Privacy Guidelines for Working Remotely

Last updated: May 4, 2020 (version1.1)

Purpose and scope

As a result of the COVID-19 pandemic, SFU is supporting its employees in working remotely from home. Working from home will often require employees to access or use personal information about students, staff, faculty, alumni, donors or other individuals. This guideline provides some useful do’s and don’ts to ensure the University’s privacy obligations under the Freedom of Information and Protection of Privacy Act are upheld while employees work off campus.

Physical Records

- Only remove information from the office that is essential to carry out your job duties.
- Check to see if you need your supervisor’s approval before removing records from the office.
- If possible, take copies of physical records and leave the originals in the office.
- Paper records should be securely packaged and kept under the constant control of the employee while in transit.
- Do not leave records unattended in a public location, including your parked vehicle.
- At home, store physical records in a locked filing cabinet or desk drawer to which you have sole access.
- Upon returning to the office, return records to their original storage place as soon as possible and destroy copies securely using the shredding services managed by SFU.

Information Security

- Do not use personal cloud storage (Google Drive, Dropbox, iCloud, etc.) to store SFU records.
- Make use of SFU’s enterprise-wide license for Zoom when video conferencing and connecting with co-workers.
- Access personal information through the secure use of the IT Services’ supported systems rather than by saving such information to mobile storage devices, where it is prone to loss or theft or other unauthorized access.
- Consider installing a privacy screen filter on your laptop screen monitor when working outside the office.
- Keep software up-to-date.
- Do not use personal email accounts as a means of transferring personal information or for composing and receiving work-related emails.
• Before sending an email, ensure you’re sending it to the correct recipient, particularly for emails involving large amounts of personal data or sensitive personal data.

• When accessing enterprise-wide or department-specific systems, you should be sure to:
  o log off the system or shut down computers when not in use;
  o refrain from accessing systems through unsecured wi-fi networks;
  o set an automatic logoff to run after a minimum period of idleness; and
  o do not share the password for a system or computer with any other person, including coworkers.

• Do not save any files containing personal information to your home or personal computers.

• Familiarize yourself with the privacy guidelines and policies available on the Archives’ website and in the University’s Policy Gazette.

Mobile Storage Devices

• All mobile storage devices that are used to store personal information, including laptops, flash drivers, external hard drives, smart phones and other such technologies, must be protected at all times through the use of a secure password and encryption.

• Be conscious that mobile storage devices can be easily lost, stolen or misplaced. The storage of personal information on such devices therefore gives rise to an increased risk of unauthorized access to personal information.

• Mobile storage devices must be kept physically secure at all times. Never leave them unattended in public locations, such as a parked vehicle.

• Mobile storage devices should ordinarily be kept in your physical possession, and when not directly in your possession, should be stored in a secure location (e.g. locked office or drawer in your home) access to which is limited to you and not to other members of your household.

• Mobile storage devices containing personal information should not be shared with others, including family members or friends.

• All files containing personal information that are saved to a mobile storage device should be encrypted.

• Files containing personal information should be securely and permanently deleted from a mobile storage device once the business purpose has been satisfied.

• You should refrain from viewing personal information on a mobile storage device within public places, but if it is necessary to do so, you should ensure that the information cannot be viewed by other individuals.

Sources

This guideline drew on several existing resources, including guidance documents issued by the Office of the Information and Privacy Commissioner of British Columbia, the University of Toronto’s COVID19 Temporary Special Telecommuting Work Arrangements Guideline, and BCIT’s Working Away from the Office Template.