Freedom of Information and Protection of Privacy Act: Quick Reference Sheet

Key FOIP Principles:

- Everyone has a **right to seek access** to the records in the custody/control of Mount Royal University – *Section 2*

- Everyone has a **right to privacy** concerning their personal information held by Mount Royal University – *Section 2*

  Under Section 1(n) **personal information** means "**recorded information**" about an "**identifiable**" individual.

  For example, aggregate non-identifiable statistics may be publicly released if the information does not readily identify an individual or invade the personal privacy of an individual.

General rules for managing Personal Information:

- **Collection**: Personal information **may only be collected** if it relates directly to and is necessary for an operating program or activity of MRU (demonstrable need) – *Section 33(c)*
- **Collection: MRU must inform** individuals that personal information is being collected about them by providing individuals a **FOIP Notification Statement** during collection – *Section 34*

  The **FOIP Notification Statement** must inform individuals (at the point of collection) of:

  - The **purpose (reason)** for the collection
  - The **legal authority** for the collection [usually under section 33(c)]
  - The **contact information** of an MRU employee who can answer questions about the collection.
    -(Title, business address, business phone number)
    -(Business email and business url) if available

Tip: The Office of the Registrar provides a **FOIP Notification Statement** for students during the application process for the purposes of **Academic Administration**
(For example, activities related to course instruction)
http://www.mtroyal.ca/AcademicSupport/StudentRegistrationRecords/FOIP/index.htm

The **FOIP Notification Statement** template is also available online:
www.mtroyal.ca/foip > Policies and Guidelines > FOIP Notification Statements and Consents

- **Use: MRU must use** personal information only for the purposes outlined during collection as indicated in the **FOIP Notification Statement** (consistent use) - *Section 39*

- **Disclosure: MRU must refuse to disclose** personal information to Third Parties (those seeking access to another individual's information) to protect the privacy of the individual the information is about.

  However, there are **allowances** for limited disclosure to a Third Party in certain circumstances listed in *Section 40* (below)

  Under section 40, ***MRU*** *may* disclose (or use) limited personal information **only to the extent** necessary to carry out its purposes in a reasonable manner – *Section 40(4)*

MRU may disclose personal information in the following circumstances…

- ✓ ***40(1)b:*** *if the disclosure would not be considered an unreasonable invasion of a 3rd party's privacy under section 17 > 17(2) includes salary "range", confirming enrolment in a school or Post-secondary program, or confirming receipt of an award or Degree obtained.*
- ✓ ***40(1)c:*** *for the purpose for which the information was collected or compiled or for a use consistent with that purpose* ***(consistent with the original FOIP Notification Statement)***
- ✓ ***40(1)d:*** *if the individual has identified the information and* ***consented to*** *the disclosure (in writing via signed form)*
- ✓ ***40(1)g:*** *for the purpose of complying with a subpoena or warrant*
- ✓ ***40(1)h:*** *to an employee of the public body…if the information is necessary for the performance of the duties of the employee.*
- ✓ ***40(1)k:*** *for the purpose of collecting a fine or debt owing by an individual to a public body*
- ✓ ***40(1)l:*** *for the purpose of determining or verifying an individual's suitability or eligibility for a program or a benefit*
- ✓ ***40(1)r:*** *if the public body is a law enforcement agency*
- ✓ ***40(1)x:*** *for the purpose of managing or administering personnel of a public body*
- ✓ ***40(1)bb:*** when the information is available to the public
- ✓ ***40(1)bb.1:*** *if the personal information is of a type routinely disclosed in a business or professional context such as, Employee Name, Employee Title, Business Address, Business Phone/Email.* ***(Business card rule)***

Protecting Personal Information:

- Mount Royal University **must protect** personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, or destruction – *Section 38*

Physical Security

- ✓ Lock cabinets and rooms containing personal information
- ✓ Ensure that files containing personal information are not easily accessible
- ✓ Use the **University Records Retention Schedule** to routinely (impartially) destroy records containing personal information. (Fewer records means less chance for a breach)

