Privacy Breach Management

Privacy breaches occur when personal information is accessed, collected, used, or disclosed without proper authorization. Such breaches can be accidental or deliberate, and may include the theft, loss, alteration, or destruction of information.

For all privacy breaches, it is important to act as soon as possible. In the event of a suspected or actual privacy breach, follow these steps:

Report the incident.
Contain the breach and, if possible, recover the information.
Investigate the cause of the breach.
Notify the necessary individuals, as specified under FOIPPA.
Take steps to prevent a recurrence.

Reporting an incident

You must report the incident immediately to your direct supervisor and CMTN's privacy officer. The privacy officer can be reached at foi@coastmountaincollege.ca.

If your CMTN laptop or other portable device has been lost or stolen:

Report the lost or stolen item to the RCMP.
Report the lost or stolen item to your direct supervisor.
Your direct supervisor must report the lost or stolen item to the VP Corporate Services and the Director of Information Technology and CIO.

Containment: Recovering Information

Once the incident has been reported, the next step is containment (i.e., taking immediate steps to stop the activity that caused the breach). This might include:

making efforts to recover lost or stolen devices or materials
asking people who received personal information in error to delete or return it
if information has been posted online in error, deleting or removing it
recalling communications sent in error.
Work with your direct supervisor and the privacy officer to ensure that the breach is fully contained.

Investigate

The third step in responding to a privacy breach is to conduct an investigation to ascertain what took place and how best to remedy the breach. This includes considering questions such as:

- What caused the breach?
- What is the scope of the breach and which personal information and records were involved?
- Who was impacted by the breach?
- What types of harms may arise from the breach, including identity theft, fraud, financial loss, physical harms, and emotional harms?

Work with your direct supervisor and the privacy officer to determine the specifics of the incident and the cause(s) of the breach. Take steps to resolve the breach and, as necessary, notify the affected individuals.

Notification

The College is subject to notification obligations under FOIPPA. If a privacy breach gives rise to a risk of significant harm to impacted individuals, the College must follow a process to report the breach to the Office of the Information and Privacy Commissioner and to the individuals affected.

Issuing such notifications is the responsibility of the privacy officer, but you may be asked to assist in the process.

Prevention

The final stage in a privacy breach response is to take steps to prevent future recurrences of the breach. Make changes to departmental processes, 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.

Questions about privacy breach management

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