Access to Information

At the University, information that is not public is classified and treated as confidential. Staff at UTM have access to a range of confidential information. One key type of confidential information is personal information, which is information about an identifiable individual, which may include, but is not limited to, faculty, staff and students. A University employee is only permitted to access personal information as necessary to fulfill job responsibilities, and information must be treated in a manner consistent with the purposes for which it was collected. Personal information must generally not be released to or discussed with anyone other than the individual whose information is involved, or other University staff who also need the personal information to do their jobs, or unless the individual has given explicit consent. Responsibility for following this “need-to-know” principle rests with everyone at the University. Both a University official seeking the personal information and an official who may disclose it are responsible for ensuring that the disclosure is properly executed.

It is a legal responsibility of the university to ensure that personal information is kept confidential and secure, and only accessed on a need-to-know basis.

The following guidelines set out required practices to ensure that UTM faculty and staff meet this obligation. If you have any questions or special requirements, please discuss these with your supervisor or contact the UTM FIPPA Liaison, in the Office of the Campus Council, 905-828-5233; cindy.ferencz@utoronto.ca.

More detailed information is available in the guidelines developed by the Office of the Vice-President and Provost titled Access and Privacy Practices: General and Administrative: http://uoft.me/AccessandPrivacyPractices

Electronic information:

• Storing confidential information on a USB key or your computer’s hard drive

Confidential information, including personal information (such as names, student numbers, contact information, academic information, financial information, etc.) should be held in a U of T institutionally run secure server environment with appropriate restricted user rights or it should be encrypted. A secure server is centrally administered and regularly maintained by IT staff with effective, up-to-date security software that is patched and updated consistent with accepted IT security expectations.

General secure server characteristics are outlined at page 18 of the following Provostial Policy, Access and Privacy Practices: General and Administrative, available here: http://www.provost.utoronto.ca/policy.htm
If local storage is required (e.g. your computer’s hard drive or a USB key), the storage device must be encrypted to protect confidential information.

This standard applies to confidential university information regardless of the type of device or platform on which it is stored and whether it is a personal or university owned device.

• **Transporting personal information outside the office**

Electronic records taken out of a University secure server environment should be protected with **strong, up-to-date encryption**.

• **File Sharing and Storage Services such as Dropbox**

Confidential information on a resource – such as Dropbox -- that is not on a secure university server, must be encrypted. The decryption password should be shared through another secure channel, such as telephone.

• **Security of Computers**

All computers require both physical and system protection, as a security baseline for confidential records or data.

The following are required practices that help to ensure that computer, software and data are appropriately and effectively protected:

-When possible, University IT security support;
-Prompt software and security updates, including operating systems and anti-virus programs;
-Full disk encryption;
-Sound user account practices, including strong passwords;
-Physical security of the machine;
-Suitable data backups.

• **Security of Mobile Devices**

Any mobile device or data store (phone, laptop, tablet, USB key etc.) that is to be used to hold or transport personal and/or other confidential information must be encrypted. Passwords or pins for devices must be strong, and of suitable length and complexity.

• **Transmission of data / Email Security**

With the exception of internal email (from one UTOR address to another UTOR address), email is generally not a secure form of communication, because if it can be intercepted, third parties can read it. Use of email to share personal information should be limited to when there is no reasonable alternative. Confidential information can be sent as an encrypted attachment. Passwords for encrypted attachments should be communicated by different means or channels, such as telephone, not another email.
If it is necessary to access confidential information from offsite, access should only be via institutionally approved virtual private network (VPN) or secure remote desktop connection.

- **Equipment retirement/disposal**

When the time comes to retire equipment, unencrypted data stored on it must be reliably destroyed prior to it leaving the custody of the university. Computers, phones, scanners, printers, flash drives, laptops and other equipment can all retain data or information that is considered confidential. Typical decommissioning will involve several full overwrites of storage media/devices with random data as a minimum standard. If a third party is to decommission the equipment, as is often the case with printers and multifunction devices for example, written confirmation from that party is required that the data have been securely and confidentially destroyed to industry standards.

For computer and data security assessments and consultation regarding full-disk-encryption, mobile device security options, network storage and secure remote access options please contact the UTM IITS Help Desk at helpdesk.utm@utoronto.ca or phone 905-828-5344.

**Paper documents:**

As with electronic information, paper documents and files containing personal information are highly confidential. These should be placed in locked cabinets whenever you are not in your office, and office doors should be locked. This follows the principle of protecting documents behind two levels of locks – one on the building and/or office, and another on a secure cabinet.

Electronic document storage and management on secure University servers is encouraged as a means to reduce the risks and storage load of hard copy records.

Particular care should be exercised when transporting hard copy records outside the office. This should only be done when absolutely necessary. The individual responsible for the office/unit should determine and communicate as appropriate, which records can or cannot be taken offsite.

**If files must be taken offsite, the following guidelines should be followed:**

- Minimizing the number of files taken;
- Taking copies rather than originals;
- Ensuring that files are secure during transit - files should not be left unattended, for example, in a parked car;
- Any confidential and/or personal information that is taken home must be kept in a locked cabinet or similar fixed unit when not in use.

The UTM Office of the Registrar has developed a standard operating procedure for dealing with student information received in paper form. Such information is transferred
to a secure electronic format as soon as possible. More detail is available from the Office of the Registrar.

Always use a cross-cut shredder to securely destroy confidential paper records.

**Clean desk policy**

When leaving your office, ensure that all confidential documents, including documents with personal information, are locked in a cabinet or drawer, and that your computer is locked and password protected.

**Parents and third parties:**

The university often receives requests from parents or other third parties for access to student information; these individuals may be persistent in their inquiries. Parents do not have a right to such information; in fact, privacy legislation prevents the university from sharing any personal information with a third party unless the individual (e.g., the student) has consented. Only share student information with a parent or other inquirer if there is previous written authorization from the student, or the student attends in person and authorizes the sharing.

**Emergency situations:**

We have an obligation to provide personal information in compelling circumstances that affect the health or safety of an individual, where providing that information would help to reduce the health or safety concern. Health and safety trump privacy. Consult your manager or director whenever there is a health or safety concern, and be sure that you follow the University’s Emergency Disclosure of Personal Information guideline:


**Loss of information:**

If any personal information is lost or misplaced, e.g., a document, file, USB key, laptop, etc., you have an obligation to report this immediately to the UTM FIPPA Liaison, in the Office of the Campus Council, 905-828-5233; cindy.ferencz@utoronto.ca. In such cases, please notify your Director immediately. Consequences can best be controlled with quick intervention.