PROCEDURE

Title: **PRIVACY BREACH PROTOCOL**

Procedure No.: **2014c**
Effective Date: 2010 June 22

Department: Director's Services – Corporate Services

Reference(s):
- Municipal Freedom of Information and Protection of Privacy Act
- Personal Health Information Protection Act
- Education Act
- General Data Protection Regulation
- Privacy and Records Information Management Policy
- Privacy and the Management of Personal Information Procedure

1.0 PURPOSE

The privacy breach protocol has been adopted to allow for a prompt, reasonable and coordinated response should personal information be breached. It is designed to clarify roles and responsibilities, and support effective containment, investigative, and remediation activities.

2.0 PRIVACY BREACHES

A privacy breach occurs when personal information is collected, used, disclosed, lost or stolen, retained, or destroyed in a manner inconsistent with privacy legislation.

Personal information can be compromised in many ways. Some breaches have relatively simple causes and are contained, while others are more systemic or complex. Privacy breaches are often the result of human error; such as an individual's personal information sent by mistake to another individual. A breach can be more wide-scale, such as when a computer program change causes the personal information of many individuals to be compromised through inadvertent distribution.

3.0 STAFF RESPONSIBILITIES IN HANDLING A PRIVACY BREACH

3.1 Employees

Employees dealing with student, employee and/or business records must be particularly aware of how to identify and address a privacy breach.

All Board employees are responsible to notify their supervisor immediately, or, in their absence, the Freedom of Information Coordinator upon becoming aware of a breach or suspected breach; and contain, if possible, the suspected breach by suspending the process or activity that caused the breach.

Employees responsible for the supervision of volunteers or student placements must ensure those individuals understand their duty to report suspected privacy breaches to their supervisor.

3.2 Senior Administration, School Administrators, Department Managers, and Supervisors

Senior Administration, school Administrators, department Managers, and Supervisors are responsible for alerting the Freedom of Information Coordinator of a breach or suspected breach and to work with the Coordinator to implement the five steps of the Privacy Breach Protocol including:

- obtaining all available information about the nature of the breach or suspected breach;
- providing as much information about the breach as is currently available;
- working to undertake all appropriate actions to contain the breach;
- ensuring that those whose personal information has been compromised are informed as required;
- supporting and monitoring any remedial action; and
- ensuring details of the breach and corrective actions are documented.

3.3 Freedom of Information (FOI) Coordinator

The FOI Coordinator plays a central role in the response to a breach by ensuring all five steps of the protocol are implemented and documented.

4.0 PRIVACY BREACH RESPONSE PROTOCOL - GENERAL

The following five steps are to be initiated as soon as a privacy breach or suspected breach has been reported to the Freedom of Information Coordinator.

4.1 Step 1 - Assess

The Freedom of Information Coordinator will work with the school/department to assess the situation to determine if a breach has indeed occurred and what needs to be done.

Key persons within the Board and, if necessary, law enforcement will be contacted to respond and contain the breach.

4.2 Step 2 - Containment

Containment involves identifying the scope of the breach and taking immediate corrective action to address the breach. The goal is to minimize and alleviate any consequences for both the individual(s) whose personal information was involved and the Board.

Activities may include:

- recovering records
- revoking/changing computer access codes
- correcting weaknesses in physical or electronic security

All containment activities or attempts to contain shall be documented by the school Administrator, department Manager, or any other individual(s) involved in containing the breach. Information is to be reported to the Freedom of Information Coordinator.

4.3 **Step 3 - Investigate**

Once the privacy breach is contained, key informants such as the Freedom of Information Coordinator, the ITS department, the school Administrator or department Manager will be involved in the investigation to determine the cause and extent of the breach. .

The investigation includes:

- identifying the events that led to the privacy breach;
- evaluating if it was an isolated incident or if there is risk of further exposure of information;
- determining who was affected by the breach; e.g. students or employees and how many were affected;
- identifying who had access to the information;
- determining if information was inappropriately disclosed, lost or stolen;
- evaluating the effect of containment activities; and
- determining if any of the personal information was recovered.

4.4 **Step 4 - Notify**

Notification helps to ensure affected parties can take remedial action, if necessary, and to support a relationship of trust and confidence.

4.4.1 **Determining Required Notifications**

The Freedom of Information Coordinator, in consultation with the school Administrator or department Manager, will determine what notifications are required. Considerations include:

Reasonable expectations – is there a reasonable expectation of notification by the affected person?

Who had inappropriate access to the personal information? – does the person having inappropriate access, an individual bound by professional duties of confidentiality or a member of a college that may be sanctioned if confidentiality is breached (i.e., a teacher who is a member of the College of Teachers; a psychologist who is a member of the College of Psychologists, etc.).

Risk of physical harm - Does the inappropriate disclosure, loss or theft of information place any individual at risk of physical harm, stalking, or harassment?

Risk of hurt, humiliation, or damage to reputation - Could the inappropriate disclosure, loss or theft of information lead to hurt, humiliation, or damage to an individual's reputation, e.g. the loss or theft of information such as mental health records, medical records, or disciplinary records.

Risk of loss of business or employment opportunities - Could the inappropriate disclosure, loss or theft of information result in damage to an individual's reputation, affecting their business or employment opportunities?

