

## Storage and Disposal of Records at Home – Best Practices

When working remotely, it is important that all employees continue to follow proper practices for the storage and disposal of records, particularly for paper records that contain confidential information, such as personal data or donation information.

When considering whether a record should be retained or destroyed, remember that [Transitory records](#) should be reviewed regularly for destruction. All other records are subject to the disposition plans outlined within the Queen's University [Records Retention Schedules](#).

Please refer to these best practices for the storage and disposal of records when working in a remote environment.

### Paper Records

- Wherever possible, avoid creating paper records and copies in favour of electronic records saved within the secure Queen's University environment.
- Paper records should be stored in a secure location when not in use, such as out of sight in a drawer or in a locked filing cabinet.
- If the document is to be destroyed, determine if it includes any confidential or proprietary information.
  - If it does not include such information, the document may be recycled.
  - If it does include confidential information, it must be shredded using a cross-cutting shredder.
- If you do not have access to a shredder at home, return all confidential documents to campus and place them in the Iron Mountain secure shredding boxes.
- For documents that are to be retained, please return them to campus for proper storage.
- Any documents that are to be returned to campus for storage or destruction must be stored securely until you can visit campus.

### Electronic Records

- To protect electronic records, ensure your computer is password protected and always lock it when you are not using it.
- To ensure the security and accessibility of records, avoid saving them to your desktop, local hard drive (H:\), or One Drive. Instead, store records on the shared drive (I:\).
- If you have confidential or proprietary information stored on your local hard drive that is eligible for destruction, delete it when finished using it and empty your computer's recycling/trash bin.

For further guidance, please refer to the Records Management and Privacy Office's [Working Remotely: Access to Information, Protection of Privacy, and Records Management](#).

For any questions, concerns, or assistance with the Records Retention Schedules, please contact Advancement Data Governance and Data Quality via [e-mail](#).