Fact Sheet

Storing University Records

Records Management and Privacy Office
Kingston, ON K7L 3N6
Tel. (613) 533-6095
access.privacy@queensu.ca

We all create and receive records to support the work we do. These records might be used and disposed of relatively quickly, or they might remain active and in use for a long time. If the records have no ongoing operational value, they may be considered transitory and can be destroyed or deleted as soon as they have served their operational purpose (see the Fact Sheet on Transitory Records). For all other records, they should be governed by an authorized records retention schedule which sets out the timeframe for keeping the records before they are eligible to be destroyed or transferred to the University Archives for permanent preservation.

Sometimes records must be retained for several years after their active period of use for regulatory, legal, audit or reference purposes. Throughout this semi-active or inactive period, the records remain the responsibility of the unit that created or received them, and the unit must ensure that the records remain readable for the entire retention period—whether that retention period is a year or one hundred years.

This fact sheet sets out some considerations for the proper storage of university records such that they will retain their accessibility, integrity and readability for as long as necessary.

How to store electronic records

Electronic records are records that require a device or technology for their transmission or processing. Most records we encounter today are digital; such records include those created using office productivity tools such as MS Word documents and Excel spreadsheets. Electronic records also include audio and video recordings. Both **hardware and software concerns** need to be considered when storing electronic records.

The media on which electronic records are written (tape, disks, etc.) can degrade if not stored under proper environmental conditions, free from pests and fluctuations in humidity. In addition, the devices used to read the records may no longer be available after a period of time. VCRs and cassette players are becoming scarce, and most laptops no longer have a built-in CD/DVD drive, let alone the ability to read a floppy disk.

Obsolescence in software is also problematic. Many popular software programs that were once ubiquitous no longer exist, making records stored in such programs virtually useless.

Research Data

Research data belong to the researcher, not to the University. Research data are not defined as "university records" under the Queen's University Records Management Policy.

Nevertheless, retention periods may be determined by other authorities. For example, the Senate Policy on Integrity in Research requires research data to be preserved for at least 5 years after the research is published, and Health Canada requires clinical trials data to be kept for 25 years.

In addition, researchers may want to retain their data for their own purposes for a long period of time.

Researchers may find this fact sheet useful in deciding how best to store their data. In addition, see Queen's University Library's guide on Research Data Management.

It may be tempting to copy digital records to an external hard drive, a USB drive, a laptop, or some other sort of removable media, off the Queen's network to free up space or in the belief that the records will be safer. However, it's much safer to keep the records on the university network. Not only are removable media prone to being stolen or lost, but the records on the network will be managed and migrated through software and hardware updates with the assistance of knowledgeable IT staff. If necessary, the records can be stored in a separate directory with appropriate access permissions.

Some specialized electronic records in analogue format may require assistance from technical experts. Consult the Records Management and Privacy Office for further guidance.

Thinking of the cloud?

If university records are being stored in the cloud, be sure that a proper security and privacy risk assessment has been conducted on the vendor and its service. The responsible university unit continues to be accountable for its records even if they are in the custody of a third-party provider. Contact the Information Security Office for further information.

How to store hardcopy records

Hardcopy records are much less vulnerable to loss over time than are electronic records because they can be read by the human eye and so they don't require the maintenance of a device or other kind of technical apparatus. Records could be placed in a box and tucked away for a hundred years and still be perfectly legible. Yet, hardcopy records exist on a medium—usually paper—which can degrade or suffer loss or damage if not properly managed. Rodents and other pests can feast on paper or use it to pad their homes; flood and fire can damage or destroy paper; and extremes in humidity may cause inks to run and paper clips to rust, thus making records difficult to read.

It may be tempting to get inactive records out of valuable office space by squirrelling them away in a basement or a back cupboard and forgetting about them. However, such locations may not be secure for confidential records, and it's likely that years in the future, the person who put the records there will be long gone and then someone will have to be given the difficult task of sorting out what the records are and what to do with them.

Find a suitable location for the storage of hardcopy records where they are managed. If they have a high reference value, it may make sense to scan the records and destroy the originals. See the Fact Sheet on Scanning University Records for guidance. Alternatively, if it is anticipated that records will have little need to be accessed during the retention period, then sending them to the University's secure offsite storage provider may be the most sensible option.

The bottom line

University records are an asset that must be managed like any other asset. Further guidance on managing University Records can be found on the Records Management and Privacy Office website.