

Introduction

Emails created and received by University employees in the course of their work are also important and must be managed. Employees are responsible for the information that they create or transmit with email.

The email system (Outlook) is not an information management system. An information management system organizes information according to a file plan, provides secure, shared access, and most importantly applies retention and disposition rules. Emails must then be saved and managed in the corporate repository (information management system) such as DocuShare.

Why manage our emails?

- Emails are university information.
- If not managed properly, they can be inaccessible, lost or even deleted by mistake.
- Emails are not accessible when they are kept in the email system or personal folders instead of a shared workspace. By managing emails and saving them in a shared repository, we are better able to deliver services to our stakeholders in an efficient manner.
- Retaining records beyond their retention period has two distinct risks:
 - Retaining emails in one or more inboxes increases the chance that the information will get inadvertently accessed, forwarded or sent.
 - Retaining emails beyond the retention period creates an overly complex and burdensome compliance process – complicates the search process in the event of litigation or *Freedom of information and Protection of Privacy Act* (FIPPA) request.
- Avoid uncontrolled duplication.
- Corporate memory is siloed if emails are kept in email accounts. It does not promote transparency and accessibility.
- Emails are subject to FIPPA and must be provided to the Access to Information and Privacy Office upon request.

3 common types of email content

Operational email - related to the administration of University programs and activities in order to carry out services and functions.

When writing and managing emails:

- Write meaningful subject lines that describe the content and context of the body of the email message.
- Limit to one subject per email in order to facilitate filing.
- Keep messages business-like and avoid personal comments.
- CC's are used for information and not for action; limit your cc's to only those who need to know.

- Retain messages that are sent and received only if they relate to the university strategic and operational activities; all other messages can be treated as transitory and deleted.
- When retaining a series of replies or forwards, keep only the last message as long as the thread is complete and hasn't been changed in the course of the exchange.
- For more information, please consult the best practice on *What do I keep*.

Transitory email - used for a short-term period, for reference or informational purposes

- Keep them for a temporary period, only as long as they are needed.
- Delete once no longer needed.
- For more information, please consult the best practice on *What can I delete*.

Personal email - related to an employee's personal matters

Using your university email account for personal matters is not advised. [Policy 118](#) states appropriate use of University email.

Do not use your uOttawa account for personal matters

Using university email can cause problems for yourself or your family if you unexpectedly leave the University for any reason.
 Example: An employee uses their uOttawa email account for Ottawa Hydro bills. If the employee unexpectedly departs the University, they or their family has the cumbersome task of requesting and receiving approval to access the uOttawa email account to manage your affairs.

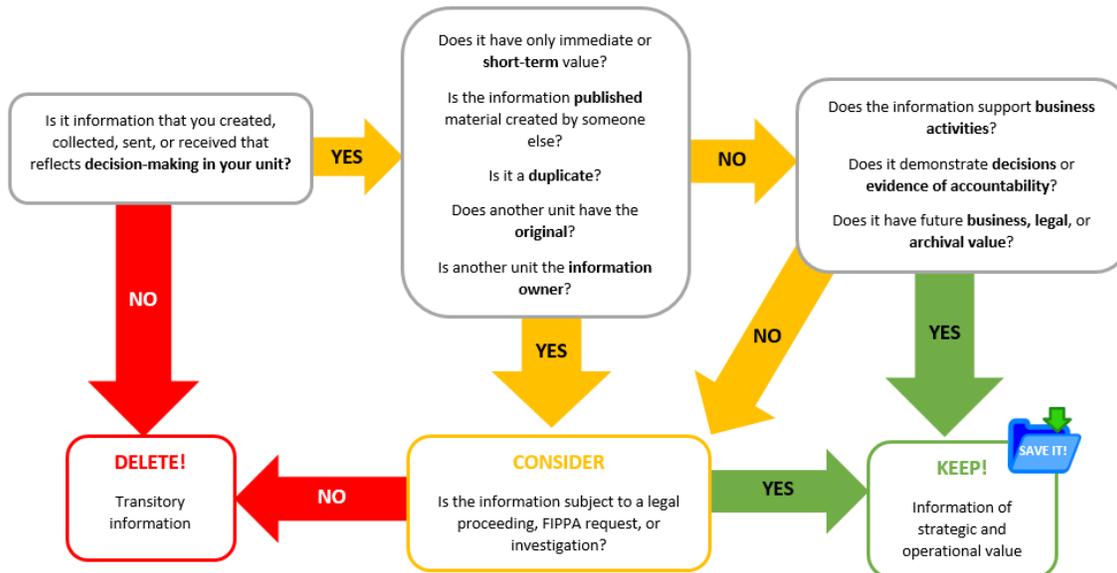
When you send an email using the uOttawa address, you are representing the University. Anything you say or include in that email is done on behalf of the University.

