UNIVERSITY OF TORONTO
DALLA LANA SCHOOL OF PUBLIC HEALTH

DALLA LANA SCHOOL OF PUBLIC HEALTH
PRIVACY POLICY

Access to Information

Faculty and staff at the Dalla Lana School of Public Health work with confidential information. At the University, Information which is not intended to be public is confidential. It is a key responsibility of faculty and 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 responsibilities.

One key type of confidential information is personal information, which is information about an identifiable individual. Personal information is protected by the *Freedom of Information and Protection of Privacy Act*. Faculty and 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.

Faculty and 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/Assets/Provost+Digital+Assets/Provost/fippa.pdf

Please follow the practices set out below. Discuss questions or concerns with your chair, manager or director, or direct report.

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 (eg. 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. 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 personal devices that are used for University work. Unencrypted personal devices must never be used to access University email or other confidential University information.

3. With the exception of internal email (from one UTOR address to another UTOR address), email is not a secure form of communication. Use of email to share personal information should be limited to cases when there are no reasonable alternatives, and information shared in this way should not include any confidential information.

4. 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.

5. Email containing personal 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.

6. Centrally administered computers at the University have generally been encrypted. Check with your IT staff to verify that your computer is encrypted before using it to store confidential information.

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

January 2017

8. Whenever possible, access University confidential information using virtual private network access approved by Division IT staff.

9. Consult IT staff to ensure the secure destruction of confidential electronic records.

Hard copy documents

1. As with electronic information, paper and other hard copy documents and files 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 the cabinet.

2. Confidential information cannot be taken offsite without official authorization and operational need or no other reasonable way to complete the 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 (eg. an offsite activity), or no other reasonable way to complete the task (eg. work cannot be completed during work hours).

3. Great care should 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 secure 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

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

Parents and third parties

1. Parents and other third parties may request student and other personal information. Privacy legislation explicitly prevents sharing any personal information with a third party unless the individual (e.g., the student) consents. Share student or other personal information outside the University only with consent of the individual to whom it pertains. The written consent must be kept for seven (7) years.

Emergency situations

1. Disclose personal 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; http://www.hrandequity.utoronto.ca/about-hr-equity/news/memo/2008_-_2009/Memo_2008-09_HR16.htm

Immediately report privacy problems

1. If any personal information is mishandled, lost, or misplaced; e.g., a document, file, USB key, laptop, etc., report it immediately to your manager/supervisor, the Chief Administrative Officer (CAO) who is the Faculty Freedom of Information Liaison (FOIL) and/or Freedom of Information and Protection of Privacy (FIPP) office. Often, consequences can be minimized with quick intervention.

Acquaintance with students and other individuals

1. If a faculty or staff member knows or is related to a student or other individual, the faculty or 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.