Privacy Best Practices

Mount Royal University – Electronic Collection/Storage/Transmission of Personal Information (Google Drive/Forms/Docs)

Google Suite: Document, Presentation, Spreadsheet, Forms, Drawings

Overview – Electronic Collection/Storage/Transmission

The **Electronic Collection/Storage/Transmission** of personal information can occur through the internet in many different ways in order to obtain personal information, which is required for business units to complete their routine operations at Mount Royal University.

The following best practices are meant to help Faculty and Staff when they need to both consider and manage the privacy risks associated with the electronic collection/storage/transmission of personal information through the internet based on the Alberta Freedom of Information and Protection of Privacy (FOIP) Act and Mount Royal Policies **810-01**, **1006**, **1601** and **1602**.

Notably, although Mount Royal University has made every reasonable effort to ensure security based on both the most up-to-date information technology practices and the available due diligence processes for internal/external service providers, current Information Technology industry standards still advise that electronic transmissions should generally be treated as unsecure due to its electronic medium (Google and Lotus Notes). Therefore, if Faculty and Staff deem that it is necessary to collect/store/transmit personal information electronically, they must also take reasonable steps to:

1) **Secure** the personal information,

2) Consider the **level of sensitivity** concerning the information at issue and

3) Evaluate the **level of security** at the source/destination of the systems involved.

General Principles for Users (Faculty and Staff)

1) Faculty and Staff must protect personal information by making **reasonable security arrangements** against such risks as unauthorized access, collection, use, disclosure, or destruction.
2) If Faculty and Staff decide that it is necessary to **collect/store/transmit** personal information electronically, they must take reasonable steps to **secure** the personal information, consider the **level of sensitivity** concerning the information at issue and the **level of security** at the source/destination of the systems involved.
3) Any collection, use, or disclosure of personal information through the means of electronic collection/use/transmission must be only if that information relates to, and is necessary for, an operating program or activity of Mount Royal University in accordance with the FOIP Act.
4) Any collection, use, or disclosure of personal information through the means of electronic collection/use/transmission must be limited and only to the extent necessary (**demonstrable need**) to enable Mount Royal University to carry out its purpose to fulfill its mandate as prescribed under the FOIP Act.
5) Individuals **need to be notified** that Mount Royal University is directly collecting personal information about them in accordance with the FOIP Act.
6) Individuals should be **provided an alternative** to the electronic collection mechanism at the point of collection when possible such as, through the collection notice.

Definition - Personal Information

The Alberta FOIP Act **1(n)** defines "**personal information**" as recorded information about an **identifiable individual** (person) including, name, home address, home telephone number, race, political beliefs, health care history, education history, employment history and opinions.
In contrast, information that does not identify a person would not be considered "personal information", which means obligations under the FOIP Act do not apply.

Examples of **non-identifiable information** include, aggregate data, statistics, annual reports, general financial statements, postal codes and other information that does not identify an individual. At times, **partial names and student numbers** can be used to limit the ability for individuals to be readily identified, or tied to more sensitive personal information, in the event of a privacy breach.

Generally, electronic transmissions that involve personal information will possess a higher level of risk concerning a breach of privacy and/or causing harm than, that of, non-identifiable information where such risks would be minimal.

Additionally, while **Faculty research information** and **teaching materials** do not fall under the access and privacy provisions of the FOIP Act, similar reasonable security arrangements, as outlined below, may also be used to protect this type of Faculty information if it is collected/used/transmitted in electronic format.

FOIP Notification Statement – Collection Notice

Mount Royal University (a public body) is required, under the FOIP Act, to notify individuals that their personal information is being collected, which also applies to the **electronic collection** of personal information. Notably, the FOIP Collection (Notification) Statement is required when there is a new collection of personal information or if the personal information already collected will be used for a new purpose from that of original collection.

The **FOIP Notification (Collection) Statement** can be posted on a website or through the electronic collection mechanism being utilized including, Google Forms.

The FOIP Notification (Collection) Statement must include:

(1) The **purpose** for which the information is collected.
-The purpose of the collection means the reason(s) the information is needed and the use(s) that Mount Royal University will make of the personal information.

