UNIVERSITY OF TORONTO FREEDOM OF INFORMATION & PROTECTION OF PRIVACY OFFICE

THREE KEY ACCESS AND PRIVACY PRINCIPLES

1. CREATE EXCELLENT, PROFESSIONAL RECORDS

- Records are needed for work and to demonstrate due diligence
- Most records are releasable under freedom of information

2. SHARE PERSONAL INFORMATION FOR SAFETY AND WORK

- Emergencies, health and safety trump privacy
- Personal information can also be shared:
    - For the purpose collected
    - Within the University on a need-to-know basis
    - With the consent of the individual to whom it relates

3. PROTECT PERSONAL INFORMATION: CREATION TO DESTRUCTION

- Encrypt electronic personal information outside secure University servers
- Lock up hard copy personal information
- Destroy personal information securely:
    - Cross cut shred paper records
    - Ask IT staff to destroy electronic records securely
- Notify immediately if you suspect a privacy problem

McMurrich Building, 12 Queen's Park Crescent West, Room 104, Toronto, ON, M5S 1A8 Canada
Tel: +1 416 946-7303 • Fax: +1 416 978-6657 • www.fippa.utoronto.ca

PROFESSIONAL RECORD KEEPING

1. RECORDS ARE DISCLOSED FOR MANY REASONS

- FIPPA, lawsuit, disgruntled individual, data breach, evolving expectations …
- Consider disclosure as you create records.
- What if the record were disclosed? What would be the effect on the University?

2. HOW TO CREATE RECORDS

- As you work, decide what to document for each task.
- Is a record required by law/policy, due diligence, evidence, history, etc.
- What content and how much detail should be recorded?
- Is the record complete for its purpose; all necessary facts, opinions, etc?
- Should anything be removed; irrelevant facts, opinions, etc?
- Create excellent, professional records.
- Keep official/permanent records, delete/shred transitory records.

3. EMAILS ARE RECORDS

- E-mails are copied, printed, forwarded, archived etc.
- Send professional emails.
- Replace unnecessary emails with a phone call if possible.

McMurrich Building, 12 Queen's Park Crescent West, Room 104, Toronto, ON, M5S 1A8 Canada
Tel: +1 416 946-7303 • Fax: +1 416 978-6657 • www.fippa.utoronto.ca

UNIVERSITY OF
TORONTO

Office of the Vice-President
Human Resources and Equity

Freedom of Information and
Protection of Privacy Office

Emergency Disclosure of Personal Information at the University of Toronto – A Guideline Published Jointly by the Freedom of Information and Protection and Privacy Office, and the Crisis Manager

The University of Toronto is committed to maintaining a community where students, academic and other staff, and members of the public can safely pursue the many opportunities that the University offers. This commitment to safety is met through the deployment of various resources such as Counselling Services, the Community Safety Office, Campus Police, the Student Crisis Response Program, residence deans, and many others.

The University of Toronto is covered by the *Freedom of Information and Protection of Privacy Act* ("*FIPPA*") and its health information custodians have responsibilities under the *Personal Health Information Protection Act* ("*PHIPA*"). The University takes steps to protect the privacy of personal information in accordance with these Acts.

In normal circumstances, disclosure of personal information is handled through **consent** (both express and implied) and, within the University, is **limited to those who need to know** the information in order to discharge their duties. Confidentiality is respected and the many University staff who handle personal information are well-informed, through the FOIPP office, training, existing policies and other means, regarding their responsibilities.

