PROCEDURE 196	
Adopted	January 2015
Last Revised	
Review Date	January 2019

PRIVACY BREACH PROTOCOL

1) PURPOSE

Hastings and Prince Edward District School Board is committed to the protection of personal and confidential information under its custody or control and to an individual's right of privacy regarding personal information that is collected, used, retained and disclosed in the school system.

While protection of personal information is paramount, the board recognizes that unintentional breaches may occur. Privacy breach protocol allows for a prompt, reasonable and coordinated response to incidents involving unauthorized disclosure or inappropriate use of personal information.

This administrative procedure outlines the action to be undertaken immediately should a privacy breach or suspected breach occur. It describes the steps necessary to limit the breach and is designed to clarify roles and responsibilities, support effective investigation and containment, and assist with remediation. All employees and third party providers have a role and responsibility to assist in the containment of a privacy breach.

2) DEFINITIONS

Breach: unauthorized access or disclosure; breaking or failing to observe a trust, promise, law, agreement, or code of conduct, whether intentional or not.

Personal information: information about an identifiable or potentially identifiable individual, as defined under privacy legislation.

Third-party Service Providers: contracted third parties used to carry out or manage programs and/or services on behalf of the board. For the purpose of privacy breach reporting third party includes all contractors that receive personal information from the board, or collect personal information on behalf of the board. Examples include: school photographers, bus companies, external data warehouse services and outsourced administrative services such as external researchers and consulting services.

3) PRIVACY BREACH

a) A privacy breach occurs when personal information is compromised, that is, when it is collected, used, disclosed, retained, or destroyed in a manner inconsistent with privacy legislation. Hastings and Prince Edward District School Board is governed by the following privacy legislation: *Municipal Freedom of information and Protection of Privacy Act* (MFIPPA), *Personal Health Information Protection Act* (PHIPA), and *Personal Information Protection and Electronic Documents Act* (PIPEDA). These acts govern the collection, use, disclosure and security of personal information.

b) 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 being sent by mistake to another individual. In today's environment in which technology increasingly facilitates information exchange, sometimes a privacy breach can be more wide-scale.

Examples of potential privacy breaches include:

i) lost or misplaced personal information, such as a misplaced student assessment, report card or Ontario Student Record (OSR) or a lost USB stick containing student marks or employee contact information;
ii) stolen technologies or equipment such as laptops, iPads or smart phones that may contain personal information;
iii) disclosure of personal information to an unauthorized person or group, such as student information forms given to the wrong students or personal information disclosed to a board member or employee who did not need it to effectively decide on a matter;
iv) inappropriate disclosure of personal information, such as two employees discussing and identifying a student in a grocery store, or a similar conversation on a cell phone in a public place;
v) information used for the purpose not consistent with the reason it was collected, such as sharing of staff or parent contact information for the purpose of sales or marketing or providing personal student information for a third party sponsored contest, without informed consent; and
vi) disposal of equipment with memory capabilities, such as USB sticks, laptops or photocopiers, or paper records containing personal information in a non-secure manner.

4) ROLES AND RESPONSIBILITIES IN RESPONDING TO A PRIVAY BREACH

a) 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 (FOI) 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.

b) Principals, managers, supervisors and senior administration are responsible for:
   i) alerting the FOI Coordinator of a breach or suspected breach and working with the FOI 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 FOI Coordinator to undertake all appropriate actions to contain the breach; and
   iv) ensuring details of the breach and corrective actions are documented.

c) Freedom of Information Coordinator is responsible for:
   i) ensuring that all five steps of the response protocol are implemented;
   ii) supporting the principal, manager, supervisor and senior administration in responding to the breach; and
   iii) notifying the Information and Privacy Commissioner where appropriate.

d) Director of education or designate is the accountable decision-maker responsible for:
   i) briefing senior administration and board members as necessary and appropriate;
   ii) reviewing internal investigation reports and approving required remedial action;
   iii) monitoring implementation of remedial action; and
   iv) ensuring that those whose personal information has been compromised are informed as required.

