BCIT Information Access & Privacy Office

Protecting Personal & Confidential Information Away From Office

Whenever information relating to BCIT business is used outside of the office or the classroom, there is an increased risk of loss or compromise. Under the provisions of FIPPA, all employees are responsible for the safe and secure handling of all BCIT records and information taken off-site or accessed from the off-site location, including but not limited to electronic files saved on home computers.

Physical Records

- Only remove information from the office that is essential to carry out your job duties.
- If possible, take copies of physical records and leave the originals in the office.
- Paper records should be securely packaged, carried in a locked briefcase or sealed box, and kept under the constant control of the employee while in transit.
- Store physical records in a locked filing cabinet or desk drawer that you have sole access to.
- 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 BCIT.

Privacy Safeguards at Home

- Do not leave your laptop screen unattended, lock your screen or logoff each session.
- Do not share a laptop or computer used for work with family members and/or friends.
- Personal or confidential business information should not be discussed in spaces that may include other members of your household.
- Do not use personal email as a means to transfer information for work purposes.
- Never transmit SIN numbers or credit card information via email.
- When using video conferencing:
  - If recording, all participants must be notified of the purpose of recording and consent to the stated purpose(s) before recording the meeting.
  - Any personal or confidential business information must be removed from view when using camera view or screen sharing.
  - Cameras and microphones should be turned off when not in use.
  - Only disclose information that is necessary to conduct and/or participate in the video conference.
- Securely remove all BCIT information from a personal computer once no longer needed.
- BCIT may collect personal information such as your home address and personal cell or phone numbers to approve an application to work from home and to manage the employee relationship. *This information must be shared on a need-to-know basis only*. Consent is required to release such information to other faculty or staff members.

Data or Privacy Breach

A data or privacy breach occurs when personal or confidential information is: inappropriately used or disclosed, information is lost, stolen, or information is accessed without a legitimate work purpose. BCIT employees must **immediately** report a suspected breach, including loss or theft of BCIT devices **by both:**

1. Notifying their supervisor or manager, **AND**
2. Reporting the incident to:
   - **Information, Access and Privacy Office** (IAPO) : email: **privacy@bcit.ca**; or
   - Notifying the **IT Service Desk** at 604-412-7444, Option 1 or email **techhelp@bcit.ca.**

IAPO or Cyber Security will advise what next steps should be taken.

BCIT Information Access & Privacy Office

Protecting Personal & Confidential Information Away From Office

Working Remotely and Securely

At BCIT, we all have a shared responsibility to protect personal and confidential information about students, faculty, staff, alumni, and donors. By taking a few simple steps to stay secure, we all can make an impact on privacy and information security. BCIT employees are reminded that all BCIT policies and procedures must be followed regardless of their working location.

These polices include but are not limited to:

- 3502 Information Security
- 3501 Acceptable Use of Information Technology
- 6700 Freedom of Information & Protection of Privacy
- 1500 Code of Conduct
- 7100 Safety and Security

Information Security Guidelines

- When connecting to BCIT resources outside the office, use a VPN connection ("Access Anywhere" is installed on BCIT laptops but must be user activated).
- Ensure that your home computer is running an up-to-date operating system, and that any vendor-recommended updates are applied. Your web browsers and other software should also be updated.
- Encrypt any electronic device that you use to store BCIT personal or confidential business information. This includes, but is not limited to, home computers, USB flash sticks, and laptops.
- Do not accept software updates that are triggered from a website or email, such as Java or Adobe Flash.
- Do not use your personal cloud storage (Google Drive, Dropbox, iCloud, etc.) to store BCIT documents.
- Store electronic device(s) in a secure location when transporting or travelling (e.g. trunk of a car).
- Make use of BCIT delivered video conferencing and collaboration using Zoom to connect with co-workers.

Be Cyber-Aware: Never Open Unexpected Attachments – Be Careful What You Click

Many attempted phishing and ransomware attacks appear in your inbox looking like an email from a person or service that you trust. If it looks abnormal, has suspicious attachments/links, from an unusual sender, then **do not click any of the links and delete the email immediately**.

Hovering your mouse over a questionable link is one way to determine its validity. That means if you move the mouse pointer over the link, but don't click, you should see the actual target URL.

If possible, call the person or business at a phone number that you trust and ask them if the suspicious email is valid. This gives you a second method of communication to verify the email.

Responding to Information Security Concerns

If you have clicked on a deceptive link and provided your credentials, change your password immediately.

If you clicked a suspicious link or if you believe your computer may be compromised, immediately report the concerns by:

- Notifying the **IT Service Desk** at 604-412-7444, Option 1 or email **techhelp@bcit.ca**