(2) The **legal authority** for the collection
*-Usually section **33(c)***
*-Mount Royal University may only collect limited personal information only if it **directly relates to**, and is **necessary for**, an operating program of the University.*
*-The personal information being collected must have a **direct connection** to the program or there must be a **demonstrable need** for the personal information.*

(3) The **Contact Information** of the Mount Royal University Employee who can answer the individual's questions about the electronic collection.
-Include, Title, Business Address, Business Telephone Number, website (if applicable)

As an additional best practice, the FOIP Notification (Collection) Statement should also notify individuals that the personal information is being collected electronically, where it is being stored (external/internal) and also provide alternative options for collection if the individual so chooses.

Example - FOIP Notification (Collection) Statement - Initial Collection:
The personal information that you provide electronically on this application form is collected under the authority of the Post-Secondary Learning Act and the Freedom of Information and Protection of Privacy Act of Alberta section33(c)

The collected information will be used for the purpose of academic administration and stored with a [Third Party Vendor - Name], which may be housed on servers residing outside of Canada, and therefore, may be subject to the laws of a foreign jurisdiction. Although Mount Royal University has made reasonable efforts to protect the privacy of users, the University cannot guarantee protection against possible disclosure of electronic information residing in another country. Questions regarding the collection of personal information, or to inquire about alternatives in regards to the electronic collection of personal information, can be directed to Office of the Registrar at: 4825 Mount Royal Gate, SW; Calgary, AB; T3E 6K6 or by phone at 403.440.6246.

Authentication of Identity

The authentication of identity is the process of proving or ensuring that the individual is who they purport to be.

Protecting privacy often requires verifying or **authenticating the identity** of the individual providing personal information especially when that information is intended to be collected electronically.

Notably, the **verification of an individual** through the internet can significantly lower the **level of assurance** that the transaction, concerning the personal information at issue, is with the correct person who owns the information. However, assurance of authentication can be increased if the business unit has standardized processes in place to ensure the individual's identity. Typically, it is something only the individual the information is about would know (password, pin number, security question).

For example, Google forms can be set to only allow individuals to access the form using their unique **@mtroyal.ca** account login as a form of authentication of identity.

Key considerations

The **level of authentication** implemented should be appropriate to the **level of sensitivity** of the personal information being collected/stored/transmitted. The collection of (High-Risk) sensitive personal information may require **multi-factor authentication** and stronger security protocols.

Example #1 - The person is required to only communicate using their official **@mtroyal.ca** address.
(Low-Risk or Medium-Risk)

Example #2 - The person is required to login using their unique (assigned) username and password, which prompts the person to enter their personal information.
(Medium-Risk or High-Risk)

Example #3 - The person is required to login using their unique (assigned) username and password, which prompts the person to enter a security question. The person can then enter their personal information into the database for collection.
(High-Risk or Sensitive personal information)

Types of Encryption

Encryption is an electronic security measure, or protocol, where information is encoded in a way that provides access to that information to only those parties who are, in fact, authorized to access the information. For example, Google Gmail automatically encrypts electronic transmissions using ***https (Hypertext Transfer Protocol Secure)*** in order to protect against data interception by an unauthorized person during transmission; however, the encryption technology will still not protect the information from being printed or forwarded by a human recipient.

There are several types of encryption:

- *Email Transmissions (In Gmail - https - Hypertext Transfer Protocol Secure)*
- *Full disk encryptions (converts disk information into unreadable code)*
- *Data file encryption (converts datafile information into unreadable code)*
  Note: Google Docs (Document, Presentation, Spreadsheet, Form, Drawing) are not encrypted.
- *Database encryption (converts database information into unreadable code)*
- *Network Drives (Limited Access to Network Drive)*
  Note: Google Drive is encrypted.
  - Storage of (High-Risk) or Red level information not recommended
  -Storage of (Medium-Risk) or Yellow level information possible; however, use partial names and student numbers for additional protection (best practice).

Generally, the more encryption that is implemented for a project will provide greater protection against unauthorized access to the information being stored; however, multi-factor encryption can also take a significant amount of resources to implement, which also needs to be considered as well. As a best practice, more sensitive information requires multi-factor levels of encryption to prevent against privacy breaches due to the increased level of harm.

Types of Storage (Internal and External)

There are two types of storage for electronic information, which are internal storage and external storage.

Internal storage means that the information being collected/transmitted electronically is stored on severs located within Mount Royal University. For example, Banner and/or File Directories such as the *H:Drive* are internal electronic space that store electronic information.

Internal storage is generally viewed as more secure than external storage because the information remains both in the **custody** and **control** of the University. Furthermore, electronic transmissions and storage are "typically" directed inwards, that is, towards the University.

