Procedure Title:	Privacy Breach Reporting
Procedure ID:	#OP 1-111C
Manual Classification:	College Policies
Linked to Policy:	1-111 Access to Information and Protection of Privacy
Approved by Senior Management Team (SMT):	June 18, 2025
Effective Date:	July 1, 2025
Next Review Date:	July 1, 2028
Contact for Procedure Interpretation:	Associate Vice President Finance and Policy

1.0 – Purpose

The purpose of this procedure is to enable an efficient and coordinated response to a privacy breach, to clarify roles and responsibilities, to establish a process to investigate, identify the scope of, contain and remediate the breach and to prepare for possible involvement of the Ontario Information and Privacy Commissioner (IPC).

2.0 – Definitions and Acronyms

College Community: Any person who studies, teaches, conducts research at or works at, or under, the auspices of the College and includes without limitation, employees or contractors; appointees (including volunteer board members); students; visitors; and any other person while they are acting on behalf of, or at the request of the College.

Personal Information: As defined under FIPPA, personal information means recorded information about an identifiable individual, including:

a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual;
b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;
c) any identifying number, symbol, or other particular assigned to the individual:
d) the address, telephone number, fingerprints or blood type of the individual;
e) the personal opinions or views of the individual except where they relate to another individual;
f) correspondence sent to the College by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence;
g) the views or opinions of another individual about the individual; and;
h) the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

Personal information does NOT include:

- the name, title, contact information or designation of an individual that identifies the individual in a business, professional or official capacity
- information about an individual who has been dead for more than thirty years

records of graduation that are otherwise publicly disclosed

Privacy Breach: covers every instance of theft, loss, and collection, use, retention, disclosure or destruction of PI that is not consistent with privacy law, whether intentional or in error. Some examples of privacy breaches include:

a) Loss or theft of portable devices containing PI;
b) Misdirected faxes or e-mails containing PI;
c) Cyberattacks, including ransomware attacks on records of PI; and
d) Deliberate unauthorized access to Records under the Custody or Control of the College, by a member of the College Community or others.

3.0 – Guiding Principles

This procedure sets out the steps to take when any member of the College Community becomes aware that a privacy breach involving personal information has occurred.

4.0 – Scope

All members of the College Community are responsible for appropriate management of personal and confidential information, and to report and act on any breaches that they become aware of or are involved in.

College Department Head(s) are responsible for:

a) Responding to inquiries from the College Community related to concerns about PI
b) Responding to suspected breaches for their respective department(s)
c) Notifying the Privacy Coordinator and/or Officer of all Privacy Breaches and suspected Privacy Breaches within their Department
d) Working with staff in their own Department(s) to follow the steps in this procedure to enable timely reporting to the Privacy Coordinator and/or Officer
e) Ensuring Department staff are trained on and comply with this and all required procedures
f) Containing Privacy Breaches and mitigating against future Privacy Breaches

The Privacy Coordinator and Privacy Officer are responsible for:

a) Maintaining a record of all confirmed College Privacy Breaches;
b) Working with Department Head(s) to assist with responses to internal PI inquiries and concerns;
c) Providing formal notification to individuals affected by a confirmed Privacy Breach;
d) Consulting with other Departments, senior management or legal counsel, as may be necessary;
e) Notifying the IPC of Privacy Breaches, where required; and Reporting Privacy Breach statistics to the IPC annually.

5.0 – Operating Procedure

The below outline the process of responding to and reporting a Privacy Breach.

5.1 – Part 1: Privacy Breach Notification within the College

Immediately upon learning of the privacy breach, employees are notify their direct supervisor(s) who in turn shall notify the applicable Department Head(s). The Department Head(s) will notify the Privacy Coordinator and/or Officer.

Employees are not to initiate investigation of the breach unless specifically asked to do so by their Department Head(s).

Depending upon the nature and seriousness of the breach, the Department Head(s), together with the Privacy Coordinator and/or Officer, shall involve their Senior Management Leader.

The Department Head is responsible for notifying the College Privacy Coordinator and/or Officer as soon as reasonably possible after discovering or being notified of the breach.
The Department Head may need to ensure "Part 2: Contain the Breach" is followed, before compiling enough information to report to the Privacy Coordinator and/or Officer.