Do not use personal email accounts for University matters

When you are conducting University business, you must use your uottawa.ca email account. Using your personal account for University business becomes a problem when a FIPPA request is made, since emails are subject to FIPPA.

Remember: Emails are subject to FIPPA.

To help you determine the value of the content of an email consider:



Access to Information and Protection of Privacy

The *Freedom of Information and Protection of Privacy Act* (FIPPA) applies to emails and employees must search all information under their custody or control, including emails sent or received. Once an access to information request is received, it is a criminal offence to delete or alter the email. Contact aipo@uottawa.ca if you have any questions.

- Be prudent about emails that you create and what you attach to them. Once you send an email, you have no control over what the recipient may do with it. This can lead to unintended disclosure of personal or confidential information.
- Do not include any content in an email you would not want publicly disclosed.
- Do not send personal information by email, instead use a secure means of transmitting personal and confidential information (Ex. [LiquidFiles](#)).
- Avoid unnecessary forwarding of email to reduce the risk of a privacy breach.
- When accessing your email off of campus be mindful of unsecure Wi-Fi and use a Virtual Private Network (VPN). Consult the [Best-Practice on Working Outside of the University](#) for more information.

How do I manage my email?

- Regularly dispose of transitory and personal emails. Please consult the best practice on *What can I delete*.

- Regularly file emails of operational and strategic value in a shared repository according to the *General Classification Plan*. This allows for easier retrieval and proper retention and disposition of information.
- Preserve the integrity by making sure that all saved emails include:
 - the message,
 - the sender and recipient,
 - time and date,
 - any attachments.
- Regularly delete emails sent or received for informational purposes only, or where you are in cc.

Don't forget to manage your SENT emails as well! They are just as important.

Who needs to save them?

One individual should be selected and identified as the person who is responsible for saving and storing all information, including emails, related to projects or issues. All other staff implicated in the project can then confidently delete all duplicate records.

Example	Who is responsible?
A new program is being conceptualized, researched, and implemented in your unit	The Project Manager is responsible for ensuring all relevant emails relating to the project are retained. All other staff involved can delete duplicate copies of emails.
You receive emails related to a University Committee that you are a member of.	The University Secretary, or the individual identified as the secretary in the Terms of Reference, is responsible for ensuring that emails related to this committee are retained. All other members can then delete any duplicate emails.
Cases where many units are implicated in a specific case/issue. (Example: involving a campus incident.)	Use your best judgment. Initiate a conversation with all units involved to determine which units will be responsible for saving which types of information. If possible, save them in a central, shared repository where all units involved can have access.

When should I save them?

Emails can be saved at a number of different stages depending on the particular issue they relate to.

- When an email is obviously significant save it as soon as it has been sent or received.
- At the end of a project you could save significant emails and then delete the remainder.
- Threads: Save as soon as it is clear that the conversation has finished. If it is not clear, save it at the point when a definitive conclusion or decision has been made. Only save one copy of the most complete “thread” and not each individual message.

Attachments

Be sure to save all relevant attachments along with the message. This ensures the integrity of the email is preserved.

If emails and their attachments are kept in mailboxes, there are risks:

- Versions of documents that should have been deleted could remain in mailboxes and will need to be provided in the case of a FIPPA or litigation request.
- Keeping duplicate versions of a document within your email can create confusion as to which version is the correct version.

Shared Mailboxes

When using shared mailboxes it is important that the users of the mailbox have a shared understanding of how messages will be managed.

Users should agree on:

- Who should answer which messages and how this will be indicated to the team.
- How will users indicate when a message has been read or is being processed?
- Who is responsible for capturing any business records contained in the email?
- Where will the different types of email be retained if needed for reference? (Which shared repository?)
- How long will messages in the inbox be retained?

HINT: Use the colour coded sorting tool in Outlook

Disposition of email

Don't forget to delete your deleted!!

Identify transitory emails and delete them FREQUENTLY. Please consult the best practice on *What can I delete*.

Follow the University of Ottawa [Records Retention and Disposition Schedule](#) to determine how long emails related to strategic and operational activities must be kept.

When you leave your position

When you leave your position, for any reason, make sure that you do not take the contents of your mailbox with you. Remove and save any important emails in the appropriate repository as provided by the University (Example: DocuShare, Shared Drive, etc.), and delete all transitory emails. Refer to the *Information Management Handbook* for more information on what to do with the information in your custody when you leave the University.