External storage means that the information being collected/transmitted is stored on servers located outside of Mount Royal University. In many cases, the information is often stored in "**the cloud**", where a third party company has been contracted by the University to provide Software as a Service (SaaS). The software can include collection/storage/transmission functionality.

For example, Google stores (**custody**) electronic information that remains under the **control** of the University. As a more specific example, Google Drive can store information, while Google Forms provides the ability to collect information through the internet.

External storage is generally viewed as less secure than internal storage because the information is stored, or is in the **custody** of, a third party company; however, there are ways to increase the level of security by performing a Privacy Impact Assessment (PIA) and ensuring that the vendor regularly audits their information security practices and controls.

A **Privacy Impact Assessment (PIA)** is a mitigation tool recommended by the Government of Alberta that is reviewed by the University FOIP Office, Legal Services and Information Technology Services in order to help mitigate the privacy risks associated with collecting/storing/transmitting electronic information using a third party company. Notably, part of the PIA process also includes ensuring that the contract requires that the vendor audits their overall information security practices, on a regular basis, by an impartial third party.

The current recommended **Security Auditing Standard** is **SSAE 16 Type II**, which certifies that the vendor regularly audits their Logical Security, Privacy Controls, Administrative Controls, Data Center Physical Security, Incident Management and Change Management. The certification must apply to the vendor *actually contracted* to be responsible for maintaining University data rather than a secondary company, which the contracted vendor is relying upon in order to be considered a compliant provider. Additionally, the University must be able to request proof of the certification from the vendor as a way to prove that the third party company has appropriate security controls.

Generally, one should note that the definition of mitigate in *Black's Law Dictionary* is to *make less severe*. In short, although a Privacy Impact Assessment does provide documented reasonable due diligence, there will always still be a need for the user to also consider the **level of sensitivity** when transmitting personal information through the internet in order to protect privacy.

Common examples of the associated risks of using electronic collection/storage/transmission include:

- The Email with sensitive personal information is printed and lost by the recipient.
- The Email is sent to the wrong recipient by the user.
- The database encryption is successfully hacked or accessed (ie. the Heart Bleed Bug Virus).
- The encrypted Email or wireless signal containing sensitive personal information is intercepted.

The FOIP Act applies to all records in the **custody** or under the **control** of a public body notwithstanding specific records that do not fall under the Act.

Notably, the University can actually have **control** over records, but *not necessarily* have **custody**. This situation often arises a third party company is provided custody of University records; however, control is maintained through a contract. Examples include; Google, Offsite Records Storage

Custody: refers to the physical possession of a record by the University

Control: refers to the authority of the University to manage what is done with information being stored including the right or authority to manage, restrict, request

Levels of Sensitivity and Harm - Personal Information

Level of sensitivity: Always consider the level of sensitivity of the personal information you are about to collect/store/transmit, what security measures are in place and the associated consequences even if personal privacy is still breached despite any security precautions that have already been implemented (including encryption).

No matter what security protocols are implemented there is always a risk that the electronic personal information may still be accessed by an unauthorized person.

(High-Risk) Sensitive personal information: Is information that readily identifies a person that could cause **significant harm** either to them or the University if disclosed to an unauthorized Third Party.

Label Color	Sensitivity Classification	Possible Harms	Examples
Red	**(High-Risk) Sensitive Personal Information**	Unauthorized access could be reasonably expected to cause **significant harm** to individuals or the University. *Financial Harm* - Identity theft - Financial fraud - Loss of funds - Sanctions (Penalties) for contravening legislation *Damage to Reputation and/or Credibility* - Impaired decision making - Major political impact - Loss of public trust - Breach of legislation, contract, or regulatory standards - Contravention of the FOIP Act - Impact on service levels *Physical or Personal Harm* - Hazard to public safety - Personal or social hardship - Embarrassment	*Financial Information* *-date of birth* *-social insurance number* *-tax information* *-banking information* *-credit card information* *-purchase card industry (PCI) compliant information* *-personnel/student files* *Contact Information* *-address* *-phone number* *-Email address* **Higher risk if linked with date of birth, banking info, etc* *Health Information* *-health Information about individuals maintained by health professionals* *-diagnostic, treatment of care information regarding individuals* *-benefits* *Business Information* *-sensitive (confidential) draft deliberations that have not been publicly released.* *-solicitor-client privilege* *-business trade-secrets of a third party* *-vendor bids* *-draft proposals* *-contracts* *-information within a report of an arbitrator, mediator, or other person appointed to resolve or inquire about a dispute.* *-concerning behavior team* *-emergency response records* *-security incident reports*

(Medium-Risk) personal information: Is information that may identify a person that would likely cause **serious harm** to them or the University if it were disclosed to an unauthorized Third Party.

