
TEST Load

Jan. 17, 21
PROD Load

Jan. 27, 21
User Profiles Completed
Security Basics Completed

Jan. 29, 21
Go-Live

Jan. 4, 21 - Jan. 29, 21
EDRMS Training and EDRMS CM Software downloaded

Jan. 13, 21 - Jan. 15, 21
Data Review

Jan. 18, 21 - Jan. 22, 21
Data Quality Review - Client/GRS

Scope: Data about 4154 Records in 3 ORG Units and 4 New EDRMS CM Users, Export Data Reports about 6 ORG units

Updated: January 6, 2021

Office of the Premier

EDRMS Content Manager Implementation
Security Basics Documentation

2021-01-22

Recommended by:

Sharon Larade

Business Service Manager, EDRMS

Government Records Service

Approved by:

Genevieve Elliott

Manager, Finance and Administration

File: ARCS-06450-80/24012A

Purpose: To outline security functionality for records filed in EDRMS Content Manager.

EDRMS Content Manager is an enterprise system and is administered at an enterprise level through Government Records Service (GRS).

Security

All records are created and owned by your organization. Each folder has a unique record number based on classification, and no folder can be created without classification.

Actions taken on folders and documents are audited. The audit log will identify the action, the time it occurred, and the user who took the action. There are more audits on documents as they have written content, unlike folders which are only made of metadata.

There is no way to delete a record, except by requesting deletion by GRS.

Access to your records is determined by

1. the organizations and specialized groups applied to folders,
2. the user's membership in those organizations and groups, and
3. the user's profile permissions.

Organizations and groups
Default organizations are applied to folders at the time they are opened. A document inherits the security settings from the folder in which it is placed and all documents in a folder will have the same settings. Specialized access can also be added to further restrict the security on folders. This approach is generally used to narrow access to sensitive files, for example, those which relate to executive or human resources issues. Membership in these groups must be monitored by the client. The GRS EDRMS Team and Client Services Team are associated in your configuration through their application to defaults. This access is required to support you in your work. GRS members are not able to open and read documents.

Users
Every user must, at the very least, be a member of your organization; they cannot only be a member of a special access group. Their access must be approved by someone of authority in your organization, who understands the risks associated with granting access to records. The approver may designate others in the organization as backup approvers. All requests for access must be made using either the New User Access Request form or the Modify User Access Request form . If staff leave the organization, GRS must be alerted so that the user can be deactivated in the system. Leaving them activated is a risk to security.

If a user is given the incorrect access, once notified, we will immediately remove the incorrect access, and check the audit log for any activity by the user. If the user is found to have accessed records, an information incident will be opened.

User Profiles

- Inquiry Users (IQ) - can search for documents and folders, and can read documents.
- End Users (EU) - can search for documents and folders, and can create, read and edit documents.
- Information Workers (IW)- can create, search for, and edit documents, folders, and boxes, and can move documents between folders. IW's are the ones in the office who will be managing your records. IW's must be members of your File Creator group.

Your Infrastructure

Record Types
PREM BOX - OFFSITE TRANSFERS
PREM BOX - ONSITE DESTRUCTIONS/STORAGE
PREM IGRS OOP P-FOLDER
PREM IGRS P-FOLDER

Branch
PREM IGRS Office of Protocol
PREM Intergovernmental Relations Secretariat

Groups
PREM IGRS OOP File Creator
PREM IGRS File Creator

Developing a Ministry Destruction Authorization Model

Project Plan: December 2021-April 2022

Project Overview:

The current authorization process for the destruction of government information is comprised of shared approval responsibilities between Government Record Service (GRS) and ministries. The purpose of the Records Destruction Authorization Model Project is to increase ministry autonomy and streamline authorities for the destruction of government information according to approved information schedules. The new authorization model will align with the Information Management Act (IMA) and the Managing Government Information Policy (MGIP) by shifting approval functions **from GRS to ministries.**

Ministries have now been tasked with developing a Ministry Destruction Authorization Model, to come into effect **April 1, 2022.** In order to effectively initiate this model, a governance structure will need to be established, staff leads will need to complete all mandatory training, and the new process will need to be communicated out to all IGRS staff.

Background:

To comply with the IMA, government bodies must create and maintain adequate records of their decisions and ensure:

- An appropriate system is in place for maintaining government information;
- Information is classified according to approved information schedules;
- If no information schedule exists, information must be retained until its disposition is approved by the Chief Records Officer;
- **Destruction actions are authorized and reviewable;**
- Destruction is automated through business rules, where possible;
- Information can be maintained indefinitely if necessary (e.g., in the case of a litigation hold);
- Action or date-based retention triggers can be set;
- Deletion should apply to records, their back-ups, and their metadata; and,
- **Records disposal actions are documented.**

Ministries can be called upon to provide evidence of destruction approvals for related litigation, legal action, requests made under FOIPPA, or investigations that are underway or anticipated. It is important that ministries adequately document decisions to destroy government information to be able to demonstrate that the information existed at one time but was destroyed as per an approved information schedule.

Controls to protect the privacy and security of personal information must also be in place when destroying information; FOIPPA Section 30 - Protection of personal information advises that public bodies should keep a record of the personal (and non-personal) information they destroy, are responsible for ensuring that the disposal of personal information has been approved by the designated authority, and must retain personal information that has been used to make a decision affecting an individual for a minimum of one year. GRS recommends that an adequate Ministry Destruction Authorization Model is in place to ensure that personal information is not destroyed earlier than one year.

GRS recommends that each Ministry Destruction Authorization Model should:

- Clearly define ministry roles and responsibilities for destruction approvals and overall coordination;
- Demonstrate a consistent, repeatable, defensible, and documented procedure to record ministry authorizations for information destructions which prevents the unauthorized or premature destruction of records;
- Ensure that the necessary resources, tools, and forms are available for ministry program areas to adequately document destructions;
- Ensure staff have the required knowledge and training to complete their roles and responsibilities effectively; and,
- Regularly review the authorization model to ensure adequacy and effectiveness over time.

Current IGRS Destruction Model:

All disposition of IGRS records is in accordance with relevant legislation and policy; see RIM 501 Records Destruction, and ministry/agency procedures.

- Records are created according to the ARCS/ORCS schedule
    - Office of Protocol ORCS schedule 881036;
    - Intergovernmental Relations ORCS schedule 881099
    - Francophone Affairs Program only has ARCS records
- Records that have reached the final disposition of "Destruction" are reviewed by the appropriate program manager before the "Destruction" process is started.
- Records that are destined for "Destruction", are documented on a "Records Destruction Authorization – ARS 518" form according to the appropriate records schedule. The completed form, file list and manager approval are then sent to the GRS Records Officer for approval.
- All of the documents pertaining to the destruction are filed in ARCS file 432-35 (Destruction case files – authorized by central agency)
- Records that have been approved for destruction by the Government Records Service Office are issued a destruction number and are placed within the secured shred bin within our office. If the records are too large for the secured recycle bin, arrangements are made for shredding onsite.
- When the actual destruction is completed, the ARS518 form is completed and returned to the Government Records Service Office.
- EDRMS is updated for the disposition of these records to "Destroyed"

Approach:

Step One: Get Started

IGRS employees responsible for information management (Rachael Westgate and Genevieve Elliot) will seek executive direction for the Ministry Destruction Authorization Model which best meets the needs of the organization.

Step Two: Define Roles and Responsibilities

To ensure staff have the required knowledge and training to complete their functions effectively, IGRS must clearly define and communicate the roles and responsibilities within their organization required to carry on defensible destruction of information.

It is recommended that three roles are involved in each records destruction approval: preparer, approver, and ministry coordinator.

An example of role definitions is included below:

1) **Preparer Role:** Responsible for preparing adequate documentation pertaining to government information destructions; and, possesses sound knowledge of their program's information, recordkeeping systems and relevant classifications.
2) **Approver Role:** Responsible for verifying the accuracy of destruction documentation; possesses general knowledge of records management principles; and, confirms that records are not required for operational requirements, related litigation, legal action, requests made under FOIPPA, or investigations that are underway or anticipated.
3) **Ministry Coordinator Role:** Provides governance, oversight, and administration of the Ministry Defensible Destruction Model; ensures that the necessary resources, tools, and forms are available for ministry program areas to adequately document destructions; defines, documents, and communicates ministry-specific training and knowledge requirements (e.g., destroying government information within a ministry line of business application); issues destruction control numbers and maintains documentation of approvals; and, reviews the effectiveness of the Ministry Defensible Destruction Model and implements improvements, as required.

IGRS appointments into roles will be determined by the IM resources available within the secretariat.

Preparers and approvers may reside within separate work units (e.g., administrative assistants, supervisors, managers, directors, etc.).

Step Three: Determine Role-Based Training and Ministry Documentation Requirements

Before preparing and approving the destruction of government information, employees should receive adequate training (i.e., as defined within the Ministry Destruction Authorization Model). In addition to defining ministry-specific training, GRS recommends that ministry employees responsible for preparing, approving, and coordinating the destruction of government information have taken the following courses and reviewed the following materials:

1) IM 117 Information Management: Access, Information Security, Privacy and Records Management (ITEM-652)
2) IM 112: Records Management Foundations (ITEM-1100)
3) Records Disposal module within the Records Management: Administrative Practices (ITEM-1161) course
4) Digital Recordkeeping: Developing Organizational Excellence (ITEM-1395)
5) Appropriate Recordkeeping System (PDF)
6) Critical Information (PDF)
7) CRO Directive on Documenting Government Decisions
8) CRO Guidelines on Documenting Government Decisions
9) Practitioner's Guide to the Information Management Act
10) ARCS & ORCS User Guide
11) Information Schedules
12) Key to ARCS/ORCS Codes and Acronyms (PDF)
13) Section 3 of the Recorded Information Management (RIM) Manual
14) Records Management Community | How to Manage Government Information | Destruction of Onsite Records

After the ministry roles, responsibilities, and role-based training requirements have been defined, IGRS should define the documentation that is required for defensible ministry destructions.

Step Four: Document and Communicate the Ministry Defensible Destruction Model

The Ministry Defensible Destruction Model should be documented, posted, and communicated to relevant employees. IGRS recommendation is to post on the staff SharePoint and present the new model to colleagues at an All-Staff meeting.

Step Five: Regularly Review Model Effectiveness

To ensure relevancy, effectiveness, and efficiency over time, IGRS will regularly review the Ministry Defensible Destruction Model.

Scope:

This project is inclusive of developing a governance framework and implementation strategy for records destruction only. This project is not inclusive of an audit of current records, nor does it include a review of records management best practices. It is recommended that, at the conclusion of this project, IGRS considers hosting a series of information sessions about records management best practices for staff.

Note: IGR Policy has an outdated ORCS schedule (881099) and is awaiting the availability of an ORCS developer resource to proceed with updating their schedule. Therefore, IGR Policy ORCS records will not be eligible for destruction until ORCS schedule 881099 is amended and has been implemented.

Deliverables:

1. Ministry Destruction Authorization Model Project plan
2. Templates for ministry coordinators and approvers

3. Implementation of new model; all-staff presentation

DRAFT Timeline:

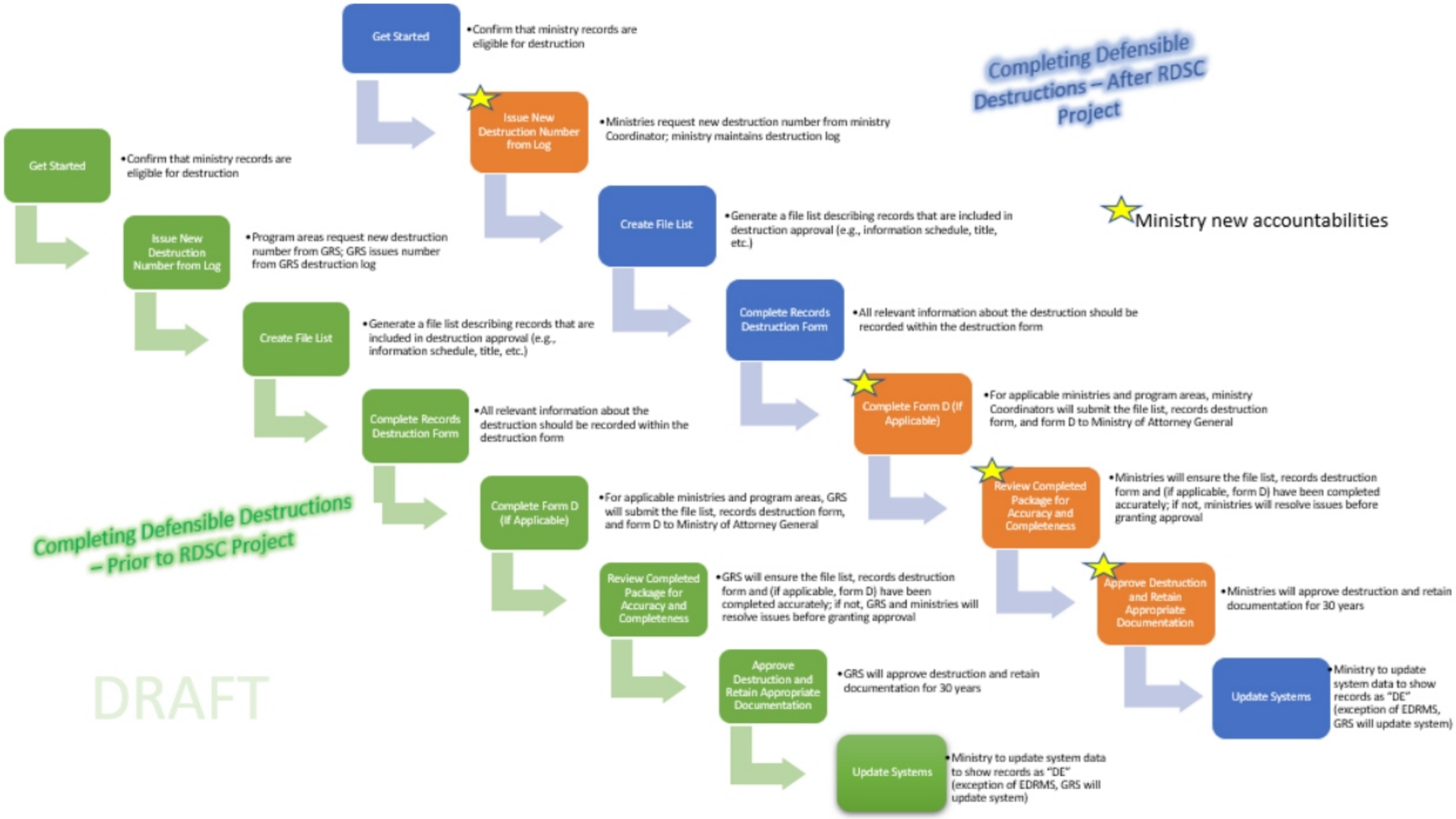
DATES	TASK
December 2021	IGRS IM contacts to create draft project plan
January 14, 2021	A/DM and DM review of draft plan
January 17, 2021	IGRS IM contacts to present plan at PNP and advise of next steps
January 17 – 28	Consultation with IGRS EDs as required
January 31	Decision Note to DM
February 7	IGRS IM contacts to share approved governance model with PNP
February 7 – March 18	Training of IGRS Destruction Authorization Team; development of required documentation/templates; preparation of all staff deck and communications plan
March 24	All Staff presentation of new destruction model; implementation date of April 1
April 1	IGRS Destruction Authorization Model go-live date
October 1	6-month review of project; maintenance; once complete, relegate to annual review

Next Steps:

- A/DM and DM endorsement of project plan
- Present for discussion/direction at PNP
- Consult with work unit leads as required
- Advance decision note to DM for sign off

Attachments:

APPENDIX 1: PROCESS MAP – CHANGES TO COMPLETING DEFENSIBLE DESTRUCTIONS



Completing Defensible Destructions – Prior to RDSC Project

Get Started
- Confirm that ministry records are eligible for destruction

Issue New Destruction Number from Log
- Program areas request new destruction number from GRS; GRS issues number from GRS destruction log

Create File List
- Generate a file list describing records that are included in destruction approval (e.g., information schedule, title, etc.)

