Privacy Best Practices

**Mount Royal University – Email
(Google Gmail)**

Overview – Email

Electronic mail (Email) is a method of sending messages between computers using electronic networks.

The following best practices are meant to help Faculty and Staff (Users) manage their University Email account in accordance with the Alberta Freedom of Information and Protection of Privacy (FOIP) Act and Mount Royal University Email Policy **1006**.

General Principles for Users (Faculty and Staff)

1) All users must conduct Email exchanges with **professionalism** and manage their Email responsibly.
2) Faculty and Staff should make every effort to use their **@mtroyal.ca address** for only work related correspondence.
3) **Personal correspondence** should be conducted with an individual's personal Email address. Occasional or Incidental personal use is allowed if it does not significantly impact work responsibilities or contravene the University Email Policy (1006).
4) The **account holder** is responsible for properly storing and filing all Email messages or attachments that are required for on-going use by Mount Royal University and to securely dispose of Email messages that are no longer required. (Process Details provided below)
5) **Unencrypted Email** is not a secure method of transmitting confidential or sensitive information over the internet. If it is necessary to send such information, users must take steps to secure it by encrypting the message (https), while also taking into account the **sensitivity of the data** being transmitted through the internet and the **level of security** at the source and destination systems.

What are my Email responsibilities?

✓ **Professionalism (Tone):** Ensure that Mount Royal business related Email communications (including chat) are kept professional (FOIP). Always keep personal (home) matters separate from business Email and refrain from emotional exchanges.

✓ **Level of sensitivity**: Always consider the level of sensitivity of the personal information you are about to Email, what security measures are in place and the associated consequences even if privacy is still breached despite any security precautions already implemented (including encryption).

No matter what security protocols are in place there is always a risk that the Email may still be intercepted or, even more likely, disclosed to an unauthorized person by the recipient due to being sent/forwarded/printed or lost.
*(Applies to both Google and Lotus Notes)*

(High-Risk) Sensitive personal information: Is information that readily identifies a person, which could cause significant harm to them if disclosed to an unauthorized Third Party. Examples of significant harm include, damage to reputation, physical harm and identity theft (financial fraud).

Information that is known to cause significant harm: includes; contact information, date-of-birth, social insurance number, banking or health information (under the Health Information Act) and, at times, confidential/draft deliberations. Identifiable Names that are often included along with this information in an electronic transmission can increase the level of harm by tying the sensitive information to an identifiable individual.

✓ **Routinely Delete:** Emails that are considered **Transitory** on a regular basis.

Transitory Emails are those communications that are considered; routine, duplicates, provided only for short-term reference purposes (Forwarded or CC'd), draft decisions, or personal transmissions.

Tips – For Quick Routine Deletions

(1) **Delete items in Drafts/Chats/Sent Folders**

Left-side : Click Draft/Chats/Sent on Left-Side, Click on the box (icon below) select **All** in the drop-down, then Click **Delete** , which can be either (**Trash Can**) or (**Discard Drafts**)

☐ ▾		**Then**	🗑	**Or**	Discard drafts
All					
None					
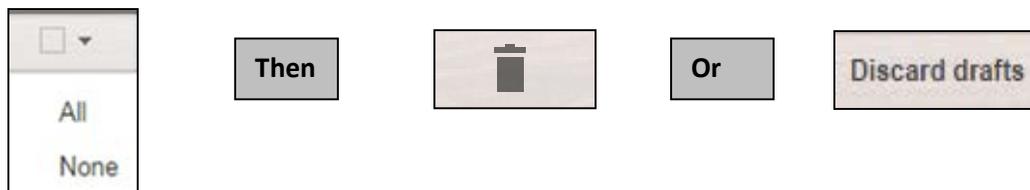
(2) **Empty your Trash Can**

Left-side : Be sure to also **Empty your Trash**, select **All** in the drop-down, then (**Delete Forever**)