Label Color	Sensitivity Classification	Possible Harms	Examples
Yellow	**(Medium-Risk) Personal Information**	Unauthorized access could be reasonably expected to cause **serious harm** to individuals or the University. *Financial Harm* - Identity theft - Sanctions (Penalties) for contravening legislation *Damage to Reputation and/or Credibility* - Loss of public trust - Breach of legislation, contract, or regulatory standards - Contravention of the FOIP Act *Physical or Personal Harm* - Personal or social hardship - Embarrassment - **Contact information** misused for marketing, sales or other physical harm.	*Personal Information* *-name* *-student/employee id* **Recommend using partial name/id number to reduce risk of harm.* *Contact Information* *-address* *-phone number* *-Email address* **Higher risk if linked with date of birth, banking info, etc* **Note**: *Faculty/Staff business contact information can be released (public) - notwithstanding any known public safety issues. (Employee Name/Title/Office info)* *Educational History* *-research material* *-grades* *-completed coursework* *-intellectual property*

(Low-Risk) information: Is information that does not readily identify a person and, therefore, is not considered personal information under the FOIP Act. Any incident where the information is disclosed to an unauthorized Third Party would not cause significant harm to a person or the University if the information was disclosed to a Third Party. The disclosure would not be considered an unreasonable invasion of a person's privacy under the FOIP Act.

Examples of (Low-Risk) information include, aggregate data, statistics, annual reports, general financial statements, Faculty/Staff Names and Business Contact Information.

Label Color	Sensitivity Classification	Possible Harms	Examples
Green	**(Low-Risk) Information**	Unauthorized access is reasonably expected to **cause no serious harm** to individuals or the University. (Public Information) Information that **does not identify** individuals. *Financial Harm* - Limited risk of identity theft *Damage to Reputation and/or Credibility* - Limited risk of loss of public trust *Physical or Personal Harm* - Limited risk of personal or social hardship - Limited risk of embarrassment	*Non-identifiable information* *-final policies and procedures* *-annual reports* *-aggregate data* *-statistics* *-public meeting minutes and agendas* *-media releases (news)* *-information (non-personal) already public* *-job postings* *-draft project collaboration documents* **Note**: *Faculty/Staff business contact information can be released (public) - notwithstanding any known public safety issues. (Employee Name/Title/Office info) (Business card information)*

Appendix 1 - Electronic Collection/Storage/Transmission Recommendations – Privacy Risk Matrix - (Page 1 of 3)

Label Color	Sensitivity Classification	MRU FOIP Office Recommendations	Transmissions (Gmail) *Mitigation strategies*	Collection (Google Forms) *Mitigation strategies*	Storage (Google Drive/Docs) *Mitigation strategies*
Red	**(High-Risk) Sensitive Personal Information** **Unauthorized access could be reasonably expected to cause significant harm to individuals or the University.**	Electronic **transmission not recommended**. (Gmail) Electronic **collection not recommended** on external servers (Google Forms) Electronic **storage not recommended** on external servers (Google Drive/Docs) ***Use of other external third party companies requires a contract vetted by Legal Services. (MRU Policy 810-1)***	✓ Gmail -auto encrypts -uses https Encryption does not prevent messages from being sent unintentionally to the wrong recipient Encryption does not prevent messages from being forwarded to an unauthorized person. Always evaluate the: (1) **Level of sensitivity** of the information (2) **Level of security** measures that have been implemented (3) **Evaluate the consequences** if privacy is still breached despite the security measures that are in place.	✓ FOIP Collection Notice (Initial Collection) ✓ Authentication Process -2 to 3 multi-factor -username/password ✓ Use only the official **mtroyal.ca** address or MRU link	✓ **Limit** stored personal information (Necessary/Demonstrable Need) ✓ Use **partial info** (name or id number) -Lower risk of information being linked to a person. ✓ **Limit staff access** -username/password ✓ **Internal Storage** *External storage (ie. Google Drive) not recommended ✓ **Encryption** -Password file -Database -Data file ✓ **Records Retention (Permanent-Secure Deletion)** -Routinely **delete** data no longer required. -Use the **MRU Records Retention Schedule** for formal (final-long term) **Business Records**. -Routinely **delete** informal (draft-short term) **Transitory Records** when no longer required for reference. -Transitory records can be deleted when no longer required for reference. ✓ **Privacy impact assessment (PIA) – Highly recommended** -Third party contract assessment to ensure company collect/use/disclose information appropriately (FOIP). -External Vendor Security Audit Certification. -Examples of current security certifications include: **(SSAE 16 Type II) (ISO 27001, 27002) (SOC1, SOC2)**