Complete Records Destruction Form
- All relevant information about the destruction should be recorded within the destruction form

Complete Form D (If Applicable)
- For applicable ministries and program areas, GRS will submit the file list, records destruction form, and form D to Ministry of Attorney General

Review Completed Package for Accuracy and Completeness
- GRS will ensure the file list, records destruction form and (if applicable, form D) have been completed accurately; if not, GRS and ministries will resolve issues before granting approval

Approve Destruction and Retain Appropriate Documentation
- GRS will approve destruction and retain documentation for 30 years

Update Systems
- Ministry to update system data to show records as "DE" (exception of EDRMS, GRS will update system)

Completing Defensible Destructions – After RDSC Project

Get Started
- Confirm that ministry records are eligible for destruction

☆ Issue New Destruction Number from Log
- Ministries request new destruction number from ministry Coordinator; ministry maintains destruction log

Create File List
- Generate a file list describing records that are included in destruction approval (e.g., information schedule, title, etc.)

Complete Records Destruction Form
- All relevant information about the destruction should be recorded within the destruction form

☆ Complete Form D (If Applicable)
- For applicable ministries and program areas, ministry Coordinators will submit the file list, records destruction form, and form D to Ministry of Attorney General

☆ Review Completed Package for Accuracy and Completeness
- Ministries will ensure the file list, records destruction form and (if applicable, form D) have been completed accurately; if not, ministries will resolve issues before granting approval

☆ Approve Destruction and Retain Appropriate Documentation
- Ministries will approve destruction and retain documentation for 30 years

Update Systems
- Ministry to update system data to show records as "DE" (exception of EDRMS, GRS will update system)

☆ Ministry new accountabilities

Ministry of Finance Information Destruction Procedures

Contents

Overview

This document informs and consolidates the Ministry of Finance's defensible information destruction policies and procedures.

Although Part 2 of the GRS Defensible Information Destruction Guide states there are two types of destructions, Information Destruction Authorizations (IDA) and Redundant Source Information (RSI) Destructions, the Ministry of Finance IDA model considers both types as one simple concept: the destruction of information.

The definition of information, for the purposes of this document, includes:

- Physical records kept on-site (paper, audiovisual, photos, discs etc.), including those managed in EDRMS (p-folders)
- Digital records managed in EDRMS (e-folders), on a LAN, or stored in systems
- Data and metadata stored in systems
- Redundant source information[1]

This process does not apply to the following records:

- Records stored off-site (these are handled through a 60-Day Notices process)
- Records with a final disposition of Selective Retention (SR) or Final Retention (FR)
- Records scheduled under the Transitory Information Schedule

If there are questions about the 60-Day Notices process, please contact your Information Management Analyst or the Ministry Coordinator.

Purpose

This document outlines the destruction process for eligible, scheduled ministry information. Information covered under this process becomes eligible once it has reached the Final Disposition stage and has a final disposition of DE (Destroy).

This Finance Information Destruction Application (IDA) Model meets the GRS requirements set by section 4.1 of the Defensible Information Destruction Guide. Requirements are met by the establishment and approval of a defensible process that includes established roles and responsibilities, authorizations, and documentation managed in an appropriate recordkeeping system. The Ministry of Finance uses EDRMS as their appropriate system.

[1] Redundant source information destruction is covered under Step 5 of this process

Roles and Responsibilities

In the Ministry of Finance, all employees have information management responsibilities, including the appropriate destruction of information.[2] In addition, the overarching responsibility for the governance of information management[3] falls to the Deputy Minister and can be delegated. When delegated, it is the responsibility of the delegated positions to ensure the proper organizational structure as well as policies and procedures are put in place and enforced within their divisions and branches.

Destruction must be adequately documented in order to comply with the *Information Management Act*, which includes maintaining a record of destruction approval for the current calendar year plus 30 years.

There are various duties that must be completed which will depend on each branch's internal structure. However, for the most part the destruction process will not change at a branch level.

Location	Roles	Overview
Ministry of Finance	All Employees	**All employees have information management responsibilities as indicated in the Appropriate Use Policy:** • Be aware of and fulfill their IM/IT obligations • Employees must only dispose of government information in accordance with an approved information schedule.
Program Area	Preparer	Preparer is the Records Management Contact assigned by the program area • Possesses sound knowledge of the program's information, recordkeeping systems and relevant classifications. • Prepares adequate documentation pertaining to government information destructions. • Acquires approvals; arranges and carries out destruction actions.

[2] Appropriate Use Policy 1.4. Employees must only dispose of government information in accordance with an approved information schedule.

[3] See the Core Policy and Procedures Manual Chapter 12: Information Management and Information Technology Management and the Managing Government Information Policy for responsibilities

Program Area	Approver	Approver is the Executive Director or their delegated authority • Confirms that records are not required for operational requirements, related litigation, legal action, requests made under FOIPPA, or investigations that are underway or anticipated.
Corporate Services Division	Ministry Coordinator	Coordinator is the Ministry Information Management Officer • Provides governance, oversight, and administration of the Ministry Destruction Authorization Model • Provides the resources, tools, and forms for ministry program areas to adequately document destructions • Issues destruction control numbers and documents approvals and actions • Verifies the accuracy of destruction documentation. • Authorizes destruction request • Maintains the OPR 432-30 file for the mandated retention period • Liaises with IMB for data destruction and destruction within systems
Any Division	Information Mgmt Analyst, or equivalent Information Management professional	Can be contacted for assistance and guidance during the destruction process
Information Management Branch (IMB)	Lead for systems-related information management	Consultation with IMB is required for all system-related destruction, including migrations or system decommissioning.
Government Records Services, CITZ	Government Records Officer (GRO)	• Update status of records logged in EDRMS once confirmation of destruction received • Authorize destruction for migrated or digitized information with an approved disposition of SR or FR as required by the Redundant Source Information Schedule process. • Authorize destruction of information with an approved disposition of SR once the information has been assessed by an archivist.

See Appendix A: list of training requirements for the roles listed above

Destruction Procedure

Information Destruction Application (IDA) Steps	Roles
1. Request IDA destruction – initiate process by contacting the Ministry Coordinator	Preparer
2. Assign and log the IDA destruction number (IDA#) **3.** Open an OPR ARCS 432-30 file. **4.** If not already completed, provide necessary forms and instructions: o IDA form (ARS518) o RSIS digitization form (ARS667) for digitization o RSIS migration form (ARS668) for migration (under development) o File list template, if necessary or include an EDRMS file list o Tobacco Litigation Form D as required	Ministry Coordinator
5. Complete destruction form(s) and create file list. • Program Area retains an OPR file under ARCS 432-35. For Redundant Source Information (RSI) • for digitized information (category 4) o Ministry Coordinator provides form (ARS667) to document the requirements of a digitization project before approving destruction of redundant source records o If GRS consultation is required, the Ministry Coordinator will contact Government Records Officer (GRO) and consult with both GRS and the program area. • for migrated & converted information (category 3) o Collaborate with IMB contact to complete the IDA form (ARS518) o Complete an ARS668 Migration RSIS Form (under development) o If GRS consultation is required (e.g. final dispositions of SR or FR, or no approved information schedule), the Ministry Coordinator will contact Government Records Officer (GRO) and consult with both GRS and the program area. o Ministry migration process to be developed	Preparer IMB Contact
6. The Preparer will acquire program area approval to confirm the information: • is eligible for destruction • is no longer necessary for operational requirements (close triggers/SO are met)	Preparer Approver

• is not needed for any litigation, investigations, or FOIPPA requests that are underway or anticipated.	
7. Submit completed documentation capturing approvals to the Ministry Coordinator via the original email chain and include IDA# in email subject line.	Preparer
8. Review documentation for accuracy and completeness. If necessary, return documentation to Preparer for edits or clarification. Confirm the IDA contains appropriate schedules/classifications, and that IM practices and principles are present. • See ARCS or appropriate ORCS If accurate and complete, provide the administrative destruction approval. If either of the following applies, send to GRS@gov.bc.ca for final review and approval: • Seeking destruction authorization for digitized or migrated information with an approved disposition of SR or FR as required by the Redundant Source Information Schedule process. See the Redundant Source Information Schedule for whether an additional form is required. • Seeking destruction authorization for information with an approved disposition of SR in order to have it assessed by an archivist.	Ministry Coordinator
9. Send administrative approval to Preparer, and IMB contact, if relevant. File documentation under ARCS 432-30 and update the destruction log.	Ministry Coordinator
10. Complete destruction. IMB contact assisting with data destruction within systems and migration projects.	Preparer IMB Contact
11. Confirm destruction of records by email to the Ministry Coordinator. Preparer will CC GRS@gov.bc.ca. • Reply to original email chain and include a description of the method used to destroy the information and the actual date they were destroyed. • See RIMM Section 501A for approved methods of destruction ○ Records are considered destroyed when: ▪ They are put into a secure Shred-It bin	Preparer Ministry Coordinator

▪ They are shredded (by the employee or by a contracted company) as per RIMM Section 501A ▪ Otherwise destroyed as per RIMM Section 501A GRO team updates EDRMS status and replies all confirming completion. All parties file confirmation emails.	
12. Update tracking log, include date of destruction confirmation.	Ministry Coordinator

Commitment to Review

The Ministry Information Management Officer commits to completing a fiscal year-end review of the destruction program to evaluate the program's effectiveness and efficiency and to action adjustments to the model where necessary.

Approval of Information Destruction Authorization Model

Name	Title	Date
	Ministry Information Management Officer	
	Senior Data Architect, Lead for Information Management in Systems	
	Ministry Chief Information Officer	
	ADM, Corporate Services Division Information Management Ministry Lead (IMML)	

Appendix A: Resources

Training

Role-Based Learning

Ministry-specific training may be offered on an ad hoc basis

Forms

Information Destruction Log ARS

- For the Ministry Destruction Coordinator

ARS518 – Information Destruction Authorization (IDA) Form

- Required for all destruction applications

ARS661 – File List

- Required if there is no EDRMS-generated file list

ARS667 – Destruction after Digitization Authorization Form

- Required for the destruction of redundant source information after digitization

ARS668 – Migration RSIS Form (under development)

- Required for the destruction of redundant source information after migration or conversion

Form D – Tobacco Litigation Form

- Required to check for records that contain information potentially relevant to tobacco litigation.

Tools

Defensible Destruction Process Checklist

FIN Information Management Policies and Procedures Manual (to be updated)

Additional Information

Managing Government Information Policy (MGIP)

Defensible Information Destruction Part 1

- Establishing an Information Destruction Model
- For the Ministry Destruction Coordinator

Defensible Information Destruction Part 2

- Completing Destruction
- For any employees involved in the destruction process

Administrative Records Classification System (ARCS)

Operational Records Classification Systems (ORCS)

Special Schedules

- Executive Records
- Transitory Information
- Redundant Source Information

Digitization Resources

- Digitizing Government Information Standard
- Digitizing Government Information Guide
- How to Use the MFD to Digitize It Right

Project Name: CRMS Conversion to EDRMS Content Manager (EDRMS CM)

Office of the Premier

Last Updated: January 5, 2021

Purpose To transition approximately 4,000 CRMS records into EDRMS CM and manage change for approximately 4 staff.

Background CRMS manages physical records through their life cycle from creation to disposition. As EDRMS Content Manager (EDRMS CM) is the corporate application approved to manage both physical and electronic government records, Government Records Service (GRS) is now focusing on the migration of CRMS records to EDRMS CM. Office of the Premier (OOP) is one of many clients who will move forward in this transition. EDRMS CM is supported by Ministry of Citizens' Services staff in the Information Management Branch and GRS. GRS staff offer EDRMS CM e-learning, daily business helpdesk support of EDRMS CM use, and a variety of EDRMS CM on-line guides and other web resources.

Objectives

To migrate information about approximately 4000 records from CRMS from 3 CRMS ORG Units into EDRMS CM and reports from about 6 ORG units not migrating to EDRMS CM.

To support Office of the Premier staff in the use of EDRMS CM for the management of physical records through online EDRMS CM e-learning and EDRMS CM help desk for approximately 4 users.

To obtain information from the project to inform and support future CRMS to EDRMS CM migration projects.

In Scope

- Migration of Office of the Premier files metadata that are active, semi-active and destroyed/archived that is currently in CRMS into EDRMS CM for 3 ORG Units.
- Reports about data in CRMS not migrating to EDRMS CM for 6 ORG Units
- Configuration in EDRMS CM for physical folders
- eLearning resources for approximately 4 staff.

Out of Scope

- EDRMS CM for electronic records
- Information Management Assessment.
- Changes to the EDRMS CM systems architecture.
- Implement advanced EDRMS CM functionality (e.g., workflow).
- Integrate the use of EDRMS CM with current business applications.
- Any records in CRMS that are not currently in the list of ORG units in scope for this project. (see page 3).

Project Costs

The project will be completed using the existing staff resources of both the OOP and GRS. The cost of CITZ IMB contracted resource to convert CRMS data to EDRMS CM will be covered by GRS.

