UNIVERSITY OF THE FRASER VALLEY

Privacy and Records Management for Remote Work

This document is a follow-up to information provided online about UFV's remote working resources. We wish to remind employees of their obligations under BC's Freedom and Information and Protection of Privacy Act (FIPPA) to keep all personal information that is in their custody or under their control safe and secure (this refers to information relating to students, employees, and other individuals with whom UFV interacts). The tips below will help ensure employees working from home are supported in protecting others' personal and sensitive information and maintaining good records and information practices.

Confidentiality, Privacy & Records

- Be mindful of where information is stored by ensuring records are not left unattended. When working remotely, records should be kept under the constant control of the employee, including during meals and other breaks. If this is not possible, the records should be temporarily stored in a secure location, such as a locked room or desk drawer.
- Take extra precautions to safeguard information that contains personal identifiers, confidential matter, or hard copy documents. Electronic records containing personal information should be transported by an encrypted storage device. USB, external hard drives, and computers (Mac and Windows) can all be easily encrypted. Even your home devices can and should be encrypted for your own protection.
- Employees should only remove records containing personal information from the office when it is absolutely necessary for the purposes of carrying out their job duties. If possible, only copies should be removed, with the originals left in the office. Copies are considered transitory records and can be destroyed securely on campus when the employee returns to campus.
- Laptops and other devices should be kept under the constant control of the employee while in transit. When an employee travels by car, the device should never be left unattended, even when locked in the trunk for a short period of time. Always keep devices on your person when in transit.
- When working away from your primary workstation, a laptop or home computer should be locked, logged off, or shut down when not in use. To the maximum extent possible, the employee should maintain constant control of the laptop, particularly when working at locations outside the office other than home. If this is not possible, it should be temporarily stored in a secure location, such as a locked room or desk drawer.
- There may be some documents that employees will not be permitted to take out of the departmental office due to privacy/confidentiality concerns. Consult with your immediate supervisor.
- When using a home computer that is shared with others in the household, ensure that you limit access to files containing personal information or confidential business information through the use of individual profiles (logins) per person. Keep passwords secure.
- Avoid the use personal email for any UFV work communication, but particularly as a means to transfer records containing personal or confidential information for work purposes.
- Conduct telephone calls to discuss employment or other matters involving personal information or confidential business information in private and outside the earshot of others.

Records Maintenance & Remote Access

- Use UFV’s network shared drive to store and access records when possible. For more information on accessing shared drives remotely, visit UFV ITS.
- If your department is using Microsoft Teams or other chat platforms, you could be creating and storing records. Notes, minutes, and files created and stored within chat platforms are subject to records management practices. Ensure transitory records are appropriately destroyed when no longer useful.
- If you are using a personal device for work-related business, you are still generating UFV records that must be maintained according to normal records retention practices. Ensure records created on a personal device are saved and stored on UFV’s network once complete. Delete records from your personal device once they are appropriately saved.
- University records that are to be disposed of in the course of the employee’s work should be destroyed on site at UFV. Ensure records are safeguarded until they can be safely returned to campus for disposal.
- Keep records organized by making time to routinely manage your e-mail inbox. For tips on managing e-mail as records, click here.

For more information or inquiries regarding records, contact Records Management.