Appendix 1 - Electronic Collection/Storage/Transmission Recommendations – Privacy Risk Matrix - (Page 2 of 3)

Label Color	Sensitivity Classification	MRU FOIP Office Recommendations	Transmissions (Gmail) *Mitigation strategies*	Collection (Google Forms) *Mitigation strategies*	Storage (Google Drive/Docs) *Mitigation strategies*
Yellow	**(Medium-Risk) Personal Information** **Unauthorized access could be reasonably expected to cause serious harm to individuals or the University.**	Electronic **transmission may occur**. (Gmail) Electronic **collection may occur** on external servers (Google Forms) Electronic **storage may occur** on external servers (Google Drive/Docs) ***Use of other external third party companies requires a contract vetted by Legal Services.*** ***(MRU Policy 810-1)***	✓ Gmail /Forms/Drive -auto encrypts -uses https Encryption does not prevent messages from being sent to wrong recipient. Encryption does not prevent messages from being forwarded to an unauthorized person Always evaluate the: (1) **Level of sensitivity** of the information (2) **Level of security** measures that have been implemented (3) **Evaluate the consequences** if privacy is still breached despite the security measures that are in place.	✓ FOIP Collection Notice (Initial Collection) ✓ Authentication Process -1 or 2 multi-factor -username/password ✓ Use only the official **mtroyal.ca** address or MRU link	✓ **Limit** stored personal information (Necessary/Demonstrable Need) ✓ Use **partial info** (name or id number) -Lower risk of information being linked to a person. *Faculty/Staff names and business contact information may be disclosed (FOIP). ✓ Restrict collection of **high-risk** sensitive personal information (Red) ✓ **Limit staff access** -username/password -limited access (Google Drive) ✓ **Internal Storage** is preferred *External Storage requires reasonable security considerations (ie. Google Drive possible - encrypted) ✓ **Encryption** - Password file - Database - Data file ✓ **Records Retention (Permanent-Secure Deletion)** -Routinely **delete** data no longer required -Use the **MRU Records Retention Schedule** for formal (final-long term) **Official Business Records**. -Routinely **delete** informal (draft-short term) **Transitory Records** when no longer required for reference. -Transitory records can be deleted when no longer required for reference. ✓ **Privacy impact assessment (PIA) – *(Optional – Best Practice)** -Third Party contract assessment to ensure company collect/use/disclose information appropriately (FOIP). -Examples of current security certifications include: **(SSAE 16 Type II) (ISO 27001, 27002) (SOC1, SOC2)**

Appendix 1 - Electronic Collection/Storage/Transmission Recommendations – Privacy Risk Matrix - (Page 3 of 3)

Label Color	Sensitivity Classification	MRU FOIP Office Recommendations	Transmissions (Gmail) *Mitigation strategies*	Collection (Google Forms) *Mitigation strategies*	Storage (Google Drive/Docs) *Mitigation strategies*
Green	**(Low-Risk) Information** **Unauthorized access is reasonably expected to cause no serious harm to individuals or the University.**	Electronic **transmission can occur**. (Gmail) Electronic **storage can occur** on external servers (Google Drive/Docs) Electronic **collection can occur** on external servers (Google Forms)	✓ Gmail /Forms/Drive -auto encrypts -uses https	✓ Not applicable: -Public information -Non-identifiable information -Not personal information -Not sensitive information	✓ Not applicable: -Public information -Non-identifiable information -Not personal information -Not sensitive information

Appendix 2 - What electronic records are considered Official University Business?

Some electronic records may be retained because they provide evidence regarding Official University Business. Notably, more important decisions should have formal documentation supporting the action or decision that has taken place. Examples of formal documentation include, signed letters, final meeting minutes, policies, or final reports.

Official University Business electronic records should be printed and filed in accordance with the Mount Royal University Records Retention Schedule, which protects the electronic documentation from alteration and also ensures that it is destroyed in accordance with legal requirements.