Work-plan Overview

Deliverable/Milestone	Targeted Completion
Project charter approved	January 6, 2021
Project Kick off meeting	January 6, 2021
Client provide EDRMS CM preferred structure	ASAP
Setting up of EDRMS CM Configuration, (meeting, document, & EDRMS CM work)	ASAP
Download of EDRMS CM software complete	January 29, 2021
User Profiles Forms complete	ASAP
Security Basics for Physical Folders	January 27, 2021
Data migration testing completed	January 13, 2021
User profiles created in EDRMS CM	January 27, 2021
EDRMS CM Training for 4 staff	January 29, 2021
Data conversion to production completed	January 17, 2021
Data Quality Control	January 22, 2021
Go-Live	January 29, 2021

Governance

Name/Project Role	Responsibility
Genevieve Elliott	Sponsor
Melanie Peterson	Project Lead
Sharon Larade	EDRMS Business Service Mgr
Lisa Barwise	Project Manager

Stakeholders

List any additional Stakeholders here.

Critical Success Factors

- Effective communications—will need to define audience and messaging
- Availability of sufficient and dedicated resources in the Ministry, IMB, and GRS to support the project
- Support for Information Workers to take the time necessary to use EDRMS CM for management of physical records
- Clearly defined and accepted project roles and responsibilities.
- Active engagement and participation by the Information Workers.
- Proactive communication and change management strategies delivered and applied by the Project Lead in collaboration with the project team.

Risks

- Lack of availability of dedicated resources. Any changes in availability or allocation of resources, and/or changes in GRS or business unit priorities will have a significant impact to the critical path.
- Reorganization activities. EDRMS CM is a corporate application. Any branch moved to a different ministry would still be supported.

.

Project Team

Name/Project Role		Responsibility
Project Sponsor **Genevieve Elliott**		Responsible for the project and promotes it. Reviews and approves project charter, including project scope. Acquires and ensures sufficient branch resources. Attends Project Kick-off meeting. Ensures major objectives are being met. Confirms access permissions meet branch requirements for privacy and security. Reviews and approves Security Basics Document Resolves issues arising from the project. Responsible for project communications.
Client Project Lead **Melanie Peterson**		Reports status, plans and issues to the sponsor as required. Works with GRS Project Lead and PM to manage issues, decisions, changes, and problems to resolution. Ensures user information forms are submitted to GRS to establish. EDRMS configuration and user profiles. Confirms which staff will be using EDRMS CM Confirms staff have completed EDRMS CM training. Attends EDRMS CM Security Basics meetings. Attends Project Status meetings. Assist with training materials design for off-siting and disposition training.
Client Program Staff		Complete online training sessions—for searching and identifying off-site locations, including accession numbers. For staff responsible for records transfer to off-site storage only attend EDRMS CM disposition training before completion of off-siting activities.
GRS Business Lead **Sharon Larade**		Manages business unit and external team relations. Confirms EDRMS CM configuration decisions with Client. Responsible for the delivery of the final product. Identifies required GRS resources. Approves Security Basics document. Ensures all project tasks and deliverables conform to quality management standards where they exist and are appropriate . Provide input into communications products. Create Security Basics documentation. Leads business unit post implementation reviews products.
GRS Sr. Records Management Application Analyst **Joanna Thompson**		Set up EDRMS CM structure (organizations, record types, access groups). Work with CITZ IMB to prepare data for conversion to EDRMS CM Test and EDRMS CM Production environments. Work with Client Project Lead and GRS Records Team to review test data and production data.

Project Team

Name/Project Role		Responsibility
GRS EDRMS HELP Team Lead **Pam McRae**		Assist Project Lead in determining the number of records to be converted by running reports by ORG Unit and Classification. Provides helpdesk support.
GRS Ministry Records Officer **Beverly Qualizza**		Liaison between GRS and Client. Works with the Client to determine the appropriate records structure to be used in EDRMS CM. Review test data and production data. Answers general records management questions. Provides classification assistance.
GRS EDRMS Access Analyst **Rhonda Campbell**		Create EDRMS CM user profiles based on authorized access forms completed by Client Project Lead.
GRS Project Manager **Lisa Barwise**		Plans and controls all project activities. Manages the project team. Communicates status and project information to GRS Business Lead and Client Project Lead. Assists Project Lead with reports to Sponsor, committees, and project stakeholders as required. Manages issues, decisions, changes, and problems to resolution.

Ministry Name	Org Unit ID	ORG Unit Name	Total Records	Confirmed Disposition Recommendation
Office of the Premier	IGRS	Intergovernmental Relations Secretariat	1164	Migrate Data to EDRMS
Office of the Premier	IGRS-OP	Intergovernmental Relations Secretariat - Office of Protocol	2576	Migrate Data to EDRMS
Office of the Premier	IGRSOPARCH	IGRS - Office of Protocol - Archives	366	Migrate Data to EDRMS
Office of the Premier	IGRSARCH	Intergovernmental Relations Secretariat - Archives	46	Export Data
Office of the Premier	IGRS MOGH	Intergovernmental Relations Secretariat - Min's Office	388	Export Data
Office of the Premier	IGRS MOJM	Intergovernmental Relations Secretariat Min's Office - J	13	Export Data
Office of the Premier	IGRS MOJV	Intergovernmental Relations Secretariat Min's Office -N	102	Export Data
Office of the Premier	IGRS MONY	Intergovernmental Relations Secretariat Min's Office -N	10	Export Data
Office of the Premier	IGRS MOSH	Intergovernmental Relations Secretariat Min's Office -S	42	Export Data

Sponsor Approval:
Genevieve Elliott

Approved ________________ Date: January 6, 2021 ____________________

Client Project Lead Approval
Melanie Peterson

Approved ____________________ Date: January 6, 2021 ____________________

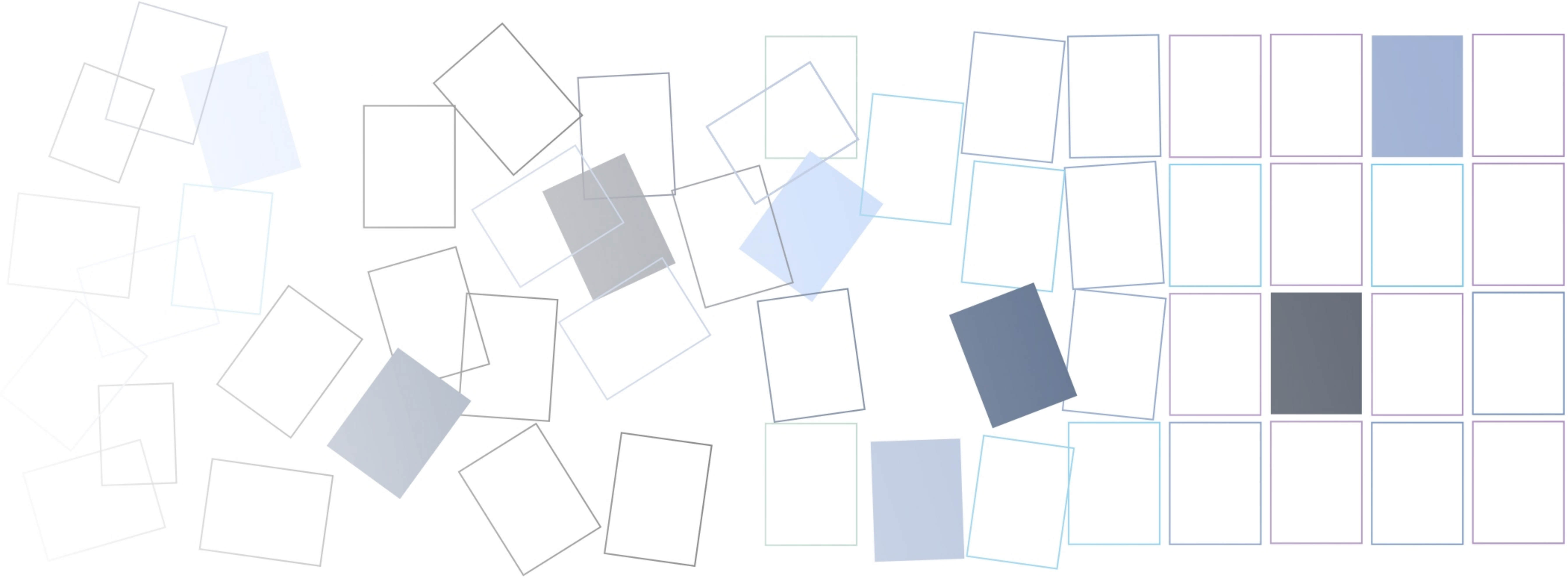
EDRMS Business Lead Approval
Sharon Larade

Approved ____________________________ Date: January 7, 2021 ____________________

Government Records Officer Approval
Beverly Qualizza

Approved ______________________________ Date: January 7, 2021 ____________________

Email *Guide*



At a Glance

Using your Email Account

Sending Email

Protecting Sensitive Information

Searching For Emails

Managing Your Email

Purpose

Email is a fundamental communication tool for BC Government employees. The sheer volume and diversity of the emails we create and receive on a daily basis means that managing them effectively can seem like an impossible task. This guide will help you navigate the world of email so it can be as effective a tool as possible.

Don't worry, good information management practices can help you manage your emails. Implementing simple information management procedures in your office will help you to wade through the swathes of emails and separate the valuable messages from the rest. Proper email management will not only make your life easier, it will ensure that important government information is available to meet business and legislative requirements. Your ministry or branch may have its own guidance on the management of email. This guide is intended to compliment that guidance.

This guide will help you to comply with the *Freedom of Information and Protection of Privacy Act (FOIPPA), the Information Management Act (IMA),* and the Appropriate Use Policy, including how to:

- understand security responsibilities surrounding email
- understand your responsibilities when using your email account
- determine what emails need to be kept
- keep those emails in ways that protect their authenticity and integrity
- determine what emails you can delete
- delete those emails appropriately using simple tools available in MS Office 2016 for Windows

Next: When do I have to use my email account?

Using your Email Account

When to use Government Email

When do I have to use a government-issued email account?

As an employee, you are required to use your government email when conducting government business (except in extenuating circumstances)

Not all government business requires the use of email — but when it does, you are required to use a government account. This includes when you are working outside the office, whether temporarily or as an external mobile worker.

Can I use my personal email account or an email account related to another organization for personal use while at work?

Per the Appropriate Use Policy, reasonable personal use of government-issued IT device by employees is permitted as long as you follow these rules:

- ▶ Your use of non-government email account on a government-issued device should be limited during work hours and must not interfere with your duties and responsibilities.
- ▶ Any use of personal email for personal use while at work must be lawful, must not compromise the security of government IT resources or government information, and must not be used for personal financial gain.
- ▶ The use of a government-issued computer, laptop, smartphone or other device must be consistent with the Standards of Conduct, whether that use is directly related to your employment duties or not.

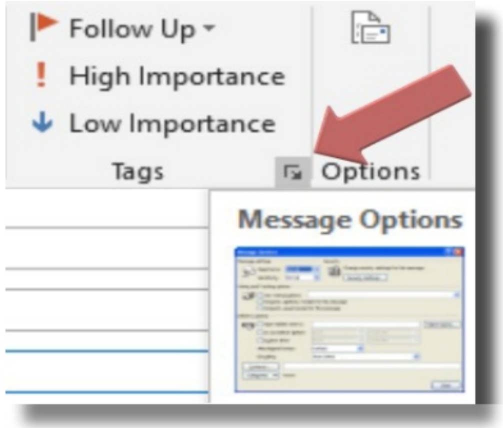
Next: Can I use my government email account for personal emails?

Using your Email Account

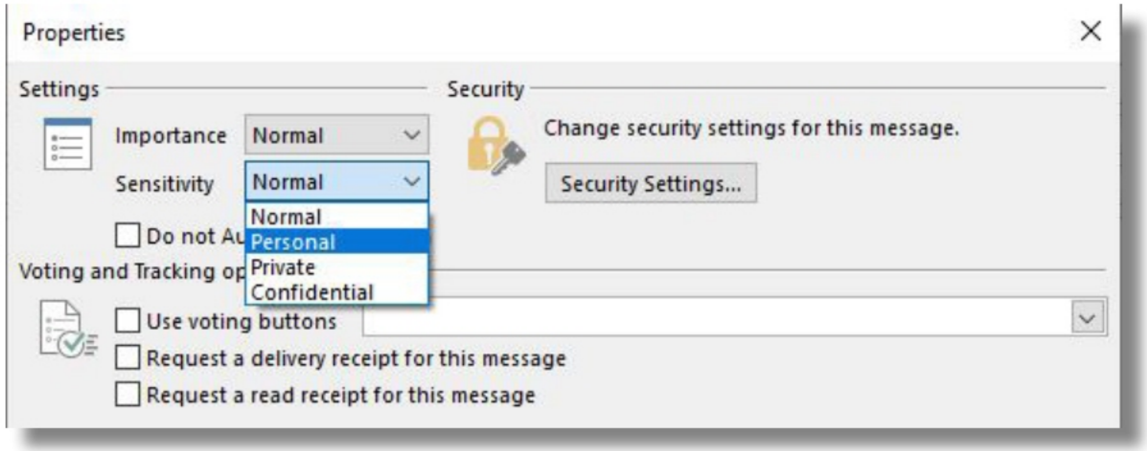
When to use Government Email

Consider using the features in your email system to mark emails as personal to easily distinguish them from government records. Do not mark government information as personal. To mark your emails as personal, use the categories feature as described below, or create a personal folder in your inbox. You can also mark an email as personal in the file properties in Outlook 2016 for Windows:

- ▶ When writing a personal email, click the small arrow to right of the word Tags to open Message Options.



- ▶ In the Message Options dialogue box under Settings, choose Sensitivity and select Personal from the dropdown list. Your recipient will then see your message marked as personal.



Properties

Settings

Importance: Normal

Sensitivity: Normal

Normal
Personal
Private
Confidential

□ Do not Au

Security

Change security settings for this message.

Security Settings...

Voting and Tracking op

□ Use voting buttons

□ Request a delivery receipt for this message

□ Request a read receipt for this message

Next: Accessing Email Outside the Workplace

Using your Email Account

Accessing Government Email Outside the Workplace

How can I access my email when working outside the workplace?

There are a number of ways you can securely access your email when working outside the workplace:

- ▶ using your government-issued smartphone, tablet, or laptop. For more guidance on the use of mobile devices, see the Mobile Device Guidelines for B.C. Public Service Employees;
- ▶ using a web browser (e.g. Internet Explorer, Chrome, Safari) to log onto the Outlook Web Access (a.k.a "Summer") at (https://summer.gov.bc.ca/).