Risk of identity theft - Is there a risk of identity theft or other fraud in the system? How reasonable is the risk? Identity theft is a concern if the breach includes unencrypted information such as names in conjunction with social insurance numbers, credit card numbers, driver's license numbers, personal health numbers, debit card numbers with password information, or any other information that can be used for fraud by third parties (e.g., financial).

4.4.2 Notification to Authorities or Organizations

Examples of organizations that may need to be notified include: police if theft or other crime is suspected; insurers; Information and Privacy Commissioner; a regulatory College; credit card companies and financial institutions; third party contractors or other parties that may be affected; other departments or staff; or, union or other employee groups.

4.4.3 Notification Timeline

Affected individuals shall be promptly notified. Depending on the nature and scope of the breach and status of the investigation, notification may occur in stages. For example, an initial notification may be given to ensure that the affected individuals receive information directly from the school Administrator or department manager with updates as required and a report of findings and action taken upon completion of the investigation.

4.4.4 Method of Notification

The method of notification shall be guided by the nature and scope of the breach and in a manner that reasonably ensures that the affected individual will receive it. Direct notification, e.g., by phone, letter, email or in person is preferable and shall be used where the individuals are identified. Where it is not possible to determine the affected individuals, for example when a student information system has been breached, posted notices, media releases, website notices or letters to all students or staff shall be considered.

4.4.5 Who is Responsible for Notification to Affected Individuals

Individual(s) shall be notified by the department associated with the breach. For example, where the breach is for student information, the School Administrator of the school shall be responsible for providing notification; where the breach is for staff information, Human Resource Services shall be responsible for providing notification. The Freedom of Information Coordinator will assist with the content of the notification.

For breaches that are more broad in nature, the Freedom of Information Coordinator shall be responsible for notification.

4.4.6 **Content of Notification**

Notification shall include:

- a description of the incident and the personal information involved;
- the nature of potential or actual risks or harm, if any, and the appropriate action for individuals to take to protect themselves against harm;
- what mitigating actions were/are being taken; and
- a contact person for questions or to provide further information; and/or contact information for the Information and Privacy Commissioner, as appropriate.

4.5 **Step 5 - Implement Change**

Once the breach has been resolved, the Freedom of Information Coordinator shall work with the school Administrator, department Manager or Superintendent, or ITS department to develop a prevention plan or take corrective actions as required. The extent of the response shall be determined by the significance of the breach and whether it was systemic or isolated. Responses may include: audits, review of policies, procedures and practices; employee training; or review of service delivery partners. Consideration shall be given to testing and evaluating remedial actions to determine if they have been implemented correctly and notifying the community of any changes or preventative measures that have been implemented.

5.0 **PRIVACY BREACH RESPONSE PROTOCOL – SPECIAL CIRCUMSTANCES**

5.1 **Legislative Requirements under the Personal Health Information Protection Act (PHIPA)**

5.1.1 **Notice to Affected Individual**:

Under the *Personal Health Information Protection Act,* a Health Information Custodian (HIC), having knowledge that personal health information in their custody or control was lost, stolen or used/disclosed without authority, is required to:

- notify the individual of the theft or loss or unauthorized use or disclosure of the individual's personal health information; and
- include in the notice a statement the individual is entitled to make a complaint to the Information Privacy Commissioner.

5.1.2 **Notice to the IPC is required when**:

- The HIC has reasonable grounds to believe the personal information in their custody or control was used or disclosed without authority by a person who knows or ought to have known they were using or disclosing the information without authority (example: snooping); or
- The HIC has reasonable grounds to believe personal information in their custody or control was stolen (example: stolen records from car, computer hacking); or
- The HIC has reasonable grounds to believe that, after an initial loss or unauthorized use or disclosure of personal health information in their custody or control, the personal health information was or will be further used or disclosed

without authority (example: a subsequent breach could happen from the initial breach); or
- The loss or unauthorized use or disclosure of personal health information is part of a pattern of similar losses or unauthorized uses or disclosures of personal health information (example: an automated process results in similar breaches over time); or
- The HIC determines the loss or unauthorized use or disclosure of personal health information is significant taking into consideration the sensitivity and volume of information, the number of individuals affected, and whether more than one HIC was responsible; or
- The HIC is required to give notice to a College of an event described in section 17.1 of the Act that relates to a loss or unauthorized use or disclosure of personal health information (see Notice to College below).

Notice to the IPC generally is not required if:

- The breach was not intentional; and
- The breach was a "one-off" incident and not part of a pattern; and
- The breach is contained; and
- The scope of the breach was not significant; and
- There are no risks of identity theft, physical harm, hurt/humiliation or damage to reputation, or loss of business or employment opportunities.

5.1.3 **Notice to College**

A HIC is required to give written notice to their College within 30 days of the following events:

- an individual they have employed as a HIC who is a member of a College, is terminated, suspended or subject to disciplinary action as a result of the unauthorized collection, use, disclosure, retention or disposal or personal information; or
- the employee resigns and the HIC has reasonable grounds to believe the resignation is related to an investigation or other action by the custodian with respect to an alleged unauthorized collection, use, disclosure, retention or disposal of personal health information by the employee.

5.2 **Legislative Requirements Under the General Data Protection Regulation (GDPR)**

There may be additional considerations regarding breach notification for international students, recruited from a European country, attending a school in the board.

As such, any breach involving the personal data of an international student from a European county, must be reported immediately to the Freedom of Information Coordinator for assessment and response.