☐ ▾	**Then**	Delete forever
All		
None		
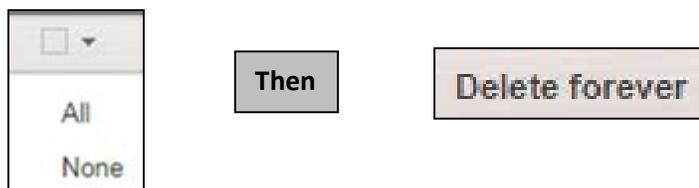
(3) **Delete Downloads:** Google (Gmail) will save any attachments that are opened (downloaded)

Go to your C: Drive or **C:\Users\[Your User Name]\Downloads**, click **Edit**, then **Select All**, then **Edit** (again), then **Move to folder**, select **Recycle Bin**, then press **Move**.
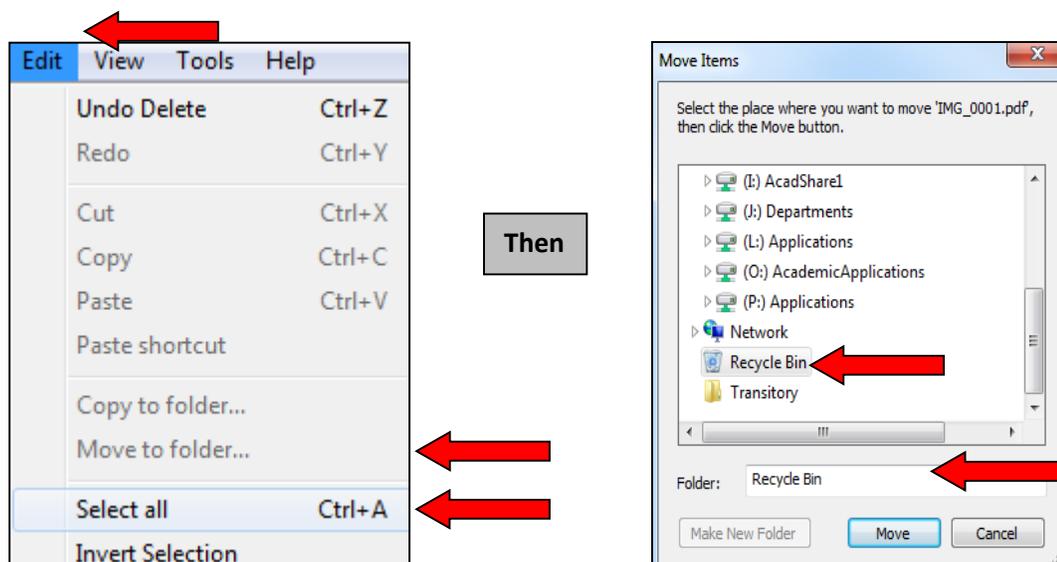
*Be sure to also **Empty you Recycle Bin**!

Legal Holds (FOIP)

If a department or user has been **notified** of a formal access-to-information request under the FOIP Act or is involved in a formal legal discovery – The Email **must not be deleted** if it is required for these reasons. (MRU Policy **1006** and **1602**)

✓ **Routinely File:** Always file Emails that are related to **Official University Business** based on the University Records Retention Schedule Policy (Print, File, Delete Electronic Copy)

Official University Business Emails are those that; provide evidence of a University business activity, final decision, or transaction that are needed to be retained for long-term reference regarding University business. These Emails often provide evidence of accountability, compliance, or protect the rights of individuals (See Quick Tips below).

Helpful Hints

(1) Best practice is to print Official Emails and file (Classify) them under the **MRU Records Retention Policy** (MRU does not currently have an Electronic Records System).
   - Emails left in a Google Account are often only accessible by the owner of the account rather than by the University.
   - Emails left in a Google Account cannot be easily assigned a code under the Records Retention Classification system. Additionally, there is no record of destruction as required under the FOIP Act .

(2) Use **Filters (Rules)** and **Labels (Folders)** to create folders and place your Emails into the folders based on your business specific function/topic/subject.

Electronic Filing Methods

Option #1 – Drag and Drop Method - File As Emails are received
   - Create a **Label (Folder)** : Click on the **Cog** (Top-right), then **Settings**, then the **Labels tab**, then **Create New Label** [Enter Folder Name, then Create]
   - Drag and Drop (select the received Email), then drag it to the created **Label (Folder)**
      -Most official business activities can be managed by function and there is often a records retention code to help determine when to print/file the records
      - If the Label (Folder) contains Transitory Emails such as newsletters then routinely delete the Emails in that Label (Folder)
   - For multiple Emails, Check-mark (select) all Emails, then select **Move To**, then select the Label you want the Emails to go to.