If you are using the Outlook Web Access on public computer, select the option the says This is a public or shared computer. This will provide additional security by automatically logging you off after a short period of inactivity. Be sure to log off and close all browser windows to end your session.

You can also establish a secure remote connection to the government network, such as a Virtual Private Network (VPN) or Desktop Terminal Service (DTS). This also allows you to access files saved to your network drives. For instructions, please read the Remote Access Services User Guide.

Next: Protecting Email Outside the Workplace

Using your Email Account

Protecting Government Email Outside the Workplace

Viewing your email remotely using the Outlook Web App (i.e. https://summer.gov.bc.ca) on a non-government-issued device is sometimes necessary. However, using a personal or public device means that you need to take extra precautions to ensure that sensitive government information is secure. When using a personal or public device:

- do not open, download, or save any attachments which may contain confidential information; and
- be aware of your surroundings and prevent others from viewing confidential information that may be contained in the body of the email.

For more information on the types of information that may be considered confidential, see the BC Government Information Security Policy.

It may also be necessary to use a secure remote connection like VPN or DTS. When using VPN or DTS:

- do not download or save attachments to the local hard drive of a non-government device as the files may contain confidential information; and
- do not print any emails, attachments, or other documents when using remote access tools (unless you are printing to a printer on the government network).

Only in rare, extenuating circumstances is it permissible for you not to follow these requirements. In such cases, however, you must follow the rules set out in the Appropriate Use Policy.

Next: Can I ever use my personal email account for work purposes?

Using your Email Account

Use of Personal Email Accounts

Can I ever use my personal email account for work purposes?

The Appropriate Use Policy states that only in rare, extenuating circumstances are you permitted to use a non-government email account for government business. It must be absolutely necessary to do so. For example, you may not forward work emails or documents to your non-government email account simply to work on them at home or to create a convenience copy.

In extenuating circumstances where you are unable to securely access your government email account via the three methods outlined previously, you must always follow these steps:

- ▶ Send or receive the least amount of confidential information necessary to deal with the extenuating circumstance until you are able to use government email again.
- ▶ Send a copy of the email to your government email account. It is recommended at this step to note the circumstances that prevented you from accessing your government email account.
- ▶ Delete the email from the inbox, sent items and trash of your non-government email account as soon as possible. You should also send an email note to your government email account noting that you have deleted the government record(s) from your personal email account, and have not made any copies of the information.
- ▶ Resume use of government email as soon as possible, including using government email for the remainder of an interaction that began via personal email.

You must exercise additional caution if the email you need to send or receive contains personal information. Most email account providers – such as Gmail or Hotmail – store your emails outside of Canada and the *Freedom of Information and Protection of Privacy Act* prohibits personal information held by the government from being accessed or stored outside of Canada, except in limited circumstances.

Next: Tips for Sending Email

Sending Email

Tips for Sending Email

- ▶ Keep email to a single topic. If the topic changes, create a new email thread. If the email covers two or more topics, consider filing it in two places.
- ▶ Be specific in the subject line. Create a clear and descriptive title. Use the subject line to indicate actions, purpose and due dates.
- ▶ Use your signature block for all outgoing email messages going to recipients outside your working group. If your email contains important decisions or actions, always include your signature block. See example below.
- ▶ Limit the number of recipients. Only include recipients who are expected to take action or make a decision on a topic. Use the 'cc' option when sending messages to recipients for informational purposes.
- ▶ Limit the use of attachments and graphics. Whenever possible, post your document to a shared location (e.g. on EDRMS Content Manager, SharePoint, shared drives/LAN) and send a link in the email.

Descriptive subject lines are important for managing emails and are helpful aids for determining whether you need to save an email or if you can delete it. Some recommended descriptive subject lines are:

- Action by <date>
- Follow Up:
- Question:
- Answer:
- Request:
- As Requested:
- As Promised:
- Thank You!
- For Information:
- FYI:
- Work/Life:

Use signature blocks for all outgoing email messages. Signature blocks may contain:

- Sender's name
- Sender's title
- Branch or Office
- Telephone number
- Postal address

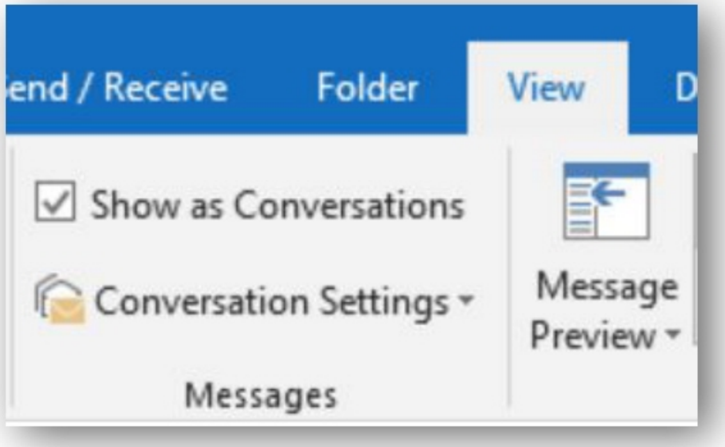
Example:
Jane Doe
Project Manager | Office of the Premier
250-XXX-XXXX | PO Box 9568, Stn Prov Gov,
Victoria BC V8W 9K1

Next: Tips for Managing Email Discussion Threads

Sending Email

Tips for Managing Email Discussion Threads

- ▶ Do not forward unnecessary information from previous emails to new recipients. Before you include another person on the thread, delete any information that is not needed for completing the task at hand. Avoid unnecessary duplication.
- ▶ It is recommended that the person who initiates the email thread be responsible for ensuring the thread gets filed. Recipients may also save emails, depending on the content and context of the message.
- ▶ Use the conversation clean-up tool with caution. When a conversation has split into separate conversations, the system may delete intermediary emails that are older than the final email in the collection. Be sure to assess and mark important decision emails prior to running the tool.
- ▶ Don't share personal information unless it is necessary for completing the job at hand. Keep personal information on a need-to-know basis. Share only the right information with the right person for the right purpose.
- ▶ Set your Outlook to 'Show as Conversation'.



☑ Show as Conversations
Conversation Settings

Next: Protecting Sensitive Information

Protecting Sensitive Information

Protecting Sensitive Information

How can I protect government information when sending emails?

You are responsible for ensuring that any confidential government information you are working with is protected. Given the ease with which email messages can be distributed and accessed by others, you need to take extra precautions when working with confidential information.

Limit the amount of confidential information transmitted over email. Use your best judgment or, if you are uncertain, check with your supervisor. Avoid using email to send confidential, sensitive, protected or secret information, except where there is a specific business requirement to do so.

Emails sent outside of the government network, such as to external contractors or service providers, may be less secure. Consider encrypting documents containing confidential information before sending, and provide the password to recipients using separate means (e.g. verbally, via Skype IM). Keep a record of the encryption key, and ensure that any encrypted messages are decrypted before filing them in the appropriate recordkeeping system. Certain documents (e.g. draft legislation) must never be included in an email.

For more information see the Information Security Policy. For further guidance on sending confidential documents over email and when to use encryption, see the BC government Digital Certificate Service or contact your Ministry Information Security Officer.

Next: Can I send personal information over government email?

Protecting Sensitive Information

Protecting Sensitive Information

Can I send personal information over government email? Are there additional privacy concerns I should be aware of?

The collection, use, disclosure, access, and storage of personal information via email must comply with the *Freedom of Information and Protection of Privacy Act* (FOIPPA). **Limit the personal information** you transmit over email, and always following the **"need-to-know" principle.** Specifically, any personal information about another person that you share in an email should be the minimum amount necessary to perform your duties. For example, when forwarding a request or question from the public, you may need to remove any personal identifiers that are not needed by your recipient. Be aware of who is on your recipient list and, if sending an email to a contractor or to an external organization, ensure personal information is not accessed or stored outside of Canada in a manner that contravenes FOIPPA. For example, sending an email containing personal information to someone outside of the government network may not be authorized under FOIPPA.

You should not send personal information over email to the public, unless the personal information is about an individual who has contacted you and you are using that same method of communication, or another method of communication authorized by that individual. For example, if a person emails asking you a question about their benefit, you are authorized under FOIPPA to respond to that person's email.

In this circumstance, take reasonable steps to confirm the identity of the person requesting the information before sending anything personal by email.

Some ministries have additional restrictions around sending personal information over email. Contact your Ministry Privacy Officer as a point of contact for ministry-specific email policy and questions to support a determination if a contractor/service provider's email is appropriate to send/receive personal information.

Next: What are "Information Incidents"?

Protecting Sensitive Information

Protecting Sensitive Information

What are "information incidents"? What should I do if one occurs?

An information incident is the collection, use, disclosure, access, disposal, or storage of information, whether accidental or deliberate, that contravenes law or policy. When personal information is involved, it is referred to as a privacy breach. You must report any actual or suspected information incidents immediately by following the Information Incident Management Process. You are required to report the incident to your supervisor and then call 250-387-7000 (1-866-660-0811) and select Option 3.

In the case of email, information incidents may include:

- you have sent a message containing personal or other confidential information to the wrong person who does not have authorization to access it; or
- you have lost a mobile device (e.g. smartphone, tablet, or laptop) which has access to your government email account.
- the security of your workstation or computer has been infected by malware or otherwise compromised;
- a personal or IDIR credential has been disclosed or used without your approval

Next: How can I prevent information incidents from happening?

Protecting Sensitive Information

Protecting Sensitive Information

How can I prevent information incidents from happening?

As a general principle, manage all confidential information on a "need-to-know" basis. Share only the **right information** with the **right person** for the **right purpose** at the **right time** and in the **right way.**

Take precautions to prevent others from accessing your email account. The appropriate use policy states that you must never share your IDIR password with anyone, including technical support or an administrative assistant.

If you need to share your email or calendar with someone else, use the delegation features available in specific applications (e.g. Microsoft Outlook).

You also need to be on the lookout for, and guard against, phishing attacks: unsolicited emails asking you to click on a link, open a document, or verify your personal information or account credentials. If an email looks suspicious, it is likely illegitimate and should be treated with caution, even if it appears to come from an official government source.

Next: Searching for Email

Searching For Email

Searching for Emails

This section will guide you through your obligations under *Freedom of Information and Protection of Privacy Act (*FOIPPA*)*. It will show you how to use the advanced find to help you search for emails.

Under FOIPPA, the public has a right to access government records. When you receive a call for records in response to an FOI request, you are required to conduct a thorough and comprehensive search for responsive records. This includes records stored in your email account.

When an FOI request is made, you must conduct a thorough search for related emails and produce them for processing as part of the response to the request. Transitory information in your account that fits within the parameters of the request must be included in any search for records. Remember that once you have received an FOI request, you must retain all records subject to the request, including transitory emails, until the request has been closed.

Cached Exchange Mode

Outlook search restricts results to 250 emails from the exchange server (online) and all cached emails (offline). If you use search often, particularly for older emails, caching the entire mailbox is recommended.

To do this click File, then Account Settings, and double click on your email address. Drag the slider all the way to the right to All. This ensures that all email in your account will be available offline.

To see all results, it may also be necessary to turn off the 'Improve search speed' function. To do this, click File, then Options. Under the Search tab, uncheck the box that says Improve search speed by limiting the number of results shown.

Next: Responding to FOI Requests

Searching For Email

Responding to FOI Requests

When there is a request for records, your FOI Coordinator will guide you through the scope of the request. The scope of the request will depend on the nature of the request and guidance will be on a case-by-case basis.

Requests under FOIPPA are often expressed in relation to a particular subject. You must provide all emails in your possession that are relevant to the request. Search all locations where emails can reasonably be expected to reside (i.e. Sent Items, Deleted Items, .PST Files, etc.).

When searching for emails, you can first use subject-based search terms used in the request. You should use your best judgment when searching for emails and expand the scope of your search as necessary.

Use the Advanced Find feature to conduct the search.

For more information on conducting a search, contact your FOI Coordinator.

Next: Search Tips

Searching For Email

Search Tips

▶ **Search using Microsoft Outlook on your government computer**

Using your mobile device (e.g. your cell phone) to conduct the search will not yield the correct results, as not all email records will be available on a mobile device.

▶ **Search shared mailboxes and the mailboxes of departed employees**

You are required to search all locations where responsive emails might be found. If you are responsible for the records of your working groups or the records of departed employees, you are required to search them in response to a request.

▶ **Be specific in your search**

Using broad search terms may result in hundreds of results. Your search may be truncated when the number of results gets too high. This may cause relevant records to be missed. It might be necessary to refine search terms to narrow the results.

▶ **Search your PST files**

You are required to search through all your email folders and files where the records can reasonably be expected to reside. This includes all email .PST files.

Next: Search Tips (Continued)

Searching For Email

Search Tips (continued)

▶ **Inspect all email threads**

The subject line text may have been an accurate description for the first message, but may not reflect the scope of the subject matter as the thread developed. Review all email records in any thread that may be relevant to the request. Determine which emails accurately represent the exchange and provide a complete thread.

▶ **Include all attachments**

Provide all responsive emails with attachments to your FOI Coordinator. On occasion, a request may specifically exclude email attachments. Please pay close attention to the scope of the request.

▶ **Search for emails sent to groups**

You must ensure that the record shows who sent and received each message and when, as well as who received a copy (since the header data will differ on each copy of the message). If a message is sent to a group or list, include information about the list.

▶ **Record your search terms**

Provide a description detailing what records were searched and who conducted the search. This description should list all potential sources of emails that have been searched, as well as individuals or program areas that have been canvassed. While it is not necessary to include all search terms, any other relevant information about the search should also be included in the description.

