CORPORATE ARCHIVES & RECORDS

Working from Home with Records

These instructions curated from IT Security, Corporate Records and Archives, and the Privacy Office will ensure your at-home workplace is safe and secure.

Electronic Records

- Be extra vigilant for phishing attempts, and malicious websites.
- Ensure your computer, and mobile devices stay current with software updates.
- Use an antivirus product to protect your device.
- Know where your files are stored. Files stored on a local home PC are not backed up.
- Whenever possible, use:
    - 'CUNAS' Network Drives (W:, V:, P: etc.)
    - Microsoft OneDrive
    - Microsoft Teams
- Use a secured wireless connection at home.
- Lock your screen if you are in a shared space.
- Report any lost or stolen devices immediately to Campus Safety Services: www.carleton.ca/safety.
- Please visit the ITS Security website www.carleton.ca/its/security for further details, including examples of phishing messages that have been reported.

Hard Copy Files

Certain procedures should be followed to properly track all materials being taken off-campus if you have no choice but to take hard copy files home.

- Keep a detailed list of files removed from campus, who is holding them, and when they are returned to campus. Assign an administrator to act as custodian of the file list and follow up with staff on their hard copy files.
- When not in use, close your files and keep them in one location. If it is not possible to place them in a secure filing cabinet or drawer, place in clean, clearly labelled boxes.
- Do **NOT** under any circumstances place files in recycling or garbage bins for regular, municipal pick-up. Any files that require destruction must be packed and stored in a clearly labelled box until they can be returned to campus and placed in shredding boxes. Contact Corporate Records and Archives directly for questions about retention and destruction of records.
- If using a personal scanner and computer to digitize any hard copy files, ensure that you transfer the digital files to the appropriate retention site: Carleton network drive, OneDrive, or MS Teams for secure storage.
- Once you have scanned the file, ensure that you completely delete the scanned image from your computer and the cache of your scanner, if applicable.
- When transporting records, do not leave them unattended in your car. Move them directly from home to university office.

Carleton University

Working with Confidential and Personal Information

Remember to consider your confidentiality obligations towards the university. If you work with confidential or personal information, make sure you work in a private setting.

For more questions or concerns about securing and working with university records from home, contact:

IT Security
www.carleton.ca/its/security
IT Service Desk: 613-520-3700

Privacy Office
www.carleton.ca/privacy
University_Privacy_Office@carleton.ca
613-520-2600, ext. 2047

Corporate Records and Archives
www.carleton.ca/records
corporate.archives@carleton.ca
613-520-2600, ext. 5097

For more information about information and record management at Carleton University, consult the following university policies:

- Access to Information and Privacy
- Corporate Records and Archives Policy
- Data and Information Classification and Protection
- Mobile Technology Security

Carleton
University