Option #2 – Filter (Rules) Method - Automatically file received Email in Folder
   - Create a **Label (Folder)** : Click on the Cog (Top-right), then Settings, then Labels tab, then **Create New Label** [Enter Name, then Create]
   - Create the **Filter (Rules)** : Click on the Cog (Top-right), then Settings, then Filters tab, then **Create New Filter** .
      -In the **From** field, enter the individual(s)/organization(s) addresses you wish filtered, then **Create a New Filter for this Search**
      -Check-mark **Skip the Inbox**, then **Apply the label** and Using the drop-down, select the Label (Folder) you want the Email to automatically go to.
      -Click on **Create Filter**

Tip: Use the same **Filter (Rules)** to also automatically send **Transitory Emails** to a **Label (Folder).** This feature works well for Newsletters you regularly receive where you can read the Email and then immediately delete them all together in one spot. (All located under one **Label (Folder)**

Electronic Filing Taxonomy

Mount Royal University has implemented Google Docs to serve as a **collaborative tool** used mainly for electronic transmissions (Email, calendaring, chat and word processing).

The majority of collaborative records are considered **Transitory (short-term)** records and can be deleted when you no longer require them for reference purposes.

Google Docs is **not** considered a formal Electronic Document and Records Management System (or EDRMS), which is software specifically designed to ensure an electronic record provides both true and reliable evidence that a business transaction or activity took place.

For example, Google Docs does not:

o   Automatically assign or classify a Records Retention Code based on the Mount Royal University Records Retention Schedule. *There is manual entry, but it is not standardized.
o   Maintain a detailed or on-going audit log of the changes made by the user.
o   Record (formally) that the electronic records have been destroyed in accordance with legal requirements and University Policy.

Users can; however, still group their Emails so that their Emails are managed based on date and function.

Below are some filing **recommendations** by using **Label (Folder)** Title.

Primary **Label (Folder)** – Function **or** Activity **or** Sender (l)

Example = FOIP Requests (LR030 – 5 Years)

Secondary **Label (Folder)** – Year (2013 **or** 2014 **or** 2015, etc)

Example = 2010

Tertiary **Label (Folder)** – File Title (File Number **or** Last Name **or** Contract Number)

Example = 2010-G-0001, 2010-G-0002

FOIP requests (LR030 – 5 Years)

2010

2010-G-0001
2010-P-0002
2010-G-0003

Privacy Best Practices

Mount Royal University – Email (Quick Tips)
(Google Gmail)

Before Clicking "Send"

- ✓ Check the **tone** of the Email – keep it professional
- ✓ Refrain from emotional exchanges
- ✓ Keep personal Emails <u>separate</u> from Emails related to University business
- ✓ **Double-check** the recipient's Email address and attachments
- ✓ Consider privacy and the risks – do not Email **sensitive information** (ie.) SIN Numbers
- ✓ Use a meaningful subject line
- ✓ Ensure that the subject content (thread) has not changed
- ✓ Limit the Email length (be concise)
- ✓ Utilize Bcc (Blind-Carbon Copy) to protect personal Email addresses

Tips for reducing the volume of Email

- ✓ Limit the use of "<u>Reply to All</u>"
- ✓ Only Carbon Copy (CC:) for those who actually "<u>need-to-know</u>"
- ✓ Use Blind-Carbon Copy (Bcc) sparingly. (Consider an in-person meeting)
     -Bcc: can be used for sending list-serv (protect privacy)
- ✓ Limit the use of attachments (Consider supplying a website url or drive directory link)
- ✓ Minimize your sign-up for vendor newsletters and listserv's
- ✓ Automatically delete regular junk mail – Use the **Filter (Rules) Method**
- ✓ Consider other forms of communication tools (office meetings or by phone)
- ✓ Evaluate whether creating an Email for the task/deliberation/discussion is suitable