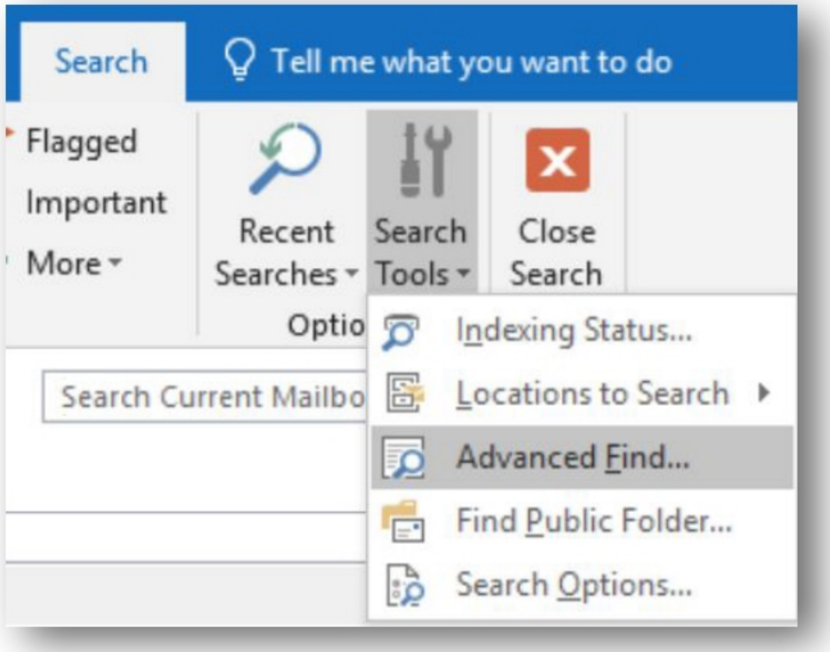
Next: Advanced Find

Searching For Email

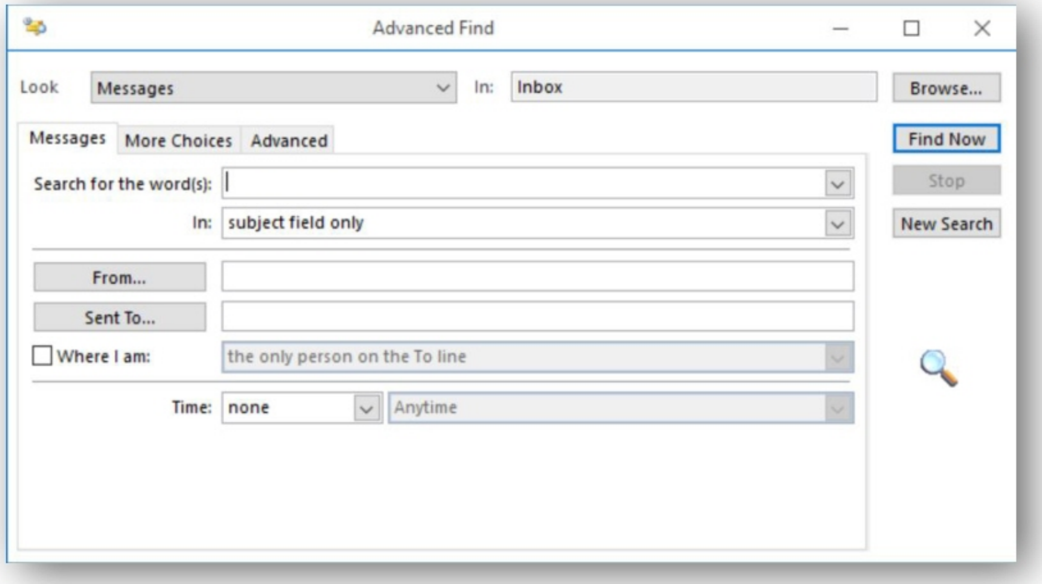
Advanced Find

To locate the Advanced Find option:

- ▶ Click the search bar above your email list to open the Search Tools tab in the Quick Access Toolbar.
- ▶ Click the Search Tools button to open the dropdown menu.



- ▶ Select Advanced Find from the dropdown menu. This will open the Advanced Search pop-out window. This window provides you with a large selection of options for narrowing your search.



Look: Messages In: Inbox

Search for the word(s):

In: subject field only

□ Where I am: the only person on the To line

Time: none Anytime

Searching For Email

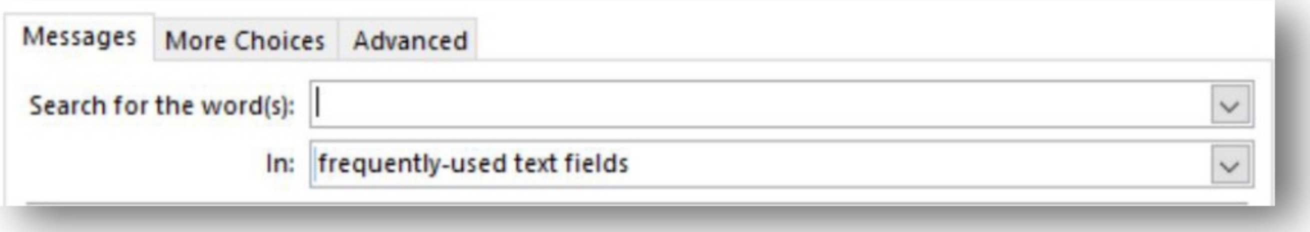
Advanced Find

▶ Search for multiple keywords in separate searches

The Search for Word(s) feature in Advanced Find is very specific and will only return emails that contain the exact wording you enter. Therefore you must conduct multiple searches for all the keywords that may be relevant to the request.

▶ Search in Frequently-used text fields

In Advanced Find, the default is set to search the subject field only. However, the keywords you are looking for may be in the message body or attachments. To search all frequently-used text fields, click the arrow to open the dropdown menu and select this setting.

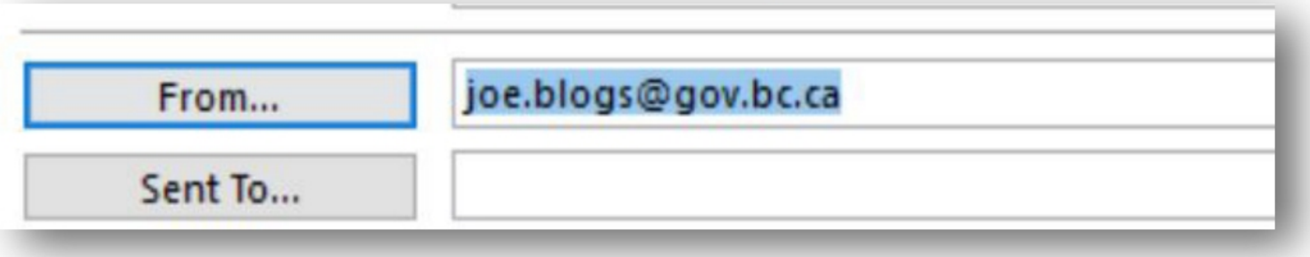


Search for the word(s):

In: frequently-used text fields

▶ Search for message sent or received from specific accounts

To search for messages sent or received from specific email accounts, open Advanced Find and select the From... or Sent To... options.

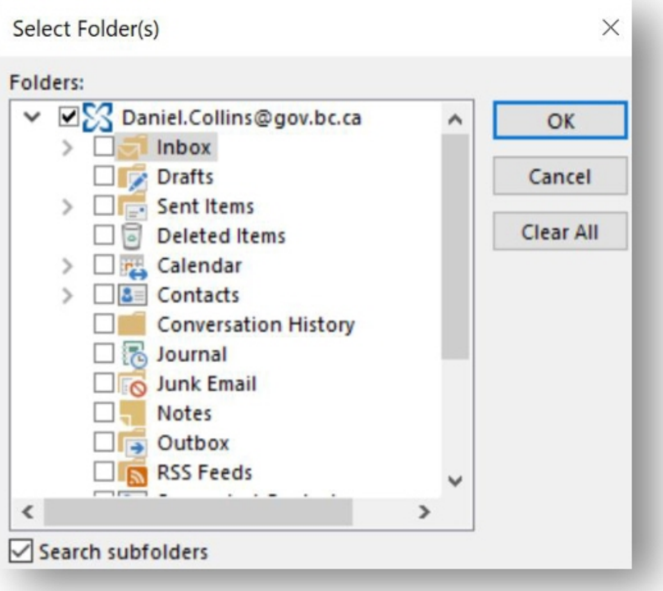


From... joe.blogs@gov.bc.ca

Advanced Find

▶ Search all folders in your account

To search all folders click 'Browse...' in the pop-out window, check the box beside your email address. Also check the box that says 'Search subfolders'.



Select Folder(s)

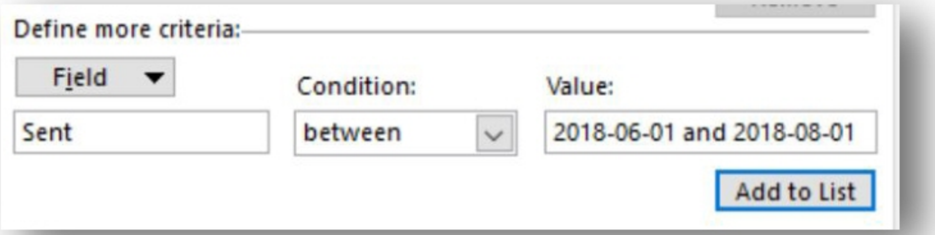
Folders:

- ☑ Daniel.Collins@gov.bc.ca
  - □ Inbox
  - □ Drafts
  - □ Sent Items
  - □ Deleted Items
  - □ Calendar
  - □ Contacts
  - □ Conversation History
  - □ Journal
  - □ Junk Email
  - □ Notes
  - □ Outbox
  - □ RSS Feeds

☑ Search subfolders

▶ Set date parameters

The request may be specific to a certain time period. You can set date parameters by opening Advanced Find and selecting the Advanced Tab. Under Define more criteria, click Field and in All Mail fields select Sent. Under Condition: select Between. Then in the Value: box, type in your date criteria in the form 'YYYY-MM-DD and YYYY-MM-DD'. Click Add to List and Find Now.



Define more criteria:

Field	Condition:	Value:
Sent	between	2018-06-01 and 2018-08-01

You can combine any number of these criteria to narrow your search, making the Advanced Find a particularly powerful tool, especially when used in conjunction with well defined categories. See the section on Managing your Emails for more information on categories.

Next: Government Emails are Government Records

Managing your Email

Government Emails are Government Records

Emails pertaining to the business of government are considered government information and, as such, must be preserved for a set time period or kept permanently. Information schedules approved under the *Information Management Act* (IMA), provide classifications and timelines for managing all government information. Emails should only be deleted or disposed of in accordance with approved information schedules and should not be subject to periodic and indiscriminate deletions.

As an employee, you are responsible for filing emails that document government activities and decisions in the appropriate recordkeeping system (e.g. an EDRMS, a case management system, or a LAN organized according to ARCS and ORCS).

Remember that your email account is a communications tool, not a place to manage records. For more information on where to file emails, see the section on Saving Emails Outside of Outlook.

Next: Deciding what To Keep or Delete

Managing your Email

Deciding what to Keep or Delete

Do I need to keep every email? When can I delete an email?

You need to save all emails that pertain to the business of government, except for transitory emails. Transitory emails contain information of temporary usefulness that is needed only for a limited time, to complete a routine action or prepare a subsequent record. You may delete transitory emails when they are no longer needed.

You must not delete any emails which may be responsive to an active FOI request or request for legal discovery.

You should save emails that document an important government decision. For more information on the duty to document government decisions see the Guidelines on Documenting Government Decisions.

Save Official Email Records

Delete Transitory Emails

Next: Examples

Examples of **official email records** include:

- ▶ emails that document business transactions (initiation, authorization, or completion)
- ▶ emails that document decisions, including instructions, approvals, advice, and signed briefing notes
- ▶ emails that document a policy decision, significant action, or how a case was managed
- ▶ formal communication about government business
- ▶ emails that contain information that is integral to a file about one event, client, or issue (e.g. a case file)
- ▶ legal advice and agreements
- ▶ unread email that is evidence of attempted consultation
- ▶ emails that contain other information that helps explain the history of a relationship, decision or project

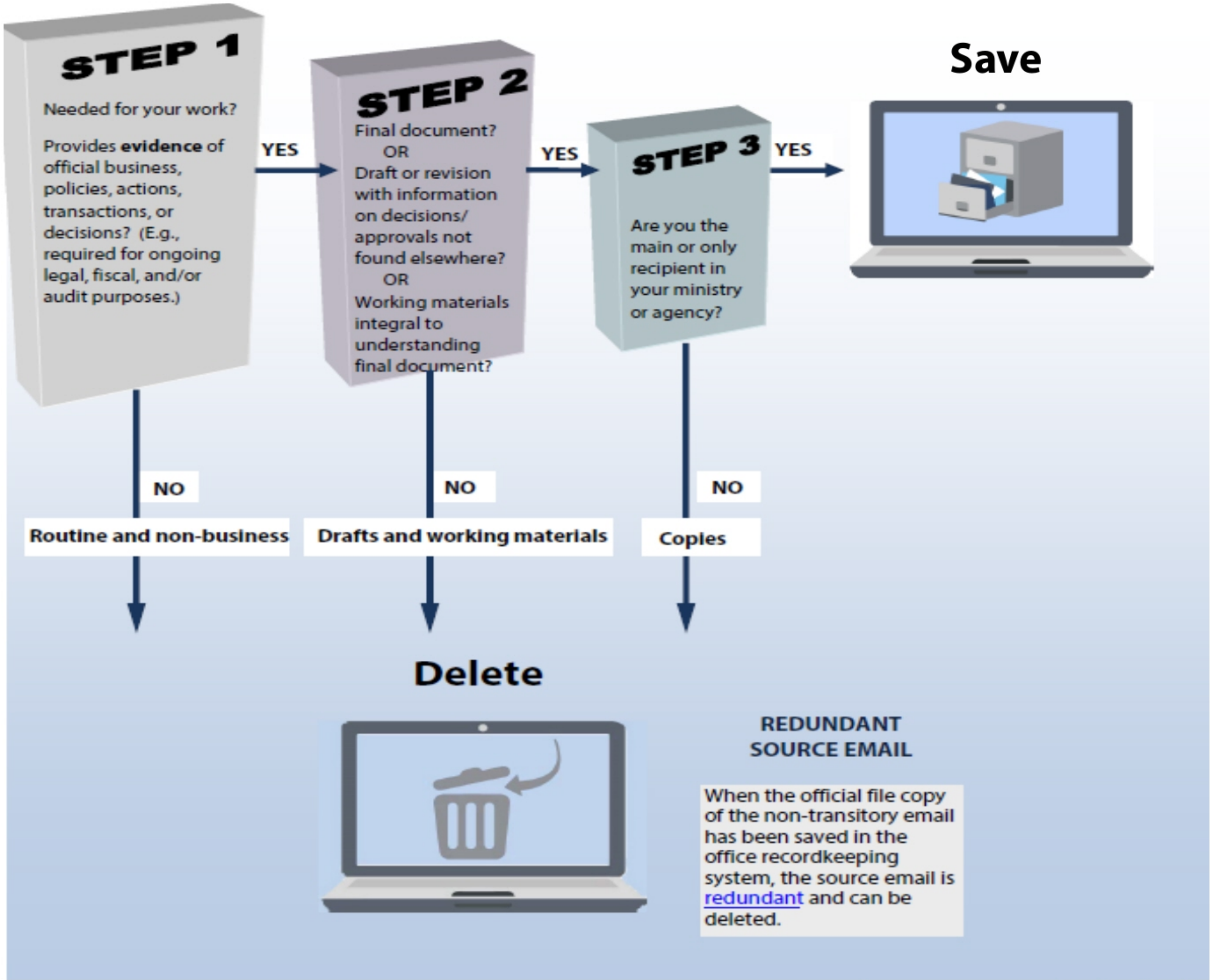
Examples of **transitory email records** include:

- ▶ announcements of social events
- ▶ cc copies (unless you are the main staff member responsible for the matter)
- ▶ emails conveying an attachment (if it doesn't add value to the attachment)
- ▶ meeting arrangements
- ▶ routine correspondence about drafts and revisions
- ▶ a request to call someone
- ▶ personal emails such as lunch/coffee arrangements and birthday wishes

Next: Email Decision Diagram

Managing your Email

Decision Diagram - Save or Delete?



