Fleming College

Policy Title:	Privacy Breach Reporting Procedure (Personal Information)
Policy ID:	#OP 111-1C
Manual Classification:	Section 1 – College Policies
Linked to Policy:	Access to Information and Protection of Privacy
Approved by Board of Governors:	
Revision Date(s):	N/A
Effective Date:	
Next Policy Review Date:	March 2023
Contacts for Policy Interpretation:	Policy and Privacy Coordinator Privacy Officer Manager of Operations - President's Office

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**").

This procedure sets out the steps to take when any member of the College Community becomes aware that a privacy breach involving PI has occurred. It is important to act immediately, to review and, if necessary, repeat some of the steps below. Some steps may have to be followed or implemented before other steps, for example, you may need to investigate the nature and scope of the breach in order to make an initial report.

Capitalized terms used below that are not defined in this procedure are defined in the Access to Information and Protection of Privacy Policy.

2.0 – Application of Procedure

This procedure applies to all members of the College Community that handle **Personal Information** ("**PI**") on behalf of the College. Under the *Freedom of Information and Protection of Privacy Act*, the College is an institution that has a legal duty to protect the PI it handles against privacy breaches.

3.0 – Accountability

a) Everyone is responsible for ensuring the security and confidentiality of PI under the Custody or Control of the College. You must review, understand and follow the College Privacy policies and procedures and your department's specific processes.

b) The College will provide training to Department Head(s) who in turn will provide training and/or disseminate information to Employees, students, volunteers, and third-party

contractors within their respective department(s) to ensure compliance with this Procedure.

c) Any suspected or confirmed breaches of privacy must be immediately reported in accordance with the “Steps” laid out in this Procedure.

d) The Privacy Coordinator and/or Officer will report annually to the Information Privacy Commissioner of Ontario all confirmed breaches of PI.

e) Individuals who fail to adhere to this Procedure may be subject to student or employment-related disciplinary action, subject to any applicable Collective Agreement.

4.0 – Definitions

“**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.

5.0 – Responsibilities

College Department Head(s) are responsible for:

a) Responding to inquiries from the College Community related to concerns about PI and/or suspected breaches for their respective department(s);

b) Notifying the Privacy Coordinator and/or Officer of all Privacy Breaches and suspected Privacy Breaches within their Department;

c) 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;

d) Ensuring Department staff are trained on and comply with this and all required procedures; and

e) 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

f) Reporting Privacy Breach statistics to the IPC annually.

6.1 – STEP 1: Privacy Breach Notification within the College

1. Immediately upon learning of the privacy breach, notify your 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.

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

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

4. The Department Head(s) is/are responsible for notifying the College Privacy Coordinator and/or Officer as soon as reasonably possible after discovering or being notified of the breach.

   NOTE: The Department Head(s) may need to ensure “Step #2: Contain the Breach” is followed, before compiling enough information to report to the Privacy Coordinator and/or Officer.

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

The College department where the breach originated and only if applicable and appropriate, members of the College Community who caused the breach (such as in the case of unauthorized access);

a) The date of the breach;
b) A description of the nature and scope of the breach; and
c) A description of the PI that was subject to the breach (not the PI itself).

   NOTE: The notification should be updated as new information is obtained, while progressing through the steps of this procedure.

6.2 – STEP 2: Contain the Breach

The Department Head(s), or their designate(s), 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; if available;

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 employment-related disciplinary action, subject to any applicable Collective Agreement;

6) Identify the individuals and organizations who are involved with or affected by the breach; and,

7) Identify the nature and scope of the breach.

6.3 – STEP 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 oral, by telephone 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; and

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.

6.4 – STEP 4: Investigate, Remediate & Record

The Department Head(s) shall:

1) Conduct an internal investigation to ensure the breach is contained, and this response procedure has been implemented. They will also review the circumstances surrounding 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 College staff.

5) Correspond with the Privacy Coordinator and/or Officer if you identify that IPC needs to be notified of the breach; and,

6) Should the IPC investigate a breach, co-operate with the IPC. Update the IPC of all remedial measures taken.

7) Provide to the Privacy Coordinator and/or Officer the following information in writing: College department where the breach originated and <u>if applicable</u>, agent(s) that caused the breach (such as in the case of unauthorized access):

    - The date of the breach;
    - The nature, scope and cause of the breach;
    - The number of individuals affected by the breach;
    - A description of the PI that was subject to the breach; and
    - A summary of the steps taken to respond to the breach.

The Department Head(s) is responsible for remediating any privacy breach and mitigating against future breaches. The Privacy Coordinator and/or Officer is responsible for maintaining a record of all College Privacy Breaches.

6.5 – STEP 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):

a) Breaches that involve a large number of individuals;
b) include sensitive PI; and
c) 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 procedure.

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.

7.0 – Related Documents

- Access to Information and Protection of Privacy Policy
- *Freedom of Information and Protection of Privacy Act,* R.S.O. 1990 c. F.31. https://www.ontario.ca/laws/statute/90f31
- "Privacy Breaches: Guidelines for Public Sector Organizations". September 2019. Information and Privacy Commissioner of Ontario. www.ipc.on.ca See the guidance section of the IPC website for more information.

8.0 – History of Amendments & Reviews