The following information should be included in the notification to the College Privacy Coordinator and/or Officer:

- The Department where the breach originated,
- Cause of the breach (such as in the case of unauthorized access);
- The date(s) of the breach
- A description of the nature and scope of the breach
- A description of the PI that was subject to the breach (not the PI itself)

5.2 – Part 2: Containing the Breach

The Department Head, or their designate, shall identify the PI that was involved in the breach and the sensitivity of it, and:

1. If possible, retrieve and secure any PI that was accessed or disclosed improperly
2. Make sure that no copies of the accessed or disclosed PI were made or retained by a person who was not authorized to view or receive that PI
3. Record the contact information of all unauthorized recipients where possible
4. If the breach involved an electronic records system, and there is a danger of additional unauthorized access to, or disclosure of, PI, change passwords and identification numbers, and if possible, temporarily disable the system and/or restrict access to the system
5. If the breach occurred due to a member of the College Community improperly accessing PI, consider suspending that individual's access rights both in the short term, and in accordance with the outcome of any College investigation or proceeding, which may include disciplinary action, subject to any applicable Collective Agreement and College Policy such as the Code of Conduct
6. Identify the individuals and organizations who are involved with or affected by the breach
7. Identify the nature and scope of the breach

5.3 – Part 3: Notification to Affected Party(ies)

If the Privacy Breach poses a real risk of significant harm to the individual or organization, notification is required. The Privacy Coordinator and/or Officer, in consultation with the Department Head(s) will consider the sensitivity of the compromised PI and whether the PI is

likely to be misused.

When notification is deemed necessary, it must be made as soon as reasonably possible and will be made by direct or indirect notification as described below.

Direct Notification: Notification may be written or verbal, by telephone, email or letter. The notification should include the following information:

1. A description of the nature and scope of the breach
2. A description of the PI that was subject to the breach, and if financial information was involved, a suggestion to contact the individual's bank, credit union or credit card company, and obtain a credit report
3. The measures that the College took to contain the breach, and any future measures it will take
4. The name and contact information of the College Privacy Coordinator
5. A statement notifying the individual of their right to contact the IPC and how to do so

Indirect Notification: If the Privacy Breach was significant in scope, or if notification to individuals is not practical or possible, the College may notify indirectly by, for example, by posting a notice.

5.3 – Part 4: Investigate, Remediate & Record

Following identification, containment and notification, the Department head will take steps to review the Breach and seek to understand how it happened and what can be done to prevent similar occurrences in the future.

As a part of this process, they will:

1. Conduct an internal investigation to ensure the breach is contained, and this response procedure has been implemented in full. They will also review the circumstances surrounding the origin of the breach.
2. Review the College's privacy policies, operating procedures and department protocols to ensure they are adequate to protect the College's PI. They will recommend amendments to College policies and operating procedures and make revisions to their department(s) protocols as deemed necessary.
3. Determine whether systemic issues need updating; for example, updating technological systems or staff privacy training.
4. Take corrective action as necessary, for example, provide updated training to their staff.
5. Correspond with the Privacy Coordinator and/or Officer if it is identified that the IPC needs to be notified of the breach.
6. Should the IPC investigate a breach, co-operate with the IPC. Update the IPC of all remedial measures taken.

Provide to the Privacy Coordinator and/or Officer with a summary of steps taken to remediate the situation.

5.3 – Part 5: Notification to the IPC (if Required)

The College, via the Privacy Coordinator and/or Officer, may contact the IPC if the privacy breach is determined to be significant. Examples of significant privacy breaches include (but are not limited to):

- Breaches that involve a large number of individuals;
- include sensitive PI, such as health or financial information

- involve theft, loss or unauthorized use or disclosure of PI

The College may also notify the IPC if it is having difficulty containing the privacy breach or if the College is unsure as to whether or how to notify affected individuals.

The Privacy Coordinator and/or Officer may contact legal counsel for guidance before contacting the IPC. The IPC may help the College develop a response.

The following information will be included in any Notice sent to the IPC:

a) A description of the nature and scope of the breach;
b) A description of the measures implemented and planned to contain the breach;
c) Whether and how affected individuals were notified;
d) The name and contact information of the College Privacy Coordinator; and
e) Updates on remedial measures taken to contain the breach and prevent future breaches.

The IPC may investigate reported breaches. When investigating a privacy breach, the IPC may, depending on the circumstances:

a) Ensure any issues surrounding containment and notification have been addressed;
b) Assess whether affected individuals were adequately notified;
c) Interview individuals involved with the privacy breach;
d) Receive representations from individuals whose privacy has been breached;
e) Obtain and review your position on the privacy breach;
f) Ask for a status report of any actions that you have taken;
g) Review and provide input and advice on your current information management policies and procedures; or
h) Issue a FIPPA report that may contain recommendations;
i) Issue an order that require proof of compliance.

6.0 – Related Documents

- OP 1-111A Access Correction Procedure
- OP 1-111B Collection of Personal Information
- OP 1-11C Privacy Breach
- OP 1-111D Use and Disclosure of Personal Information Procedure
- 1-112 Information Practices Related to Personal Health Information Policy
- 1-104 Record Retention
- OP 1-104 Record Retention
- FIPPA - Freedom of Information and Protection of Privacy Act R.S.O. 1990 c. F. 31
- PHIPA – Personal Health Information Protection Act, S.O. 2004, c. 3 Sched. A

7.0 – History of Amendments & Reviews

Date Approved	Approved By	List of Approved Amendments / Review
2020	SMT	
June 18, 2025	Senior Management Team	Updated to current format, adding and aligning definitions. General language and grammatical edits. Removal of duplicated

		direction.