STEP 1

Needed for your work?

Provides **evidence** of official business, policies, actions, transactions, or decisions? (E.g., required for ongoing legal, fiscal, and/or audit purposes.)

STEP 2

Final document?
OR
Draft or revision with information on decisions/ approvals not found elsewhere?
OR
Working materials integral to understanding final document?

STEP 3

Are you the main or only recipient in your ministry or agency?

YES

YES

YES

Save

NO

Routine and non-business

NO

Drafts and working materials

NO

Copies

Delete

REDUNDANT SOURCE EMAIL

When the official file copy of the non-transitory email has been saved in the office recordkeeping system, the source email is redundant and can be deleted.

Next: Organizing Email in Outlook

Managing your Email

Organizing Email in Outlook

My Inbox is a mess! How can I manage all my emails?

Organizing your email inbox is fundamental for proper email management. An unruly inbox will seem daunting to many. Aim to identify and act on emails as soon as they arrive in your inbox.

This section will guide you through a number of useful tools you can use to organize and classify your emails in Outlook 2016 for Windows (some of these features may not be available for other versions of Outlook). Tools include:

- ▶ Folders
- ▶ Categories
- ▶ Rules

Next: Working with Folders

Managing your Email

Working with Folders

It's useful to think about email in the context of the paper environment. In the pre-internet era, messages would arrive to your office inbox in paper form. They wouldn't just live in your inbox; you would read the messages then either file them away or dispose of them. The inbox was a temporary storage location, not a final destination. The same is true of your Outlook inbox today.

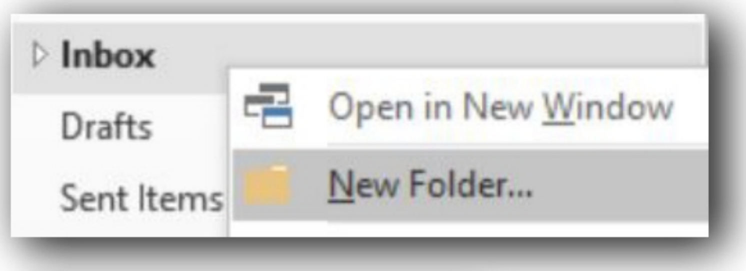
As a rule, government employees should file or delete their email as soon as possible after sending or receiving them. However, this isn't always possible or desirable. Creating custom folders in Outlook to organize your inbox will help you file and delete emails in a timely manner.

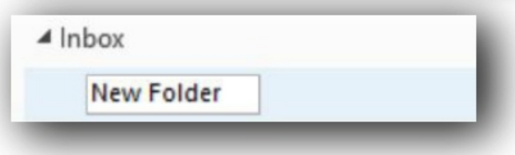
It is recommended that you create subfolders according to predefined classifications laid out in government information schedules (i.e. *ARCS* and *ORCS*). Use the file code (*ARCS* and *ORCS* primary and secondary numbers) in the subfolder name. Create a subfolder for each project you are working on or create a subject-based subfolder. Create as many subfolders as you need.

It is also good practice to create a transitory email folder for items that are of temporary usefulness. You can apply rules to the transitory folder to delete transitory emails after a specified period has elapsed. See the section on Deleting Emails Appropriately.

To create a new folder:

- Right-click the Inbox folder in the navigation pane and choose New Folder. Type the new folder name and press Enter.
- Drag-and-drop messages from your Inbox into the new folder in the navigation pane.





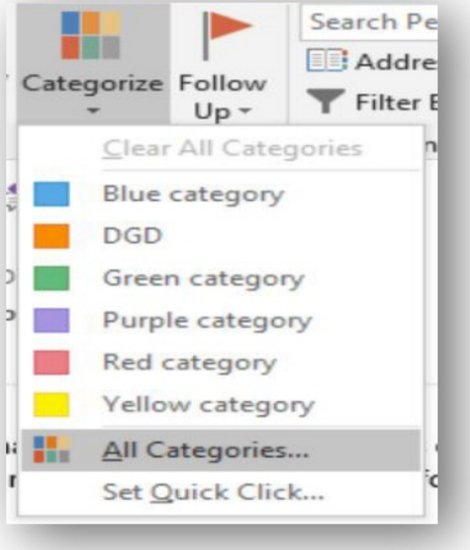
Next: Working with Categories

Managing your Email

Working with Categories

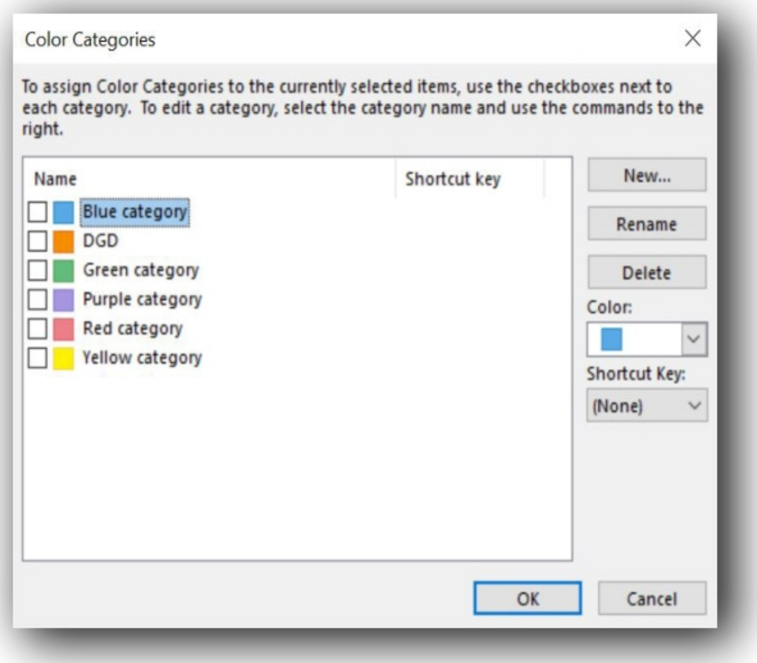
Colour Categories in Outlook are another useful way of organizing your inbox. Not only do colour categories allow you to visually identify your emails at a glance, but you can use them to perform quick sorts, populate search folders and much more.

Outlook has a number of default categories which have been named according to their colour.



To create and assign categories:

- ▶ Click the Categorize button in the upper ribbon to open the list of categories.
- ▶ At the bottom of the drop-down list, choose the option to view all categories. In this pane you can add or delete categories or rename them according to your preference. Choose categories that work for you. You can also create a shortcut key to quickly assign categories to email.
- ▶ Go back to your inbox, click on the email to highlight it, then click on the categorize button again to select the category from your list (right clicking on the email also brings up the Categorize option).


Color Categories

To assign Color Categories to the currently selected items, use the checkboxes next to each category. To edit a category, select the category name and use the commands to the right.

Name	Shortcut key
□ 🟦 Blue category	
□ 🟧 DGD	
□ 🟩 Green category	
□ 🟪 Purple category	
□ 🟥 Red category	
□ 🟨 Yellow category	

Color: 🟦
Shortcut Key: (None)

Next: Working with Rules

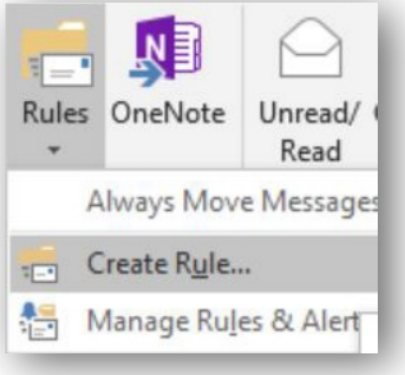
Managing your Email

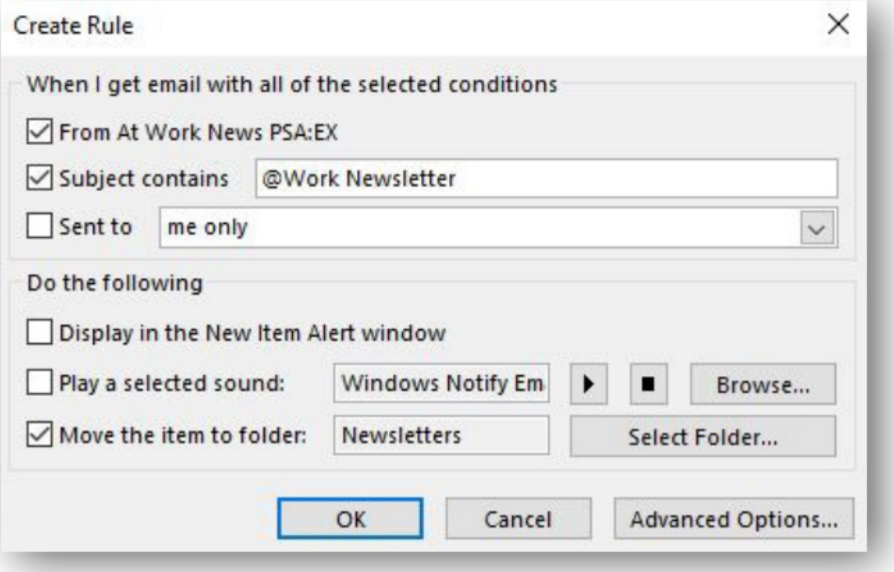
Working with Rules

Rules can be useful for automatically sending email to a specified folder. If there are specific people, subjects, categories, or topics that will always go in the same folder, you should set up a rule that automatically routes those emails to that folder.

To set rules:

- ▶ Click on the Rules button in the upper panel to open the drop-down menu.
- ▶ Select Manage Rules and Alerts.
- ▶ In the Rules tab, select Create Rule. This will allow you to choose from a number of rule templates that you can customize, or you can create your own rules from scratch using the Advanced Options.




Create Rule

When I get email with all of the selected conditions

☑ From At Work News PSA:EX

☑ Subject contains: @Work Newsletter

☐ Sent to: me only

Do the following

☐ Display in the New Item Alert window

☐ Play a selected sound: Windows Notify Em

☑ Move the item to folder: Newsletters

Next: Saving Email Records Outside Outlook

Managing your Email

Saving Email Records Outside Outlook

A recordkeeping system is a shared filing system in which records, including government emails, are captured, protected, retained and destroyed in accordance with approved information schedules. A recordkeeping system, when used in conjunction with recorded policies and procedures, defined roles and responsibilities, and on-going training, constitutes an appropriate system for managing government information.

An appropriate recordkeeping system should:

- contain logical, organized naming conventions that can be followed by all staff;
- ensure the preservation and accessibility of records over time;
- protect against accidental or unauthorized access, alteration, copying, movement or deletion;
- minimize duplicate storage of records; and
- permit the retention requirements of information schedules to be applied accurately and efficiently.

This section will provide guidance on how to save emails to your office's recordkeeping system. It will walk you through:

- **Saving Email - Responsibilities**
- **Tips for Saving Email Records**
- **Preferred Email Preservation Formats**
- **Locations for Saving Emails**

Next: Saving Email - Responsibilities

Managing your Email

Saving Email - Responsibilities

▶ Managing email is the responsibility of every employee

It is the responsibility of all staff to manage their emails appropriately. You should identify emails that are records of your business activity, move them from your Outlook mailbox, and manage them alongside related records in your office's recordkeeping system.

▶ The email sender is responsible for saving internal email

It is the responsibility of the sender of an email or the initiator of a dialogue to decide if the email and/or attachment(s) constitute an official record. If the email or its attachment(s) contain key decisions and/or actions taken, it should be considered a record, renamed (if appropriate), and saved in the most appropriate place.

▶ The principal receiver is responsible for saving external email

If you are the sole recipient of an external email or, if there are several recipients, and you are responsible for the most relevant work area, you are responsible for deciding if the message forms part of an official record or not and taking responsibility for its management.

▶ Working groups should assign responsibility for shared mailboxes

When managing emails in a shared mailbox, working groups should be clear as to who is responsible for the retention, naming, capture and disposal of emails within the mailbox. Without the identification of clear responsibilities, emails may be lost or duplicated. It is recommended that the folder owner take responsibility for a shared mailbox.

Next: Tips for Saving Email Records

Managing your Email

Tips for Saving Email Records

A complete record includes sufficient content, context, and structure to ensure that the information can be accessed, understood, and preserved for as long as necessary, and that its value as evidence will be maintained. To do this, you need to preserve all elements of the email, including the **email header**, the **message body**, and any **attachments.**

- To prevent a loss of information, move emails to an appropriate location as soon as possible.
- It is not necessary to capture every email in an email conversation thread separately. Instead emails should be captured at key points during the conversation, when key decisions are made and transactions processed.
- Email attachments should be saved as part of the record to provide context to an email. However, there will be occasions when it won't be necessary to capture both the email and its attachment. For example, if an attachment has been sent for reference purposes and you know it has been captured elsewhere.
- If the title of the email does not accurately reflect the content of the message then it should be re-titled at the point at which it is saved. Renaming email records is particularly important when they represent different points in an email string as it will identify the relevant aspects of the conversation.
- Consider dating the email in the title before saving it. For government bodies who receive a high volume of requests under *FOIPPA*, the ability to sort by date is particularly important. Use the format YYYY-MM-DD to date your emails in the title.

Next: Preferred Email Preservation Formats

Managing your Email

Preferred Email Preservation Formats

For filing on the LAN/Shared Drive/EDRMS: .MSG

MSG files are the native Outlook format. When you drag and drop an email to your desktop or to a LAN folder, this is the file format that is exported. Outlook can export calendar items, emails, contacts, and other Outlook content via MSG. This format is preferred because all header information, message content and attachments are preserved with the file. The file will retain a lot of its original functionality when reopened.

