Procedure Title	**Privacy Breach Protocol**		
Date of Issue	April 28, 2021	**Related Policy**	BP 1408-D
Revision Dates	December 1, 2021	**Related Forms**	Privacy Breach Report form (obtained through Corporate Services)
Review Date		**Originator**	Administrative Council
References			
Municipal Freedom of Information and Protection of Privacy Act (MFIPPA); Personal Health Information Protection Act (PHIPA); AP 1408-D "Protection of Privacy and Access to Information"			

1.0 RATIONALE

1.1 A privacy breach occurs when personal information is collected, used, disclosed, retained, or destroyed in any way that is inconsistent with the provisions of relevant privacy legislation.

1.2 This privacy breach protocol outlines the actions to be taken should a privacy breach, or suspected privacy breach occur. It describes the steps necessary to limit the breach, to clarify roles and responsibilities, support effective investigation and containment, and assist with remediation.

2.0 PRIVACY BREACH EXAMPLES

Personal information can be compromised in many ways. Some breaches are relatively simple and can be contained easily, while others are more complex. Privacy breaches are often the result of human error (e.g., an email intended for person A is sent accidentally to person B).

Examples of potential privacy breaches may include, but are not limited to:

i. lost or misplaced personal information – for example, a misplaced student psychological assessment, report card or USB stick containing student marks, etc.;

ii. lost or stolen technologies or equipment that may contain personal information -- for example, laptops, iPads, or smart phones, etc.;

iii. disclosure of personal information to an unauthorized person or group--for example, student report cards sent home with the wrong student(s), student marks emailed to wrong person, personal information posted publicly in error, accidentally sharing parent personal information with other staff who would not normally have access, etc.;

iv. inappropriate disclosure of personal information – for example, two employees discussing and identifying a student in a grocery store or a similar conversation on a cell phone in a public place;

v. deliberate disclosure of personal information to an unauthorized person or group for fraudulent, or other purposes -- for example, a user ID and password is posted (without consent) on a social networking site, etc.;

vi. information used for a purpose not consistent with the reason the information was collected -- for example, disclosure of staff contact list for the purpose of sales and solicitation;

vii. information collected in error -- for example, information collected from a third party, or where there is no authorization for the collection.

3.0 ROLES AND RESPONSIBILITIES

3.1 All employees are responsible for:

i. being alert to the potential for personal information to be compromised, and therefore potentially playing a role in identifying, notifying, and containing a breach;
ii. notifying their supervisor immediately, or, in their absence, the appropriate superintendent or the freedom of information and privacy coordinator, upon becoming aware of a breach or suspected breach; and
iii. containing, if possible, the suspected breach by suspending the process or activity that caused the breach.

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

3.2 Principals, managers, supervisors, and senior administration are responsible for:

i. alerting the freedom of information and privacy coordinator of a breach, or suspected breach, and working with the freedom of information and privacy coordinator to implement the five steps of the response protocol;
ii. obtaining all available information about the nature of the breach or suspected breach, and determining what happened;
iii. working with freedom of information and privacy coordinator to undertake all appropriate actions to contain the breach; and
iv. ensuring details of the breach and corrective actions are documented.

3.3 Director of education, and/or designate, is responsible for:

i. ensuring that the response protocol has been implemented;
ii. supporting the principal, manager, supervisor, and senior administration in responding to the breach;
iii. briefing senior administration and others as deemed necessary and appropriate;
iv. reviewing internal investigation reports and approving required remedial action;
v. monitoring implementation of remedial action;
vi. ensuring that those, whose personal information has been compromised, are informed as required.
vii. notifying the Information and Privacy Commissioner (IPC) of Ontario, where appropriate; and
viii. responding to questions from the public regarding the breach.

4.0 BREACH RESPONSE PROTOCOL

4.1 Initial Response

4.1.1 If a privacy breach (or suspected privacy breach) has occurred, board staff, upon learning of the breach/suspected breach, shall immediately take the following actions:

1. Contain the breach to stop any more information from being revealed
2. Notify your immediate supervisor
3. Involve the freedom of information and privacy coordinator
4. If requested by the freedom of information and privacy coordinator, complete the Privacy Breach Report form.

4.2 Containment

4.2.1 The first step in responding to a privacy breach is to stop the inappropriate flow of data. This may include actions such as, but not limited to, ‘recalling’ a message sent via O365, taking information down from a website, retrieving items from a garbage can, calling the recipient and asking them to destroy the information, or changing a password.

4.2.2 The names and contact information of any persons that received information (that should not have) must be documented, as there may be a need to follow-up later with them.

4.2.3 Involve the board's freedom of information and privacy coordinator (Corporate Services Department) to ensure all containment efforts are in place.

4.2.4 Document all breach and containment activities.

4.3 Assess and Investigate

4.3.1 Once the breach is contained, then the assessment and investigation into the breach needs to take place. This step will be led by the board's freedom of information and privacy coordinator (Corporate Services Department).

4.4 Notification

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

Based on the information gathered and assessed under section 4.3 the freedom of information and privacy coordinator will determine the level of notification that is required. Ideally, the department associated with the breach will notify the impacted individual(s) if notification is required.

4.5 Prevention of Future Breaches

4.5.1 Once the breach has been resolved, the freedom of information and privacy coordinator shall work with the principal/manager/supervisor or superintendent to develop a prevention plan or take corrective actions, if required. The extent of the response will 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.