e) Third-party service providers are responsible for:
   i) taking reasonable steps to monitor and enforce their compliance with the privacy and security requirements defined in the contracts or service agreements;

ii) informing the board contact or FOI Coordinator of all actual and suspected privacy breaches;
iii) documenting how the breach was discovered, what corrective actions were taken and report back;
iv) undertaking a full assessment of the privacy breach in accordance with the third party service providers' contractual obligations;
v) taking all necessary remedial action to decrease the risk of future breaches; and
vi) fulfilling contractual obligations to comply with privacy legislation.

5) RESPONSE PROTOCOL

a) Unauthorized disclosure of personal information is the defining characteristic of a privacy breach, regardless of whether it was intentional, accidental or the result of a theft or malicious intent.

b) All privacy breaches or suspected privacy breaches must be reported to the principal or supervisor, or in their absence, to the appropriate superintendent or FOI Coordinator. Once reported, the supervisor or superintendent will contact the FOI Coordinator and the following response steps will be implemented. Form F196-1, Privacy Breach Report, will be used to guide and document the breach management process.

i) STEP 1 – Respond

(1) Assess the situation to determine if a breach or potential breach has indeed occurred and what needs to be done.
(2) When a breach has been identified, contact the appropriate area to respond to the breach.
(3) Report the privacy breach to key persons in the board (for example the director or designate) and, if necessary, to law enforcement.

ii) STEP 2 – Contain

(1) Identify the scope of the breach and contain it. Containment involves taking immediate action to put an end to the unauthorized access, where possible. For example, retrieving hard copies of any personal information that has been disclosed, revoking or changing passwords and identification numbers, temporarily shutting down the system/ device, or correcting weakness in physical or electronic security.
(2) Document the breach and containment activities.
(3) Develop briefing materials.
(4) Brief key persons on the privacy breach and how it is being managed.

iii) STEP 3 – Investigate

(1) Once the privacy breach is confirmed and contained, conduct an investigation to determine the cause and extent of the breach.
(2) Identify and analyze the events that led to the privacy breach.
(3) Evaluate if it was an isolated incident or if there is a risk of further exposure of information.
(4) Determine who was affected by the breach (e.g. students or employees), and how many were affected.
(5) Evaluate the effect of containment activities.
(6) Evaluate who had access to the information.
(7) Evaluate if information was lost or stolen.
(8) Evaluate if information has been recovered.

iv) STEP 4 – Notify

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

(1) The FOI Coordinator shall consult with the director of education to determine what notifications are required. Considerations may include notification to the affected individual and authorities and organizations such as: police, the Information and Privacy Commissioner, financial institutions or other parties that may be affected; other departments and employees; unions or employee groups and the board members.

(2) In determining if notification is required to the affected individual(s) the following shall be considered.
   (a) Who had access to the breached personal information?
   (b) Does the loss of theft place an individual at risk of physical harm?
   (c) Is there a risk of identity theft or other fraud?
   (d) Is there a risk of hurt, humiliation of damage to reputation?

(3) Notification should be done promptly, and shall include:
   (a) a description of the incident and the information involved;
   (b) the nature of potential or actual risks or harm;
   (c) what mitigating actions the board is taking;
   (d) appropriate action for individuals to take to protect themselves against harm;
   (e) a contact person for questions or to provide further information; and
   (f) contact for the Information Privacy Commissioner, if the office of the Information and Privacy Commissioner (IPC) is investigating. Include an explanation of the individual's right to complain to the IPC.

v) STEP 5 – Implement Change

When determining what changes and remedial actions need to be implemented, consider whether it is necessary to:

(1) review the relevant information management systems to enhance compliance with privacy legislation;
(2) amend or reinforce the existing policies, procedures, and practices for managing and safeguarding personal information;
(3) develop and implement new security or privacy measures, if required;
(4) review employee training/awareness on legislative requirements, security and privacy procedures and practices to reduce potential or future breaches, and strengthen as required;
(5) test and evaluate remedial actions to determine if they have been implemented correctly and if policies, procedures, and practices need to be modified; and/or
(6) recommend remedial action to the director of education or designate.