At times, the commitment to safety and the commitment to protection of privacy intersect. This intersection requires those having discretion and decision-making authority to exercise sound judgement regarding potential disclosure in the interests of safety. **In addition to the typical consent mechanisms or where otherwise legislatively authorized *FIPPA* permits disclosure of personal information in the University's custody and control "in compelling circumstances affecting the health or safety of an individual if upon disclosure thereof notification is mailed to the last known address of the individual to whom the information relates" (s. 42(1)(h). Personal information may also be disclosed "in compassionate circumstances, to facilitate contact with the spouse, a close relative or a friend of an individual who is injured, ill or deceased" (s. 42(1)(i).**

When a University employee (this term includes all faculty and staff) is faced with circumstances where the normal consent and other statutorily-permitted routes for disclosure are not available and where compelling health or safety interests are at stake or significant compassionate considerations are involved, the following procedures are to be followed:

- the employee is required to consult with the employee's supervisor (and, if the employee's supervisor does not have an administrative role, also with a relevant administrative or academic-administrative manager).
- Considering the nature of the issue and the obligations and freedoms under *FIPPA,* they are to assess jointly whether disclosure should be made.
- In cases of doubt, the reviewing employees are required to contact one of the following or their designates (current incumbents identified):
  - the Vice-Provost Students (Jill Matus);
  - the Vice-President Human Resources and Equity (Angela Hildyard);
  - the Director of the Freedom of Information and Protection of Privacy Office (Rafael Eskenazi);
  - or one of the University's internal legal counsel working in this area (Steve Moate or Nora Gillespie).
- In the case of UTM and UTSC the Vice-President and Principal and/or one of the above should be called.
- Wherever possible, a brief record of the disclosure decision should be maintained in a confidential file.
- The obligation to write, upon disclosure, to the individual to whom the information relates must be kept in mind.

As stated by the Information and Privacy Commissioner, "life trumps privacy" and this paramount principle must considered as a starting point in protecting health and safety as effectively as possible when making difficult judgement calls. Support in making the appropriate judgement calls will be facilitated by the wide variety of skilled resources available within the University.

March, 2009

University of Toronto

VICE PRESIDENT & PROVOST

FIPPA - GUIDELINE REGARDING SECURITY FOR PERSONAL AND OTHER CONFIDENTIAL INFORMATION

Personal and other confidential information should at all times be protected with effective security as described in University policy and Information Security and Privacy Practices.

Personal and other confidential information in electronic form should be kept in a secure server environment with appropriate restricted user rights. If it is outside a secure server environment, personal and other confidential information in electronic form must at all times be protected with properly implemented encryption.

Personal and other confidential information in hard copy form should be kept in a secure institutional environment. If it is outside a secure institutional environment, personal and other confidential information in hard copy form must at all times be protected with strong, effective security measures.

June 2011

www.provost.utoronto.ca | Contacts | University Switchboard: (416) 978-2011
University of Toronto, 27 King's College Circle, Toronto, Ontario, Canada M5S 1A1

Security Reminder for Working Offsite

If working offsite, follow security requirements for confidential information. All information that is not officially designated as public is confidential, including information about identifiable individuals, student records, grades, human resources records, non-public financial information etc.

Do not take confidential information offsite (e.g. home for work) unless you have:

Official Authorization; official University, Division or department policy or practice that permits the record to be taken out. If there is any doubt, consult with your direct report.

Demonstrable operational need/No other reasonable means; the record must be taken offsite to fulfil your duties. There is no reasonable alternative to taking the record offsite.

For hard copy records, minimize risk as follows:

Take as few records as you can for expected work. If possible, take copies, not originals.

In transit; Carry records in a locked satchel or case. Do not leave records unattended, e.g. at restaurants, washrooms, public transit, etc. Don't read where others could see records.

At home; Protect records from unauthorized individuals, including family or friends. Lock records away when not in use, e.g. locked cabinet in your locked home.

For electronic records:

Access records remotely only on authorized, secure networks with encrypted communication.

Use a strong password to protect your electronic devices and laptop.

Be sure your computer has up-to-date security, including firewall, anti-virus and anti-spam.

Electronic records taken out of a secure University IT environment should be encrypted at all times, e.g. use an encrypted USB memory stick or encrypted hard drive on your laptop.

Resources:

University of Toronto Security for Personal and Other Confidential Information practice:
http://www.provost.utoronto.ca/Assets/Provost+Digital+Assets/Provost/fippa.pdf

University of Toronto Encryption resources:
http://encrypt.utoronto.ca/

For questions, contact Howard Jones, Coordinator, FIPP Office at (416) 946-7303, howard.jones@utoronto.ca