Best practices recommend not keeping an electronic record in more than one format. If the electronic record 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 electronic record to be filed if required.

Official University Business electronic records 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

Appendix 3 - What electronic records are considered Transitory?

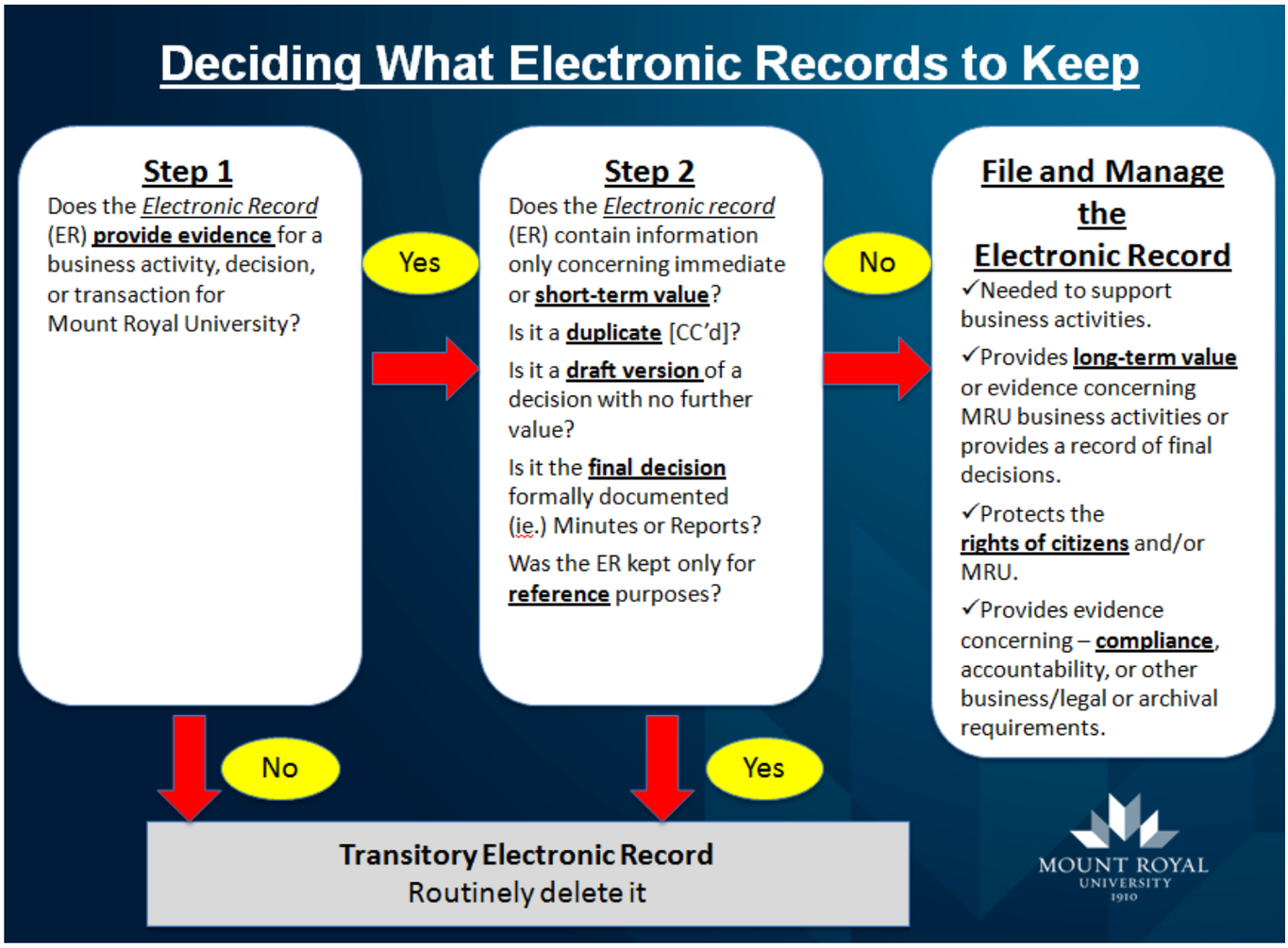
All Transitory electronic records can be routinely deleted once you no longer require them for reference purposes without referring to the formal Mount Royal University Records Retention Schedule.

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

Transitory electronic records 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]

Appendix 4 - How do I decide what Electronic Records are Transitory or for Official University Business?



For Additional Information - Contact

Mount Royal University Information Management and 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 on **FOIP**