Privacy Best Practices

Mount Royal University
Responding to a Privacy Breach – A Quick Guide

Overview – Privacy Breaches

A privacy breach occurs when there is an unauthorized collection, use, disclosure or destruction of personal information, which involves information belonging to an "identifiable" individual under the *Alberta Protection of Privacy Act* ("the POPA").

Examples of personal information may include, but not limited to; Name, Home Address (Personal), Phone Number (Personal), Social Insurance Number, Credit Card Number, Health Information and Gender Identity.

The collection, use, disclosure or destruction of personal information is considered "**unauthorized**" if it occurs outside of the regular **legal allowances or allowable circumstances** provided under the POPA.

These legal allowances are intended to outline how Mount Royal University must appropriately manage personal information under its custody and/or control, which it requires for its mandated operating programs and activities.

The most common privacy breach is when there is an **unauthorized disclosure** of personal information to either an external third party or unintentional internal disclosure of personal information to the incorrect employee.

Examples of privacy breaches include:

- An email, fax or mailed letter that is sent to the wrong recipient
- A system or database that has been hacked (compromised) by a foreign party
- A laptop or electronic portable device that has been lost or stolen
- Specific records (paper/electronic) have been lost or have failed to be securely destroyed

How to Respond to a Privacy Breach

Step 1 - Contain

Make every effort to immediately contain the breach to prevent further harm to the individual(s) the information is about. Examples in this step may include:

- ✓ Finding or retrieving the electronic device
- ✓ Temporarily shutting down a web-site or system
- ✓ Finding or retrieving a mailed letter from a recipient
- ✓ Taking down a posting
- ✓ Revoking access
- ✓ Correcting a weakness in physical security
- ✓ Documenting the date/time the breach was discovered and contained
- ✓ Contacting applicable University Department (i.e. ITS) to help with containment (as required or necessary)
- ✓ Stopping the activity that caused the breach

Tip: If the personal information has been accidentally "**received**" by Mount Royal University - Do not "**re-send**" the record containing the personal information back to the sender.

(1) Keep the received record (temporarily) and provide standardized notice regarding receipt to the sender. *Generally describe the record received without transmitting any unnecessary personal information.

(2) Shred/Destroy the received record once the sender acknowledges your notification.

(3) Be aware that the organization that sent the personal information is responsible for notifying the affected individual(s).

Step 2 – Investigate

Once the breach is contained – investigate (or determine) the cause of the breach and the associated risks concerning the breach.

Contact the MRU Access and Privacy Office (ext 7288) and the appropriate Manager(s) of the Department to help formally document the following in a **Privacy Breach Report**:

- ✓ What personal information is involved? Is it Financial/Health Information?
- ✓ How many individuals were affected by the breach?
- ✓ Who was affected by the breach? Students/Staff/Faculty?
- ✓ What harm may have been caused by the breach?
- ✓ What caused the breach?
- ✓ How many individuals had unauthorized access to the information?
- ✓ How long was the information accessible?

Step 3 – Notification

When the **initial investigation** is complete – Mount Royal University Access and Privacy Office must determine (as soon as practicable) whether to provide a **notification letter** to the affected individual(s) based on its initial findings (**Step 2**).

Generally, the **notification letter** to the affected individual(s) must:

- ✓ Provide the initial results of the investigation (**Step 2**) so those concerned are well informed and are able to take appropriate measures to protect themselves, including the following:
  - Date/Time period of breach
  - Description of the circumstances of the breach
  - Description of the information involved (Name, address, etc)
  - Risks to the individual(s) caused by the breach
  - Immediate steps taken by the University to control/reduce harm
  - Future steps planned by the University to prevent future breaches
  - Steps that individual(s) can take to further mitigate the risk of harm
  - Contact information of the University employee who can answer questions
  - Other authorities or organizations contacted (as required)
  - Inform individuals of **their right** (under the POPA) to request that the review the matter.
  - Supply the contact information for the **Alberta Information & Privacy Commissioner**.

Note: The **notification letter** may be signed either by the Information Management & Privacy Advisor (MRU Access and Privacy Office) **or** by the Associate Vice-President/Director/Manager/Dean of the Department where the privacy breach occurred (as deemed appropriate).

However - it is crucial to **contact the MRU Access and Privacy Office** (ext 7288) in order to ensure that the notification letter has met the specific legal requirements under the POPA.

Step 4 – Prevention (Management Review)

The Information Management & Privacy Advisor and the Manager of the Department will work together to ensure that the necessary process changes are implemented, so that a similar privacy breach will not occur again in the future.

The recommendations provided through the **Privacy Breach Report** will be presented to the Manager responsible for the respective Department concerning the breach.

The final **Privacy Breach Report** will be sent to the affected individual(s) by the MRU Access and Privacy Office to keep them informed of the preventative steps taken as a result of the breach by the University.

All **Privacy Breach Reports** are kept on file by the MRU Access and Privacy Office in the event there is a request for review by the **Alberta Information & Privacy Commissioner**.