Privacy Tune-up Fact Sheet

Recently, Internal Audit and the FIPP Office, surveyed University Units to assess privacy practice, and identified by audit a need for action in five areas:

---

1. Office Privacy Policies

Units that handle confidential information must have operational privacy policies.

The FIPP Office will provide a checklist, template and model privacy policy.
We can help you to customize the model policy for your needs or to develop your own.

---

2. Personal information sharing and disclosure
3. Security and destruction of electronic records
4. Privacy breach response

These are key elements of office privacy policies, privacy training, and University privacy policy.

FIPP Office training for faculty and staff covers these and other key privacy topics.

---

5. Third-Party confidentiality agreements

Confidentiality agreements are required to share confidential information with external parties.

The FIPP Office provides a checklist, template and model confidentiality agreement.
We can help you to draft confidentiality agreements for consultants or agents.

Key to the Privacy Tune-up are accurate identification of units that need privacy policies or confidentiality agreements, and up-to-date privacy training. To help with these, we ask that you:

- Identify units that handle confidential information and do not have privacy policies.
- Identify units which may need privacy training or a refresh (see attached training history).
- Promulgate the requirement for third party confidentiality agreements within your Division.
- Identify offices/units in your Division which need privacy policies or confidentiality agreements.
- Extend privacy training invitations to Academic Chairs and their staff.

The FIPP Office will deliver training, and assist as requested with policies and agreements.

Checklists and templates for privacy policies, confidentiality agreements and training materials
are posted at: www.fippa.utoronto.ca/privacytuneup/resources