Email Security – Username/Password

- ✓ Create a strong password by ensuring that it:
     - o is at least <u>eight-characters</u> long
     - o contains a combination of letters, numbers and symbols (%,&,*)
     - o does not contain a complete word in a dictionary
     - o is not password1, password2, 123456, abc123, etc

- ✓ Change your password on a **regular basis**
     - o every 1 to 3 months

- ✓ Protect your username/password - **PHISHING**
     - o **Never** enter your username/password if requested to do so via <u>Email link</u>
     - o MRU ITS and/or other MRU Faculty/Staff **will never Email** and ask for you to enter your username/password using a link.
     - o Be cautious concerning any Emails requesting your username/password. Imposters will try to "pose" as MRU ITS or MRU Faculty/Staff.

What Emails are considered Official University Business?

A **small percentage** of Emails may be retained because they provide evidence regarding Official University Business. Notably, more important decisions should have formal documentation supporting the action taken (rather than just an informal Email). Examples of suitable documentation include, signed letters, meeting minutes, policies, or official reports.

Official University Business Emails should be printed and filed in accordance with the Mount Royal University Records Retention Schedule, which protects Email from alteration and ensures the Email is destroyed in accordance with legal requirements under the Records Retention Schedule.

Best practices recommend not keeping an Email record in more than one format. If the Email has been printed and filed, the electronic copy should be deleted so that it is retrievable in only one place.

The employee making the final decision for the task is responsible for sending the Email to be filed if required.

Official University Business Emails that need to be retained include records that…

- ✓ Document the final decision of an issue
- ✓ Provide evidence of a business transaction
- ✓ Demonstrate compliance with accountability, or is needed for other business/legal requirements, such as policy development
- ✓ Protect the rights of citizens and/or the University
- ✓ Have potential business, legal, research, or archival value
- ✓ Messages related to employee work schedules and assignments

---

What Emails are considered Transitory?

Studies indicate that approximately 80-90% of your Email is considered Transitory as it is considered an informal means of communication. Most formal decisions that actually need to be retained are typically recorded using more formal mechanisms such as, signed letters, meeting minutes, policies, or official reports, which all document a final decision.

All Transitory Email can be routinely deleted once you no longer need them – without referring to the formal Mount Royal University Records Retention Schedule.

Always set time aside regularly (such as once a month) to delete Transitory Emails.

Transitory Emails are those records that…
- ✓ Are only required for a limited time
- ✓ Will not be required in the future
- ✓ Ensure the completion of a routine action (Helpdesk Tickets)
- ✓ Help in the preparation of a subsequent final record. (Draft decisions)
- ✓ Are not required to provide evidence of a University business activity, decision, or transaction
- ✓ Are CC'd to you or considered duplicates
- ✓ Simply provide an FYI, where no action/decision is required
- ✓ Are provided to you simply as a reference (FYI or Announcements)
- ✓ Have an expired life span (meeting notices, appointments)
- ✓ Are related to a personal matter (Lunch arrangements)
- ✓ Are considered in regards to a personal matter
        [when the Email comprises of 100% personal content]

Deciding What Emails to Keep

Step 1
Does the Email **provide evidence** for a business activity, decision, or transaction for Mount Royal University?

Yes

Step 2
Does the Email contain information only concerning immediate or **short-term value**?

Is it a **duplicate** [CC]?

Is it a **draft version** of a decision with no further value?

Is the **final decision** formally documented (ie.) Minutes or Reports?

Was the Email sent only for **reference** purposes?

No

File and Manage the Email
✓Needed to support business activities.

✓Provides **long-term value** or evidence concerning MRU business activities or provides a record of final decisions.

✓Protects the **rights of citizens** and/or MRU.

✓Provides evidence concerning – **compliance**, accountability, or other business/legal or archival requirements.

No

Yes

Transitory Email
Routinely delete it

MOUNT ROYAL UNIVERSITY 1910

For Additional Information - Contact

Mount Royal University Information Management & Privacy Office

-Telephone: (403) 440-7288
-Website: www.mtroyal.ca/foip

For the Employee FOIP (RIM) Toolkit on MYMRU: Click on **Employee** Tab under **Legal Services** – Click **FOIP**