UNIVERSITY OF TORONTO

Privacy Policy (August 2015)

Information Technology Services
Office of the Chief Information Officer

Access to Information

Information Technology Services staff in the Office of the CIO work with confidential information. At the University, information that is not intended to be public is considered to be confidential. It is a key responsibility of staff to ensure that University confidential information is kept secure at all times and is only shared with individuals who need it for official University purposes.

One key type of confidential information is personal information, that is, information that may be used to identify an individual. Personal information is protected by the *Freedom of Information and Protection of Privacy Act*. Staff are only permitted to access, use or disclose personal information as required for the purpose for which the information was collected, or a consistent purpose, and to fulfil official University responsibilities. For most purposes, personal information may only be shared with the individual to whom it pertains, and with University faculty or staff who need the information for official University tasks or functions. Key exceptions are compelling health or safety concerns, emergencies, and consent of the individual.

Staff are required to protect personal and other confidential information at all times with effective security, as described in University policy and Information Security and Privacy Practices, including security requirements for personal information set out in:
http://www.provost.utoronto.ca/public/pdadc/2011_to_2012/2.htm

As an IT professional, it is your duty to protect information that falls within your purview. Please follow the practices set out below in relation to information management. Discuss any questions or concerns with your manager or director, or your direct report(s) as required.

Need-to-know sharing

Within the University, personal information should only be shared with individuals who need the information to carry out official University functions or duties. 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.

Electronic information

1. Electronic confidential information, including personal information (e.g., names; student numbers; contact, academic, or financial information) should not be stored on local devices (e.g. computer hard drive or USB key). It should be kept on secure University resources, such as ROSI, Blackboard, or private network drives. If local storage is necessary, including on your computer's 'C' drive or a printer/copier, all confidential information must be encrypted.

2. Confidential information cannot be taken off-site without official authorization. Information may be carried off-site for operational need or when there is no other reasonable way to complete a task. Only take confidential information out of its University setting if authorization was given by the University office or official responsible for the information. You also need operational need (e.g., an offsite activity), or no other reasonable way to complete the task (eg. work cannot be completed during work hours).

3. Mobile devices, including laptops, smartphones, tablets and other devices, which store confidential information, including student data and University email, must be encrypted. This requirement applies equally to University and personally-owned devices that are used for University work. Unencrypted personally-owned devices must never be used to access University email or other confidential University information.

4. Official University email is secure, and may be used for personal and other confidential information, when all senders and recipients are official University email addresses. Email sent from one UTOR account to another is considered secure. Non-institutional email is not a secure form of communication. Use of email to share personally identifiable information should be limited to cases when there are no reasonable alternatives, and information shared in this way should not include any confidential information.

5. If necessary, confidential information can be shared through the use of strongly encrypted attachments, where the passphrase is communicated to the recipient securely through a different channel.

6. Email containing personally identifiable information that is used for an official purpose should be kept for one year. Other email that is not operationally necessary should be deleted as soon as it is no longer required.

7. Centrally administered computers at the University, as a rule, have encrypted hard drives. Check with your IT staff to verify that your computer drive(s) is/are encrypted before using to store confidential information.

8. Set your computer to lock within five minutes if you are absent, so that it may only be accessed with your password.

9. Whenever possible, access University confidential information using virtual private network access approved by Information Technology Services. (See: http://vpn.utoronto.ca/)

10. Consult IT staff to ensure the secure destruction of confidential electronic records. When disposing of electronic assets such as desktop computers, laptops and mobile devices, ensure that the storage drives are properly destroyed so as to prevent any recovery of data.

Hard copy documents

1. As with electronic information, paper and other hard copy documents containing personal information are highly confidential. These should be kept in locked cabinets when you are not in the 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 cabinet.

2. Confidential information cannot be taken off-site without official authorization. Information may be carried off-site for operational need or when there is no other reasonable way to complete a task. Only take confidential information out of its University setting if authorization was given by the University office or official responsible for the information. You also need operational need (e.g., an offsite activity), or no other reasonable way to complete the task (eg. work cannot be completed during work hours).

3. Great care must be exercised in transporting paper documents outside the office. If you must take files home, take as few at a time as possible, take copies rather than originals, and ensure they are secured, and with you during transit. Any confidential and/or personal information that is taken home must be locked when not in use.

4. Always use a cross-cut shredder to destroy confidential paper and other hard copy records.

Clean desk policy

- When leaving your office, lock confidential documents in a cabinet or drawer, then lock your office door.

Parents and third parties

- Parents and other third parties may request student and other personal information. Privacy legislation explicitly prevents sharing any personally identifiable information with a third party unless the individual (e.g., the student) consents. Share student or other personally identifiable information outside the University only with consent of the individual to whom it pertains.

Emergency situations

- Disclose personally identifiable information to alleviate compelling circumstances affecting health or safety. Safety trumps privacy. Consult your superior if there is a health or safety concern. Follow the University's Emergency Disclosure Guideline available at: http://www.hrandequity.utoronto.ca/about-hr-equity/news/memo/2008_-_2009/Memo_2008-09_HR16.htm

Immediately report privacy problems

- If any personally identifiable information is mishandled, lost, or misplaced; e.g., a document, file, USB key, laptop, etc., report the loss immediately to the FIPPA office and your superior. Often, consequences may be minimized with quick intervention.

Acquaintance with students and other individuals

1. If a staff member knows or is related to a student or other individual, the staff member should immediately inform his or her supervisor and avoid any discussion of the student record, or other personal information or related matters, with the student or with others, pending direction from the supervisor.