What is a privacy breach?

A privacy breach occurs when personal information is used or disclosed in a way that does not comply with the privacy protection requirements of the *Freedom of Information and Protection of Privacy Act* (FOIPPA). Personal information can be breached in many ways, including system and mechanical failure, whether accidental or intentional; cyber attacks or breaches; unauthorized access (e.g., curiosity); and theft.

Some common examples include:

- losing a laptop or other mobile devices that contains personal information
- accidentally sending an email containing personal information to the wrong recipient
- posting personal information online where it can be accessed publicly
- phishing or cyber attacks
- snooping in personal files at work for reasons unrelated to your employment duties.

How should a privacy breach be managed?

For all privacy breaches, it is important to act immediately. In the event of a suspected or actual privacy breach, take the following steps to reduce the impact of the breach.

1. **Report the Incident –** Report the incident immediately to your supervisor and CMTN's privacy officer. If your CMTN laptop or another portable device has been lost or stolen:
    a. Report the lost or stolen item to RCMP.
    b. Report the lost or stolen item to your direct supervisor.
        i. Your direct supervisor must report the lost or stolen item to the VP Corporate Services and the Director of Information Technology and CIO.
2. **Contain the Breach and Recover Information –** Make every effort to recover the confidential or personal information to lessen the impact on the individuals involved in the breach. Appropriate actions might include recalling an email, recovering missing records or equipment, correcting physical security flaws, or isolating the activity that led to the incident.
3. **Remediate –** Work with your supervisor and the privacy officer to determine the specifics of the incident, its impact on people and CMTN, and the cause(s) of the breach. Take steps to resolve the breach and, as necessary, notify the affected individuals.
4. **Prevent –** Identify lessons from the breach, understand your responsibilities, be diligent in the handling of confidential or personal information, and be an active participant in developing a culture of prudent information management.

The privacy officer works with the department responsible for the privacy breach and the IT Services Department. Privacy breaches may also require the involvement of the Human Resources Department.

Questions about privacy breaches?

Please contact Aman Kang, the privacy officer by emailing foi@coastmountaincollege.ca.