Fact Sheet

Retention and Disposal of Personal Information

Many departments at Queen’s collect and retain personal information. Following responsible, secure procedures for retention and disposal of personal information is not just good practice, it’s the law. Ontario’s Freedom of Information and Protection of Privacy Act (“FIPPA”) governs all aspects of the lifecycle of personal information. This fact sheet explains FIPPA’s requirements for retention and disposal.

What is Personal Information?

Personal information is anything that can be used to identify someone, including their:

- race, national or ethnic origin, colour, religion, age, sex, sexual orientation, marital status
- educational, medical, psychiatric, psychological, criminal, or employment history
- financial transactions
- name, address, telephone number, fingerprints, or blood type
- identifying number (SIN, student ID, employment ID), symbol, or other particular assigned to them
- personal opinions or views
- correspondence that is confidential, even if only implicitly
- another’s views or opinions about them
- pictures, audio, or video recordings of them
- anything else that could be used to identify them

What is a Record?

A record is anything that can be read, viewed, or listened to at a later date, however made, including:

- anything on paper (written, typed, printed, drawn, etc.)
- email, and all digital files
- any audio or video recording
- any duplicates of a record (older versions, or photocopies/scans for office use)

Quick Facts

a) Minimum retention periods:
   - Cassette tapes: 45 days
   - Everything else: 1 year
b) Appropriate disposal:
   - Only use the approved shredding service from Queen’s Procurement
c) Record of disposal:
   - Complete and retain a copy of the Authorization for Destruction of Records form

Personal information is NOT:

- information about someone who has been deceased for more than 30 years
- information about a corporation
- a name, title, or contact information that identifies someone in their business, professional, or official capacity, even if they conduct their business from home
Retention

Security and Confidentiality
When deciding the degree of security necessary to ensure the safety of personal information, consider the:

- type and amount of personal information your office retains and stores
- number of people with access
- consequences of a privacy breach, both to the individual and the University

Three Types of Security Measures

1. Physical Security
   - Locks on doors and file cabinets
   - Computer screens not viewable by passers-by
   - Secure fax machines and printers

2. Procedural Security
   - Regularly change codes, passwords
   - Controlled distribution of keys
   - File check-out procedures
   - Use a “shred by” date-stamp for duplicates

3. Digital Security
   - Encrypt mobile devices such as cellphones, USB keys, tablets, laptops, and external hard drives with personal information on them
   - Encrypt files before attaching them to email

Minimum Retention

All personal information must be kept for at least 1 year after its last use. Personal information stored on audio or video cassette tapes, however, need only be kept for 45 days after its last use.

These are minimum retention timelines; there are any number of other reasons that your office should be keeping records for longer. Consult the Records Retention Schedules for the retention that matches your records.

Disposal

Once it has reached the end of its lifecycle, personal information may be disposed of. Records, including records containing personal information, can only be disposed of in accordance with an authorized records retention schedule. Records will either be destroyed, or transferred to the University Archives.

Transferring Records to the University Archives
Some records will be placed in the University Archives on a permanent basis. To transfer records, contact the University Archives.

Destroying Records
Most records will be destroyed when they reach the end of their lifecycle. Be sure to follow the approved destruction methods when destroying or deleting records, especially records containing personal information.
Transitory Records

Not every document containing personal information is considered an official record. Many are transitory records and can be securely disposed of without a record of disposal. See the Fact Sheet on Transitory Records.

Approved Destruction Methods

Paper Records
- Do NOT use a shredder designed for home-use
- Make sure you are using the approved shredding service from Queen’s Procurement
- Ensure that files are stored in a secure place before they are collected for shredding

Video & Audio Cassettes
- Record over, or
- Consult the Privacy Officer to identify an alternate method that meets FIPPA’s technical requirements

Digital Records
Simply deleting files before disposing of a computer is insufficient since forensic software can retrieve information on hard drives, including personal information; instead:
- Dispose of hard drives, and other digital media through IT Services
- Do NOT simply reformat a hard drive, as forensic software can still retrieve personal information

Record of Disposal

FIPPA requires documentation when records containing personal information are disposed of. Queen’s Records Management has developed the following forms:
- For destruction, complete the Authorization for Destruction of Records form.
- For transfer to Queen’s Archives, complete the Records Transfer to Archives form.

Remember...

Care must be taken either when transferring or destroying personal information to ensure its security and confidentiality during handling and transit. This means ensuring that records can’t be reconstructed after they’ve been destroyed.