Reporting Privacy Breaches: Guidelines

Ontario's *Freedom of Information and Protection of Privacy Act* (FIPPA), governs the collection, retention, use, disclosure and security of personal information and establishes rules for organizations to follow in order to protect individuals' privacy.

A privacy breach:

is an unauthorized collection, use or disclosure of someone's personal information (PI), in contravention of the *Freedom of Information and Protection of Privacy Act* (FIPPA) or *Personal Health Information Protection Act* (PHIPA) which:

- may affect an individual or a group
- may be discovered in the course of conducting college business

Examples of unauthorized collection, use or disclosure:

- information collected in error
- information used for a purpose not consistent with the original collection
- lost or misplaced PI
- stolen PI (laptops, data drives or disks)
- accidental disclosure of PI to an unauthorized person or group
- deliberate disclosure of PI to an unauthorized person or group (for fraudulent or other purposes)

If a privacy breach is suspected or confirmed, report it to:

Your immediate supervisor (or, if unavailable, the next available level of management) and the FOI Coordinator will take the lead in investigating the incident. Use the companion *Privacy Breach Report Template* to record details

Follow the four steps outlined on the next pages

Personal information is recorded information about an identifiable individual, and includes

- ethnic origin, race, religion, age, sex, sexual orientation, marital status, etc.
- information regarding educational, financial, employment, medical, psychiatric, psychological or criminal history
- identifying numbers, e.g., S.I.N., student number
- home address, telephone number
- personal opinions of, or about, an individual
- correspondence sent to the institution by an individual that is of a private or confidential nature
- the individual's name where it appears with or reveals other personal information

Reporting suspected or confirmed privacy breaches

Decisions on how to respond to a suspected or confirmed privacy breach should be made on a case by case basis. Take each situation seriously and undertake steps 1, 2 and 3 on the following pages in quick succession.

Preliminary questions:

What was the date of the incident?

What was the location of the incident?

When was the incident discovered?

How was the incident discovered?

What happened?

Step 1: Contain

Contain the incident and assess the situation immediately. Contact the Information and Privacy Coordinator.

Key Questions

Have you contained the incident? This step includes such actions as: recovering information, changing access codes, shutting down systems, stopping the unauthorized collection, use or disclosure.

Have you designated an appropriate individual to lead an initial assessment? This should be someone who has appropriate decision-making authority and responsibility within the unit(s) concerned.

At this preliminary stage, have the appropriate internal staff members been made aware of the incident?

Does criminal activity (e.g. theft) appear to be involved? If yes, Security should be notified

Have the details of the incident that are known at this stage been recorded? This step will aid in later investigation and corrective actions.

Step 2: Assess the Risks

Assess the types of personal information involved and the sensitivity of the information to determine the appropriate response and notification to affected individuals. Examine the situation fully and work with the IPO to ensure that any necessary details of the breach and any corrective actions are documented for later investigation and review.

Key Questions

Personal information

What personal information was involved? Determine what data elements were involved.

What format were the records in? Indicate the format(s) of the records involved: paper, electronic or other; on network server, workstation, portable media (data drive, disk, audio or video tape, microfiche), etc. Determine whether the information was encrypted, anonymized or otherwise not easily accessible, and what physical or technical security measures were in place at the time of the breach.

Assess the Risks – personal information, continued

How sensitive is the personal information involved? In most cases, the more sensitive the information, the greater the harm to individuals from a privacy breach. Sensitive personal information would include (but is not limited to) health, financial, student or employment information, especially in combination.

Cause and extent of the breach

What is the cause and extent of the breach? Determine what caused the breach and assess the extent of the unauthorized access to, or collection, use or disclosure of, the personal information, including number and types of possible recipients.

Is there a risk of ongoing breaches or further exposure of the personal information? *Ongoing or further exposure of the information* may include exposure via mass media (online or other).

Can the personal information be used for fraudulent or other purposes? Establish whether the personal information has been lost or stolen, and if so, whether it has been recovered. If criminal activity is involved, notify the Security Manager.

How many individuals were affected by the breach and who are they (e.g. employees, students)?

Foreseeable harm

Is there foreseeable harm from the breach? Assess what harm could result *to individuals* from the breach, such as risk to physical security, identity theft, financial loss, damage to reputation/relationships.

Evaluate the harm that could result *to Fleming College* from the breach, for example, loss of trust in the institution or damage to its reputation, financial losses or exposure, legal proceedings.

Consider what *public harm* could result from the breach, such as risk to public health or safety.

Step 3: Notify Affected Individuals

Based on the results of the assessment, decide whether to notify individuals affected by the breach, when and how they will be notified, and what information should be included in the notification. Consult FOI Coordinator on the notification before sending.

Key Questions

✓

Should affected individuals be notified? Consider the risk of harm to the individual (see *Foreseeable harm,* above, for relevant factors). *If any harm is possible, notification is required*, except in exceptional circumstances (e.g. where notice would interfere with a law enforcement investigation or there is a possible risk to public health or safety).

✓

Have you decided when and how affected individuals should be notified, and by whom?

✓

Have you established what should be included in the notification? Depending on the circumstances, notification could include some or all of the following:

Description of breach

Specifics of the information inappropriately accessed, collected, used or disclosed

Steps taken so far to address the breach and any future steps planned to prevent further privacy breaches

Additional information, if required, about how individuals can protect themselves (tracking credit cards, monitoring bank accounts, changing ID numbers, etc.)

Contact information for an individual (include position title) within the College who can answer questions or provide further information

NOTE: Limit distribution of the Template to only those individuals who need to be informed about the incident as part of their duties and responsibilities.

Step 4: Investigate and Correct

The FOI Coordinator will further investigate the cause of the privacy breach, work with the department concerned to prepare documentation and consider whether to develop a prevention plan. They will also determine whether Ontario's Information and Privacy Commissioner (IPC) should be informed of the breach.

A prevention plan may address such issues as:

Staff training

Policy review or development

Audit of physical and/or technical security

Review of relationships with third party service delivery partners

Audit to ensure that prevention plan has been fully implemented

If notifying a number of individuals by telephone, use a script that provides the same information to all recipients. Clearly identify the College and provide contact information.

If notifying in writing (letter or email), make the contents clear and concise. The FOI Coordinator can assist in drafting the notification if requested. Use a method that proves receipt of the letter, such as registered mail or by courier. When sending notification by email, ensure that the current email address is known. Request delivery notification and read receipts where possible.