Next: PDF

Managing your Email

Preferred Email Preservation Formats

For filing anywhere (ideal for long-term storage): .PDF

Emails can be exported from Outlook by printing them to a standard PDF file or a PDF portfolio. PDF files are stable and generally well supported, making them the de facto preservation standard for documents. The Adobe PDF conversion plug-in is available when you download Adobe Acrobat. This allows for one-click conversion of Outlook content to PDF.

You can also save attachments embedded in a PDF, just like an email; however, this method can cause compatibility issues. Best practice is to download the attachment and save it with the email content to ensure it can be opened in the future.

PDF Portfolios

PDF portfolios contain multiple files assembled into an integrated PDF unit. The files in a PDF portfolio can be in a wide range of file types. You can open, read, edit and format each component file independently. You can also append new emails to existing portfolios.

To create a PDF portfolio use the Adobe Acrobat PDF plug-in for Outlook. You can combine multiple emails, attachments and calendar items into a single file. This is particularly helpful when saving project folders to your chosen recordkeeping system.

Next: Avoid PST Files

Managing your Email

Avoid PST Files

.PST

PST files contain batches of Outlook content including emails, calendar events, tasks, etc. Folders, inboxes or entire mailboxes can be exported from Outlook in this format. PST files are not recommended for preservation purposes because they handle poorly in LANs, are easily corruptible, cannot be searched in EDRMS environments, and cannot be scanned for viruses.

When the Outlook Auto-Archive function runs on your machine, it removes specified emails from your Outlook mailbox and sends them in the form of a PST file to a location on your LAN. This practice is not recommended. The BC Government discourages the creation and use of PST files for email preservation.

Next: Your Office Recordkeeping System

Managing your Email

Your Recordkeeping System

Government bodies need to create and keep complete and accurate records sufficient to document their decision-making and work activities and this is particularly true of email records. Storing your emails in a central recordkeeping system ensures that records are preserved and available to staff, minimizes duplication, and enables the retention requirements of information schedules to be applied effectively.

Appropriate recordkeeping systems for managing emails include:

- **EDRMS Content Manager:** A comprehensive recordkeeping system with a full range of records management tools including a classification table with linked information schedules (ARCS and ORCS), and sophisticated search and retrieval functions. EDRMS Content Manager enables integrated management of both physical and electronic records and is the approved government standard.
- **LAN (Local Area Network) and shared drives:** These can be organized and administered in accordance with ARCS and ORCS. This method is viable for limited volumes and types of electronic records. Shared drives do not have the records management functionality of an EDRMS and is suitable as an interim approach pending adoption of a fully functional recordkeeping system (i.e., EDRMS Content Manager).
- **Line of business applications** (e.g. case management systems): Many line of business applications are purpose-built for managing information relating to a particular case or project. These may be appropriate for managing emails and for keeping case-related records together. However, these systems often lack the full range of records management tools of a dedicated EDRMS and records may need to be manually migrated or deleted at the end of their retention period.

Next: EDRMS Content Manager

Managing your Email

EDRMS Content Manager

EDRMS Content Manager is an integrated Enterprise Document and Records Management System (EDRMS) capable of managing the full range of corporate information. The Government of British Columbia has established EDRMS Content Manager as the standard information management software program to be used across Government.

To save emails to EDRMS Content Manager you must first enable the EDRMS add-in for Outlook. To do this, select File, then Options, then Add-ins. Go to the Manage Com add-ins button and click Go. Make sure the EDRMS add-in box is checked.

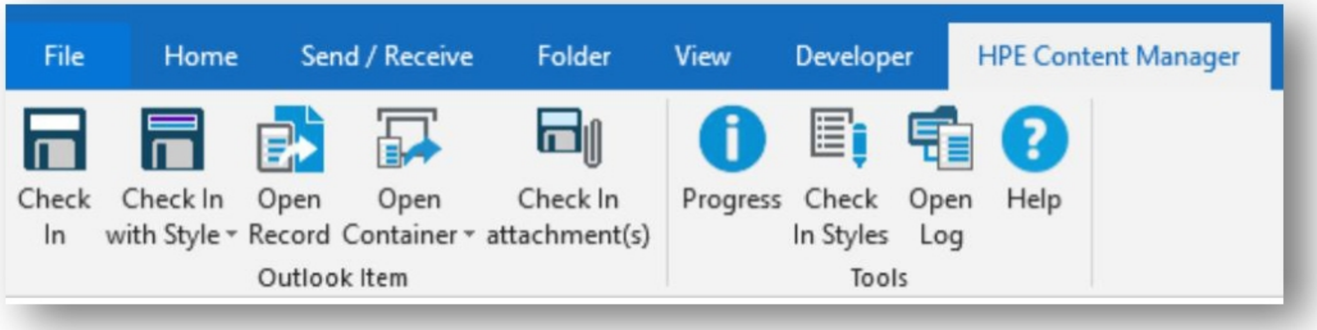
To enable the Outlook add-in from EDRMS select File, then Desktop Add-ins. Check the Outlook box and click OK.

In Outlook, there are a number of options for saving emails to EDRMS.
These include:

- Saving messages with attachments, saving message without the attachments, or saving attachments separately from the email
- Linking an Outlook folder to EDRMS so that every email that is added to the folder will be automatically saved to EDRMS.

When you have successfully saved the email in EDRMS, you can delete it from your Outlook.

For more guidance on EDRMS see the EDRMS guidance site.



Next: LAN / Shared Drives

Managing your Email

LAN / Shared Drives

Saving email to a shared folder on your office Local Area Network (LAN) is an option for offices without an EDRMS. To do this, simply:

- Copy and paste the email from your Outlook to the shared folder. This will save it as an MSG file.
- Right click on the message and click Properties.
- Check the Read-Only box, click Apply and OK. This will ensure that the message cannot be edited by others.
- You can also save your emails as PDFs on your LAN. Saving email PDFs and their attachments separately is recommended. While it is possible to embed the attachment within the PDF, this method is not stable and attachments can be difficult to open later. The ability to open and inspect attachments is critical for proper email preservation.

Next: Deleting Emails Appropriately

Managing your Email

Deleting Email Appropriately

Now that you know what constitutes an official email record and how to save them properly, you should now delete the redundant emails from your Outlook. You are also encouraged to delete transitory emails, personal emails and other non-record reference material that is taking up valuable space. Deleting emails quickly and appropriately ensures that your inbox will remain clean and clutter-free.

This section will provide guidance on simple Outlook tools that will help you to delete your emails appropriately. It will also include simple exercises you can perform to find and delete common categories of transitory email.

Tools include:

- **Clean-up Tool**
- **Auto-delete Folders**
- **Empty Deleted Items on Exit**
- **Exercise: Find and Delete Meeting Requests**
- **Exercise: Find and Delete Emails to Distribution Lists**

NOTE: You are prohibited at all times from 'triple-deleting' emails (i.e. attempting to purge an email from your 'Recover Deleted Items' folder).

This should not be confused with double deletion, which happens when deleted emails are cleared from the 'Deleted Items' folder. The double deletion process is important for clearing space in your Outlook account, but must only be done if the items in question are permitted to be disposed of.

Next: Working with the Clean-up Tool

Managing your Email

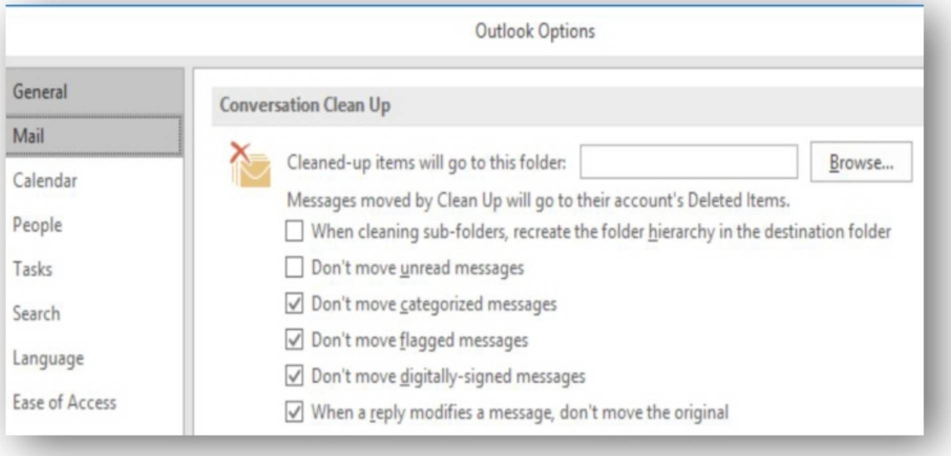
Working with the Clean-up Tool

Email threads (termed "conversations" in Outlook) can be long and cumbersome. As people reply to the email thread, the existing content is automatically included in each response, resulting in a lot of redundant information. The Clean Up tool scans conversations and removes any redundant emails from the thread.

Before cleaning up a conversation, ensure that all important emails are flagged or categorized.

To set the parameters of the Clean Up tool:

- Click File, then Options.
- In the Outlook Options pop-out window, select the Mail tab on the left and scroll down to Conversation Clean Up. By default, all cleaned up items will go to the Deleted Items folder. You can change this destination folder if you would like them to be routed elsewhere. There are options that allow you to prevent certain classes of email from being cleaned. Ensure that flagged emails and categorized emails are not cleaned.



Conversation Clean Up

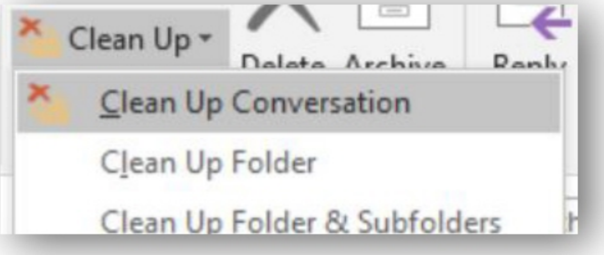
Cleaned-up items will go to this folder:

Messages moved by Clean Up will go to their account's Deleted Items.

☐ When cleaning sub-folders, recreate the folder hierarchy in the destination folder
☐ Don't move unread messages
☑ Don't move categorized messages
☑ Don't move flagged messages
☑ Don't move digitally-signed messages
☑ When a reply modifies a message, don't move the original

To run the Clean Up tool:

- Highlight the folder you would like to clean. Click Clean Up.
- From the dropdown menu, there are 3 options: run the clean up tool on a single folder; on a folder and its subfolders; or on specific conversations.
- It is recommended that you run the conversation cleanup tool regularly as part of your work routine. Use caution and refrain from cleaning email threads that may contain important information.



Next: Working with Auto-delete Folders

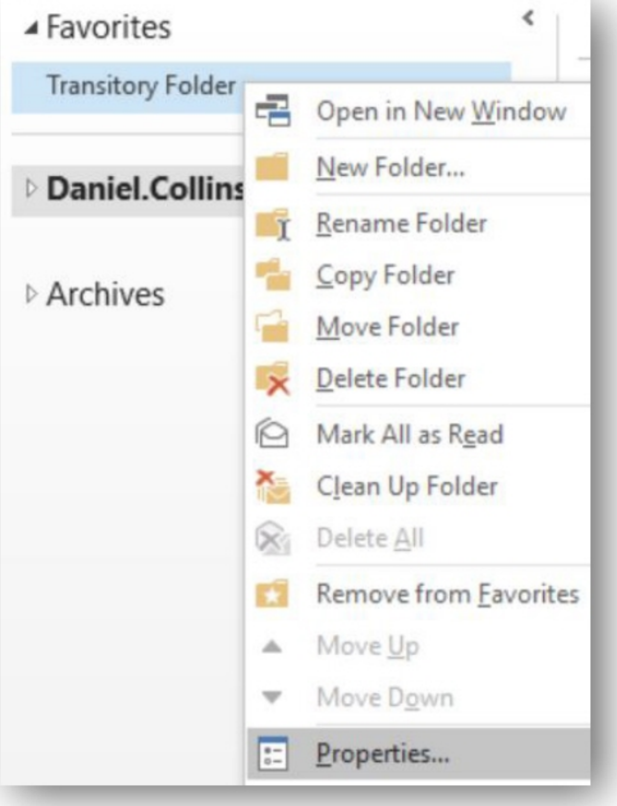
Managing your Email

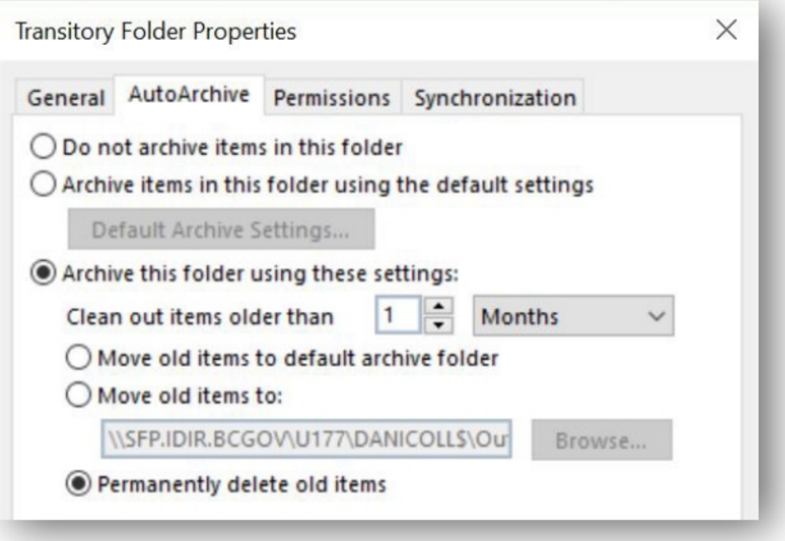
Working with Auto-delete Folders

As mentioned in the section on Folders, setting up a Transitory Folder is highly recommended. You can set Outlook Rules to autoroute certain classes of transitory emails directly to this folder. There is also the option of configuring this folder to permanently delete transitory emails after a specified period. Automating this process encourages you to think critically about what is transitory and what is an official record.

To configure this setting:

- Highlight your Transitory Emails folder in the left navigation pane, and right click on the folder to open the drop down menu.
- Select Properties.
- In the pop-out window, select the AutoArchive tab.
- Select Archive this folder using these settings. Then select Permanently delete older items. You can specify exactly how long you want your transitory emails to remain in the folder. One month is recommended. Click Apply, then OK. Your transitory email folder will now auto-delete items that are older than one month.





