## At a Glance

<table>
<thead>
<tr>
<th>Using your Email Account</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• When to use Government Email</td>
<td>4</td>
</tr>
<tr>
<td>• Accessing Government Email Outside the Workplace</td>
<td>6</td>
</tr>
<tr>
<td>• Use of Personal Email Accounts</td>
<td>7</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sending Email</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Tips for Sending Email</td>
<td>9</td>
</tr>
<tr>
<td>• Tips for Managing Email Discussion Threads</td>
<td>10</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Protecting Sensitive Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• How Can I Protect Government Information When Sending Emails?</td>
<td>11</td>
</tr>
<tr>
<td>• Can I Send Personal Information Over Government Email?</td>
<td>12</td>
</tr>
<tr>
<td>• What Are “Information Incidents”?</td>
<td>13</td>
</tr>
<tr>
<td>• How Can I Prevent Information Incidents From Happening?</td>
<td>14</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Searching For Emails</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Responding to FOI Requests</td>
<td>16</td>
</tr>
<tr>
<td>• Search Tips</td>
<td>17</td>
</tr>
<tr>
<td>• Advanced Find</td>
<td>19</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Managing Your Email</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Government Emails are Government Records</td>
<td>22</td>
</tr>
<tr>
<td>• Deciding what to Keep or Delete</td>
<td>23</td>
</tr>
<tr>
<td>• Examples of Official Email Records and Transitory Emails</td>
<td>24</td>
</tr>
<tr>
<td>• Email Decision Diagram</td>
<td>25</td>
</tr>
<tr>
<td>• Organizing Emails in Outlook</td>
<td>26</td>
</tr>
<tr>
<td>• Responsibilities for Saving Email</td>
<td>31</td>
</tr>
<tr>
<td>• Tips for Saving Email Records</td>
<td>32</td>
</tr>
<tr>
<td>• Preferred Email Preservation Formats</td>
<td>33</td>
</tr>
<tr>
<td>• Your Recordkeeping System</td>
<td>36</td>
</tr>
<tr>
<td>• Deleting Email Appropriately</td>
<td>39</td>
</tr>
<tr>
<td>• Exercise: Find and Delete Meeting Requests</td>
<td>43</td>
</tr>
<tr>
<td>• Exercise: Find and Delete Emails to Distribution Lists</td>
<td>44</td>
</tr>
</tbody>
</table>
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.
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.

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?
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.
**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
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’.
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.
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.
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

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.
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.
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.
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)
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.
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.
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 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.
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’.

▶ 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.

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.
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.
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
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** Save
- **NO** Routine and non-business
- **YES** Drafts and working materials
- **NO** Copies
- **YES** 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
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**
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).

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.

Next: Saving Email Records Outside Outlook
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

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.
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.
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.
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.
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.
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.

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.

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.

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.

**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 no attachments. Always exercise caution before deleting large quantities of email. This will not impact your Outlook calendar.

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.
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.