Privacy Policy Template and Checklist

Use this template and the Enrolment Services sample to draft your office privacy policy. Remember to also address unique/particular needs of your office not listed below:

CHECKLIST

1. **Identify information as public or confidential and describe confidential information**
   Information is confidential unless it has been specifically designated as public.
   Personal information (information about identifiable individuals) is protected by law.

2. **Explain what staff/faculty may do with confidential information**
   Only use confidential information for your work and for purposes for which it was collected.
   Confidential information can only be shared within the University on a need-to-know basis.

3. **If any confidential information can be taken offsite, indicate how and when**
   Confidential information can only be taken offsite with:
   a. official authorization,
   b. operational need, and
   c. no other reasonable means to do the task.

4. **Specify required security for confidential records at University locations and offsite**
   Records taken offsite must be secured at least as well as records at the University, including:
   a. Encrypt electronic records outside a secure institutional server.
   b. Use two layers of locks for hard copy records. (eg. locked cabinet in a locked room)
   c. Secure confidential records if you are not present, offsite, and in transit.

5. **Communicate confidential information securely**
   UTOR to UTOR email is secure for confidential information.
   Other email generally requires encryption of attachments to be secure.

6. **Destroy confidential information securely**
   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.

7. **Report privacy breaches immediately**
   Immediately report privacy issues/breaches, such as mishandling/loss of personal information.
   If in doubt, report: Always err on the side of over-reporting so that no incidents are missed.

8. **Other considerations**
   List and address all unique needs of your program/unit.

TEMPLATE

This template contains operational privacy guidelines that you can customize for your unit. It is intended to be used with the Checklist. Also refer to the Enrolment Services Privacy Guidelines.

Use these resources in preparing your own privacy guidelines or policy. Contact the Freedom of Information and Protection of Privacy Office for assistance drafting your guidelines/policies.

1. **Identify information as public or confidential and describe confidential information**

The Unit accesses/holds [describe information] which is confidential.
The following [describe information] is also personal information.

2. **Explain what staff/faculty may do with confidential information**

Faculty/staff may [describe permitted tasks/activities] with the information.

3. **If any confidential information can be taken offsite, indicate how and when**

No confidential information may be taken offsite.
--- or ---
The following [describe information] may be taken offsite with the approval of [official].

4. **Specify required security for confidential records at University locations and offsite**

Confidential information must at all times be protected from unauthorized access/viewing.
Electronic confidential records offsite must be encrypted and not left unattended while open.
Hard copy confidential records offsite must be kept in a locked cabinet at your home.

5. **Communicate confidential information securely**

Confidential information may only be communicated between UTOR email accounts.
--- or ---
Confidential information may be sent to non-UTOR email accounts as encrypted attachments.

6. **Destroy confidential information securely**

Hard copy confidential records must be destroyed with cross-cut shredding.
--- and/or ---
Hard copy confidential records may be placed in a [company X] shredding box for destruction.
Optical confidential records must be destroyed with cross-cut shredding.
Electronic confidential records may be destroyed by erasure from a University server.
Electronic confidential records may be destroyed by University IT staff.

7. **Report privacy breaches immediately**

Immediately notify [official] of any data loss/theft, breach, privacy issue.

8. **Other considerations**

Every University unit/office has its own particular circumstances.
Be sure to include all security and privacy protections necessary for your situation.