Administrative Security

- ✓ Attend FOIP Awareness Training or utilize the Employee FOIP Tool Kit Materials (MYMRU)
- ✓ Assess and implement access policies/procedures for your business area
- ✓ Only collect/use/disclose information "necessary" to perform work-related tasks
- ✓ Check identification of those who seek access to their records
    - Implement Standard Security Questions
    - Limit access to only through in-person photo id check
    - Always check ensure the identity of any individual over the phone or through email

Technical Security

- ✓ Lock your computer when left unattended (Press **CNTRL, ALT, DELETE**)
- ✓ Use passwords and granular level access for systems
- ✓ Double-check email attachments and email addresses before pressing send
- ✓ Keep emails professional and business-related
- ✓ Do not accept emails from people you don't know **(PHISHING)**
- ✓ Do not accept emails from co-workers that appear suspicious (generic) **(PHISHING)**

Portable Device (Laptop – Flash Drive - iPhone) Security

- ✓ *Refrain from storing any personal information on a portable device at all – eliminate the risk
- ✓ Limit the amount of personal information being stored on the portable device
- ✓ Do not leave portable digital devices unattended or overnight in a vehicle
- ✓ Enable strong passwords (encryption or Bit Locker) to limit access to the portable device
- ✓ Do not send personal information over unsecured public wireless or WIFI networks (data interception risk)
- ✓ Sever or routinely remove personal information from the portable device
- ✓ Learn how to shut off the portable device remotely (if possible)
- ✓ iPhones **("Settings" – "Touch ID"): (1) Use a strong password** (letters-digits-symbols combo)
  (2) Turn on **Erase Data** after 10 failed login attempts
  (3) Turn off **Notifications** viewable on the lock screen
  (4) Turn off Siri access when on the lock screen

Access to Information – Routine Disclosures:

- Business units can regularly release information to the public (or informally upon request) – if it is determined that the information can be **routinely disclosed**.

  *A **routine disclosure** is a request (or regular demand) for information by any person where access can be easily granted without redacting any information under the FOIP Act in order to protect someone else's privacy. (or relying on sections 16 – 29 of the FOIP Act)*

  Examples of records that can be **routinely disclosed** (informal basis) can include when:

  - ✓ The records being sought actually **belong to the individual** [check id before disclosing].
  - ✓ The records are in a **standardized form** where the record could be easily or routinely severed. For example, everyone's personal information is located at the top of the form.
  - ✓ The records being requested are **general in nature** and contain no personal information.
  - ✓ The requested record is **already public**. Examples: Annual Reports, Newspaper Articles

Access to Information – Formal FOIP Requests:

- Business units that receive requests for information where the disclosure of the information would result in the invasion of personal privacy can forward the requestor to the MRU FOIP Office. (www.mtroyal.ca/foip)

  *A **formal access-to-information request** is when the individual is seeking access to information that requires redacting portions of information contained in the records prior to their release because the disclosure of that information would be considered an invasion of someone else's personal privacy. (or redaction that relies on sections 16 – 29 of the FOIP Act)*

  Examples of records that would need to be formally redacted by the MRU FOIP Office and (subject to legal review by Service Alberta) can include when the records being disclosed:

  - ✓ contain information belonging to another individual (disclosure of the information in the records would result in an invasion of privacy)
  - ✓ contain information regarding business interests of another Third Party (company) (Example: trade secrets, scientific formulas)
  - ✓ would be harmful to an individual or public safety
  - ✓ contain confidential evaluations (employee evaluations)
  - ✓ would be harmful to law enforcement
  - ✓ would harm intergovernmental relations
  - ✓ contain advice from officials such as advice, consultations, deliberations, or draft plans
  - ✓ would be harmful to economic interests of a public body
  - ✓ contain test procedures, tests, and audits (harmful to test procedures)
  - ✓ contain privileged information (legal advice)
  - ✓ includes information that will be available to the public within 60 days