FREEDOM OF INFORMATION & PROTECTION OF PRIVACY OFFICE

# Access and Privacy Tip Sheet

**Purpose and Objective**

These basic access and privacy tips address most situations but do not set out all legal or practice requirements. Detailed privacy guidance on collection, use, disclosure and secure destruction is set out in the General and Administrative Access and Privacy Practices Guideline. Contact your Divisional Freedom of Information Liaison (FOIL) or the FIPP Office for specific guidance.

**Privacy Tips**

1. Only collect, use or disclose personal information necessary for official University work.
2. Only share personal information with the individual to whom it pertains, or with University officers, employees, agents or contractors who need it for official University work.
3. If you have any doubt about disclosing personal information, check with your manager, FOIL or the FIPP Office or obtain fully-informed, voluntary consent from the individual.
4. When possible, avoid emailing or faxing personal information or leaving it on voice mail.
5. Retain personal information for at least one year after the date of its last use.
6. Always use strong, effective security measures, including; keeping a clean desk, locking cabinets, using strong passwords, and encrypting attachments with personal information.
7. Prevent loss, theft or exposure; do not leave personal information in a vehicle, do not use unauthorized systems (ie. Gmail) or other unapproved services/apps for University work.
8. Securely destroy personal information; cross-cut shred hard copy records promptly.
9. Protect privacy in all contexts, including meetings, work and social conversations.
10. Do not leave documents on a fax machine, photocopier, or printer.
11. Conduct an IRRM to ensure new technologies, information systems etc. meet requirements.
12. Build privacy protection into contracts with third party service providers.
13. Report possible or suspected privacy issues to your supervisor immediately.
14. Collect, use, or disclose only as the personal information needed for your task and no more.

UNIVERSITY OF TORONTO

FREEDOM OF INFORMATION & PROTECTION OF PRIVACY OFFICE

**Access/Records Management Tips**

1. Access legislation covers all records, including drafts, e-mails, and handwritten notes.
2. Always consider possible future disclosure when creating records.
3. Only create the right records that are needed for –and defined by– business purposes.
4. Be thoughtful when creating records. Include all necessary information, but never unnecessary editorial comments.
5. Your email account is not intended to be a permanent repository. Save copies of institutional emails in the appropriate directory of your team's shared network drive or Sharepoint site, and routinely delete transitory email records.
6. Follow office and University records management and retention standards.
7. Clearly designate responsibility for shared records to avoid duplication and confusion.
8. Use Office365 sharing functionality instead of attaching copies of records to emails where feasible to limit duplication and retain control of your office's records.
9. Always do the following for records that you are responsible for:
   a. Store securely,
   b. Know the record status – draft, final, official version for circulation, etc.,
   c. Limit access strictly to those with a need to know for official work purposes.
   d. Promptly dispose of transitory records like unnecessary copies and superseded versions.