○ Do not archive items in this folder
○ Archive items in this folder using the default settings
● Archive this folder using these settings:
Clean out items older than 1 Months
○ Move old items to default archive folder
○ Move old items to:
\\SFP.IDIR.BCGOV\U177\DANICOLLS\Ou
● Permanently delete old items

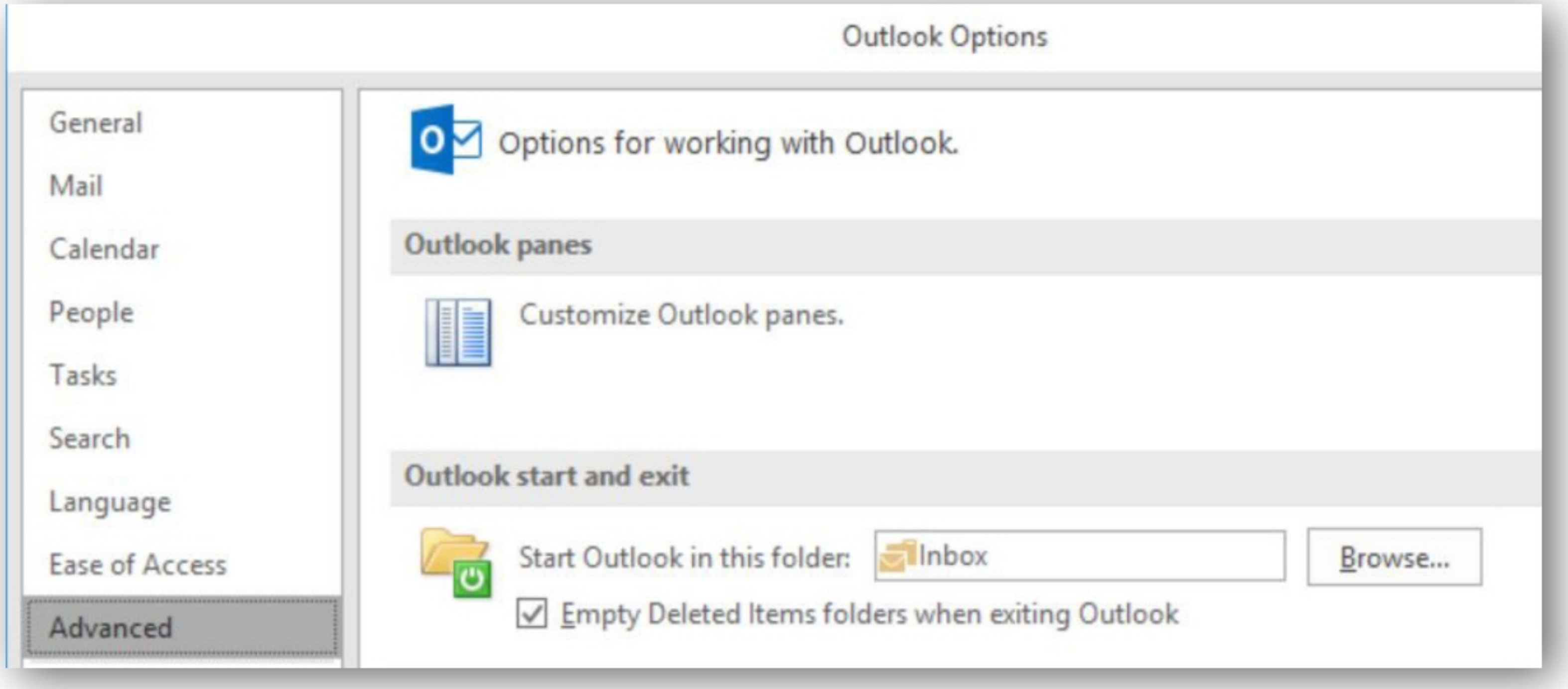
Next: Emptying Deleted Items on Exit

Managing your Email

Emptying Deleted Items on Exit

Clicking Delete in Outlook does not permanently delete the email; it sends it to the Deleted Items folder. In the default settings, this folder will not be emptied unless you do so manually. However, you can configure Outlook to empty your Deleted Items automatically when you exit the application. This is the recommended option.

- Click File then Options.
- Choose the Advanced tab on the left side. Under the "Outlook start and exit" heading, check the box that says Empty Deleted Items folder when exiting Outlook and hit OK.



Outlook Options

Options for working with Outlook.

Outlook panes

Customize Outlook panes.

Outlook start and exit

Start Outlook in this folder: Inbox

☑ Empty Deleted Items folders when exiting Outlook

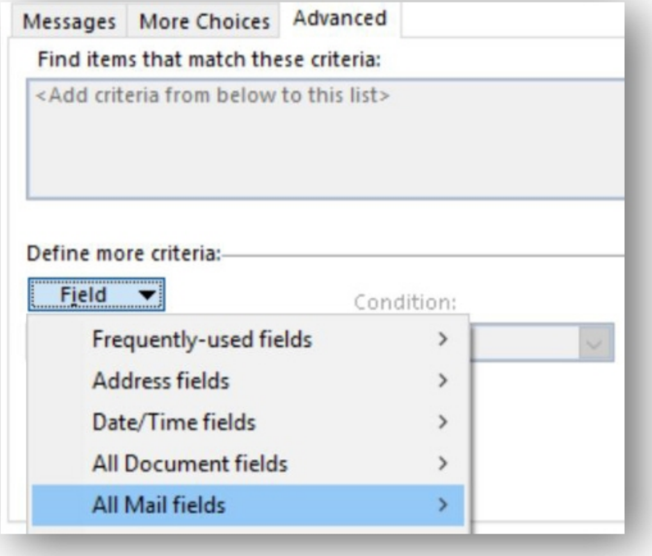
Next: Exercise: Find and Delete Meeting Requests

Managing your Email

Exercise: Find and Delete Meeting Requests

Meeting requests can quickly build up in your inbox. To find all meeting requests:

- Click on the Advanced tab in the Advanced Find window.
- Click Field to open a dropdown menu and mouse over All Mail Fields.
- From this list select Message Class. In the Value box, type "Meeting Request" and click Add to List and then Find Now. This will return all meeting requests. Select the requests you want to delete or delete them all.



Messages | More Choices | Advanced

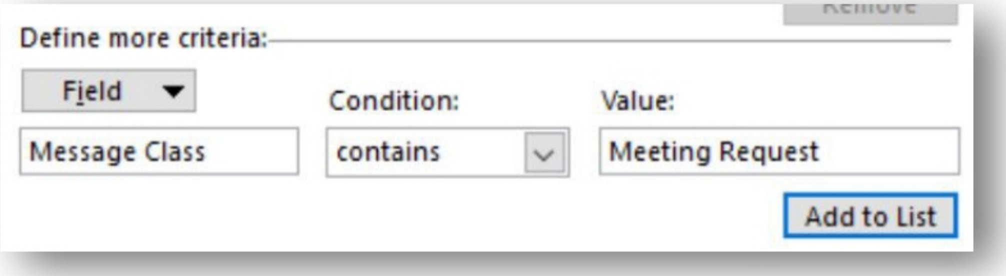
Find items that match these criteria:

<Add criteria from below to this list>

Define more criteria:

Field ▾ Condition:

- Frequently-used fields ›
- Address fields ›
- Date/Time fields ›
- All Document fields ›
- All Mail fields ›

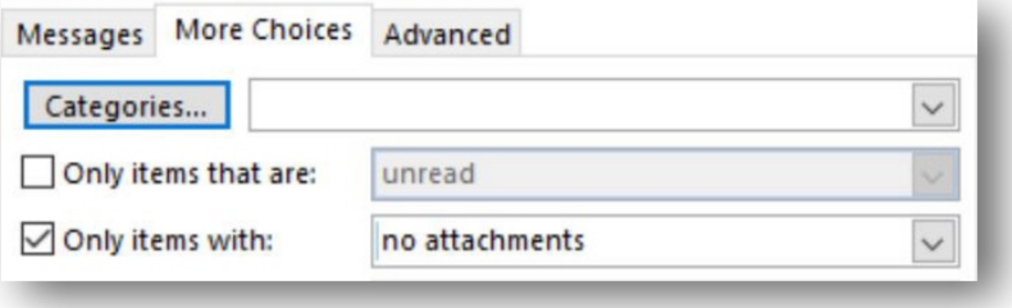


Define more criteria:

Field ▾	Condition:	Value:
Message Class	contains	Meeting Request

Add to List

NOTE: Meeting requests with attachments may be important records. You can narrow the search to exclude email requests with attachments by selecting the More Choices tab and checking the box that says Only items with and selecting no attachments. Always exercise caution before deleting large quantities of email. This will not impact your Outlook calendar.



Messages | More Choices | Advanced

Categories...

□ Only items that are: unread

☑ Only items with: no attachments

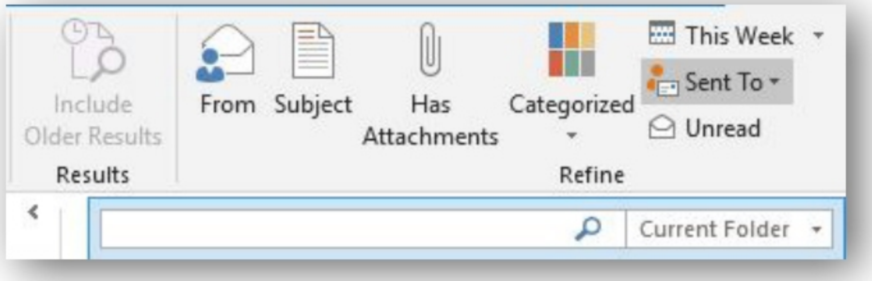
Next: Exercise: Find and Delete Emails from Distribution Lists

Managing your Email

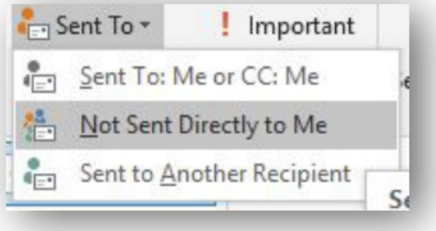
Exercise: Find and Delete Emails from Distribution Lists

Emails received through internal distribution lists are another type of transitory email. As the receiver, you are generally not responsible for filing emails received through a distribution list (although you may want to keep a copy for reference purposes). To find and delete all emails that are not sent directly to you:

- ▶ Click the search bar to open the Search Tools tab and click on Sent To to open a dropdown list.



- ▶ Click the Not Sent Directly to Me button. This should return all emails sent through distribution lists. Always exercise caution before deleting large quantities of email.



Warning: if your branch or department has gone through administrative changes, your IDIR may have changed too (e.g. from 'Blogs, Joe CITZ:EX ' to 'Blogs, Joe FIN:EX'). This may result in emails sent prior to the change getting caught up in the search. You can add your old handle to the exclusions by adding it to the search bar.

Next: Further Information

Further Information

Further Information

I have a specific question or problem. Who can I contact?

For additional information contact your Records Team or check out the Records Management Website.

For general questions about Information Management policy requirements and your responsibilities as an employee, please email GRS@gov.bc.ca.

For questions about privacy, please contact the Privacy and Access Helpline at 250-356-1851 or email privacy.helpline@gov.bc.ca.

For questions about FOI requests, please contact your FOI manager or email FOI.Requests@gov.bc.ca.

For questions about records management practices and requirements, please contact the Government Records Service Hotline at 250-387-3387 or email GRS@gov.bc.ca.

For technical support and help with your email account, please call 250-387-7000 or email 77000@gov.bc.ca.

Transitory Information Quick Tips

Not all government information needs to be retained. These quick tips will help you identify information that is transitory and understand your responsibilities as an employee. For in-depth guidance, see the Transitory Information RM Guide or contact your Records Officer.

What Is Transitory Information?

Information is transitory if it is not required to support or document a government body's actions and decision-making. Transitory information is information of temporary usefulness that is only needed to complete a routine action or prepare a subsequent record (e.g. a new version). Transitory information requirements are established in the Transitory Information Schedule.

Content and context determine whether recorded information is transitory, not its format or medium. Just like other records, transitory information can exist in any format (paper or digital) and can be created and shared over a variety of media (e.g. email, social media, handwritten notes, voice mail, MS Teams, SharePoint, wikis, digital systems).

See next page for common categories of transitory information.

What Is Not Transitory Information?

It is important to understand which records are not transitory. Critical information, such as documentation of decisions, needs to be filed in an appropriate recordkeeping system organized according to the relevant information schedule.

Consider: is the record

- □ required to document a decision?
- □ required to meet legal or financial obligations?
- □ needed to sustain government operations, programs, or administration?
- □ integral to a case (i.e. needed as context for related records in a case file)?
- □ needed for accountability purposes?
- □ covered by an information schedule (i.e. *ARCS*, *ORCS*, or a special schedule)?

If you answer "YES" to any of these questions, the information is NOT transitory.

DO NOT destroy any transitory information that:

- may be relevant to a *FOIPPA* request or legal discovery, or
- is stored in backup systems, which are an essential part of protecting government's information assets (i.e. "triple deleting" is not allowed).

Common Categories of Transitory Information

What	Features	Examples
1. **Transitory Messages** e.g. emails, MS Team chats, voice mail	Messages and attachments that do not document a business activity or decision (i.e. content lacks substance)	◦ Correspondence about meetings ◦ Announcement of a social event ◦ "cc" and "FYI" messages ◦ Message about drafts & revisions
2. **Transitory Drafts**	Drafts with no significant annotations, comments, approvals, or substantial changes	◦ Draft with minor edits & formatting updates but no changed content ◦ Incomplete draft that has been superseded by later versions
3. **Transitory Rough Notes and Working Materials**	Information used to support projects and develop official records	◦ Summary (précis) of an official record ◦ List of ideas or suggestions ◦ Flipchart (& other brainstorming records)
4. **Transitory Copies**	Copies not needed as evidence of decisions, actions, or consultation	◦ Convenience copy for a meeting ◦ Partial copy/extract ◦ Supplies of reports, flyers, or forms
5. **Transitory Systems Information**	Information that is no longer needed after it is entered into systems or generated as output Unneeded systems & internet usage documentation	◦ Cookies ◦ Data input forms ◦ Internet browsing history ◦ System output created for reference or for provision to clients
6. **Transitory Information from External Sources**	Published, solicited, & unsolicited items that have been ◦ only used for reference, ◦ referred to another office, or ◦ returned to sender.	◦ Advertising in various formats - pamphlets, catalogues, DVDs ◦ Newspapers & magazines ◦ Spam or junk mail ◦ Unsolicited correspondence not used for any actions or decisions ◦ Information redirected to the appropriate office ◦ Confidential information returned to sender

Dispose of transitory information as soon as you are finished with it!