Office Privacy Guidelines

Office Privacy Policies

- Offices that handle personal or other confidential information must have documented policies and procedures for privacy, including security, so faculty and staff demonstrably follow proper practice.
- Enrolment Services shares its privacy policy, for your use: www.fippa.utoronto.ca/privacytuneup/resources
- If you prefer, the FIPP Office will help you to develop your own privacy policy.
- The FIPP Office can support your privacy policy by providing training for faculty and staff.
- Your privacy policy should support the work of your office while protecting privacy.
- Make your policy clear and ensure that all faculty and staff understand and follow it.
- If possible, incorporate privacy in existing policies rather than creating a new policy for privacy.

The following are essential elements to address in your office privacy policy:

Identify which information is public and which is confidential

- Information is treated as confidential unless it has been specifically designated as public.
- Personal information (about an identifiable individual) is an important type of confidential information.

Sharing and disclosure of personal information

- Personal information must be shared to remedy compelling health or safety risks.

- Personal information can only be used or disclosed for the purposes for which it was collected.
- Personal information can be shared within the University, but only on a need-to-know basis.

Indicate which confidential information can be taken offsite, and under what circumstances

- Only with official authorization, operational need and no other reasonable means to do the task.

Security for confidential records at University locations and offsite

- Encrypt electronic records outside a secure institutional server.
- Maintain two layers of lockdown for unattended hard copy records.
- Secure unattended confidential records from unauthorized individuals when you are not present.
- Keep confidential records secure offsite and in transit.

Communication of confidential information

- UTOR to UTOR email is secure for confidential information. Other email generally is not.

Secure destruction of confidential information

- Confidential information must be irretrievably destroyed at the end of its useful life.
- Crosscut shred paper records and ask IT staff for guidance on electronic record destruction.

Immediate reporting requirements for privacy breaches

- Report privacy issues, such as mishandling of personal information to your supervisor right away.
- If in doubt, report. Always err on the side of over-reporting so that no incidents are missed.