**Faculty of Applied Science and Engineering**

**Privacy and Access to Information Guidelines**

At the University, information that is not public is classified and treated as confidential. Staff in the Faculty of Applied Science and Engineering 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. Personal information can be used or disclosed for the purposes(s) for which it was collected or a consistent purpose.

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 for official University functions or duties, or unless the individual has given explicit consent. Responsibility for “need-to-know” sharing belongs to both the individual receiving and the individual disclosing information. If in doubt, confirm the need to know with the recipient.

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 APSC faculty and staff meet this obligation. If you have any questions or special requirements, please discuss these with your supervisor or contact the Applied Science and Engineering FIPPA Liaison, Tom Nault, Faculty Registrar, 416-978-5894, tom@ecf.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 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

document:

http://www.provost.utoronto.ca/Assets/Provost+Digital+Assets/Provost/Provost+Digital+Asset

s/Provost/fippa.pdf

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

-User passwords should be a minimum of 8 characters and include a mixture of upper and lowercase letters, numbers and symbols.

• 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 your departmental IT resources. For faculty administrative offices, please contact the Helpdesk helpdesk@ecf.utoronto.ca

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 of confidential

information outside the office. This should only be done when absolutely necessary. The

individual responsible for the records of the office/unit should determine and clearly

communicate to faculty and staff which confidential records can be taken offsite. The default is

that no confidential records should be taken offsite other than those so identified by the person

responsible.

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

• Take as few records/files as you can to accomplish the task;

• If possible, take copies rather than originals;

• Ensure 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 enclosure when not in use.

* A log of the items removed from the office should be kept, the log should include when the items were removed and returned to the office.
* Always use a cross-cut shredder (or a commercial shredding company) to securely destroy confidential paper records.

The 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.

**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. Computers should be configured to automatically lock after not being is use for 10 minutes.

**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:

<http://uoft.me/emergencysituations>

**Instructors access to student information**

Instructors have access to student information for any course they are teaching. Care must be taken to ensure that this information and any feedback on student performance such as student marks are kept private. The Provost’s office has prepared a checklist for instructors which can be found at:

[http://www.provost.utoronto.ca/Assets/Provost+Digital+Assets/Provost/Provost+Digital+Assets/Provost/fippa+Q$!26A+for+Faculty.pdf](http://www.provost.utoronto.ca/Assets/Provost%2BDigital%2BAssets/Provost/Provost%2BDigital%2BAssets/Provost/fippa%2BQ%24%2126A%2Bfor%2BFaculty.pdf)

Faculty members who are using innovative pedagogical methods or new educational software that has not been officially adopted by the university, are asked to consult with the Faculty Registrar or the Vice-Dean Undergraduate to ensure student privacy is respected.

**Contractors and external vendors**

When engaging a contractor or vendor to provide products or services, where possible no confidential information should be shared. Where this is not possible, only the information needed to complete the contracted work should be provided. The contractor/vendor must sign a confidentiality agreement before any confidential information is shared with the vendor.

For more information review:

Instructions for Third Party Confidentiality Agreements

[http://www.fippa.utoronto.ca/Assets/FIPPA+Digital+Assets/Instructions+for+Third+Party+Confidentiality+Agreements.pdf](http://www.fippa.utoronto.ca/Assets/FIPPA%2BDigital%2BAssets/Instructions%2Bfor%2BThird%2BParty%2BConfidentiality%2BAgreements.pdf)

Confidentiality Agreement template and checklist

[http://www.fippa.utoronto.ca/Assets/FIPPA+Digital+Assets/Confidentiality+Agreement+Template+and+Checklist.pdf](http://www.fippa.utoronto.ca/Assets/FIPPA%2BDigital%2BAssets/Confidentiality%2BAgreement%2BTemplate%2Band%2BChecklist.pdf)

**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 your manager. This should also be reported to the Faculty’s FIPPA Liaison, Tom Nault, 416-978-5894, tom@ecf.utoronto.ca. Consequences can best be controlled with quick intervention.