Legal References:

- *Education Act*
- *Municipal Freedom of Information and Protection of Privacy Act*
- *Personal Health Information Protection Act*
- *Personal Information Protection and Electronic Documents Act*

District Resources:

- Administrative Procedure 147: Technology Use
- Administrative Procedure 148: Staff Password Procedure
- Administrative Procedure 170: Communications and Media Relations
- Administrative Procedure 194: Freedom of Information and Protection of Privacy
- Administrative Procedure 195: Records and Information Management
- Administrative 312: Ontario Student Record
- FORM F196-1 Privacy Breach Report
- AiM – Achievement in Motion for Student Success

PRIVACY BREACH REPORT

Unauthorized disclosure of personal information is the defining characteristic of a privacy breach, regardless of whether it was intentional, accidental or the result of a theft or malicious intent. Take immediate action when advised of a suspected privacy breach. Many of the steps outlined below have to be carried out simultaneously or in quick succession. Steps 1 and 2 are to be completed by the supervisor/person the incident is reported to, in consultation with the FOI Coordinator.

STEPS 1 and 2 – Respond / Assess / Contain

Name of person reporting suspected breach	Job Title and Work Location
Supervisor*	Person Incident Reported to (if not supervisor)*
Date and Time of Incident	Contact Number*

What happened?
Where?
What type of personal information was involved?
Who did the personal information belong to (staff, students, etc.)?
Was any action taken to limit or contain breach? Describe. *(e.g. initiated remote wipe, retrieve copies, etc.).*

STEP 3 – Investigate

Analyze/determine who was affected (e.g. employees, parents, students, contractors), and how many.

Describe the events that led to the breach and what form of breach took place.
Was the information lost or stolen? Was the containment effective? How was the information breached? Was the information recovered?
Determine if the incident is breach.

.

- ☐ No. Inform supervisor/person reporting breach. No further action is required
- ☐ Yes. Evaluate the risks, and determine what notification is required.
  - ☐ Does the loss or theft place the individual(s) at risk of physical harm?
  - ☐ Is there a risk of identity theft?
  - ☐ Is there a risk of hurt, humiliation or reputation damage?

Other relevant information.

STEP 4 – Notify

Notify the following as determined and appropriate.

- ☐ individual(s) whose privacy was breached
- ☐ police or other authority
- ☐ third / other party
- ☐ senior administration
- ☐ other departments or employees
- ☐ union or employee groups
- ☐ Board members
- ☐ Office of the Privacy Commission
- ☐ Other_____

STEP 5 – Implement Change

a) Steps taken to correct the problem.
- ☐ Develop, change, or enhance policies and procedures.
- ☐ Ensure strengthening of security and privacy controls.
- ☐ Advise IPC of investigation findings and corrective action.

b) Provide additional notices (as deemed appropriate).
- ☐ Relevant third parties.
- ☐ Consider public announcement (e.g., statement and/or apology).
- ☐ Other Ontario school boards/authorities (where shared responsibilities exist).

c) Prevent future breaches.
- ☐ Arrange employee training/awareness on privacy and security.
- ☐ Recommend appropriate and necessary security safeguards.
- ☐ Consider having an outside party review processes and make recommendations (e.g., auditing company).
- ☐ Evaluate the effectiveness of remedial actions.
- ☐ Other _____

The Director of Education or designate (FOI Coordinator) is required to sign below to formally acknowledge that the breach was handled in accordance with privacy legislation and board policies and procedures.

Name/Title

Signature

Date

Report No: