



PRIVACY BASICS FOR NEW FACULTY AND STAFF

The University follows the *Freedom of Information and Protection of Privacy Act (FIPPA)* which:

1. Regulates how personal information* is handled to protect privacy
2. Permits public requests and access to University-held records

Key Privacy Rules:

1. Responsibility for privacy protection is shared by all who work at the University
2. Only collect personal information that you need for official University purposes
3. Only use or disclose personal information as necessary:
 - a) In emergencies, or to reduce threats to health or safety, or
 - b) For the purpose information was collected or a consistent purpose, or
 - c) With the individual's documented consent, or
 - d) To others working for the University, but only on a need-to-know basis
4. Keep all personal information in secure resources provisioned or approved by University IT services
5. Keep hard copy personal information in a locked cabinet in a locked non-public room
6. Avoid inadvertent exposure of personal information at work, home, transit and elsewhere
7. Destroy securely. Crosscut shred paper records; have IT staff destroy electronic records
8. Immediately notify your supervisor, FOIL** or the FIPP Office of any privacy concern
 - If you have questions, ASK your supervisor, FOIL, or the FIPP Office as soon as possible
 - Create excellent records – disclosure may be required, through FIPPA or other processes

For more information, consult FIPPA resources at <http://www.provost.utoronto.ca/policy.htm>

- FIPPA, Q and As for Instructors
- FIPPA - General and Administrative Access and Privacy Practices
- Guideline Regarding Security for Personal and Other Confidential Information

* “personal information” is information about an identifiable individual

** Each division has a Freedom of Information Liaison (FOIL) as part of its administrative staff