FORM 196-1	
Adopted	January 2015
Last Revised	August 2017
Review Date	January 2022

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 will 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 officer.

STEPS 1 and 2 – Respond / Assess / Contain

Name of person reporting suspected breach	Job title and work location
Supervisor	Person to whom the incident was reported (if not supervisor)
Date and time of incident	Date

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

STEP 3 – Investigate

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

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 breached 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. Date the notification was made _____

- ☐ individual(s) whose privacy was breached
- ☐ police or other authority
- ☐ third / other party
- ☐ director of education
- ☐ senior administration
- ☐ other departments or employees
- ☐ union or employee groups
- ☐ Board members
- ☐ Information and Privacy Commissioner of Ontario
- ☐ 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 the Information and Privacy Commissioner of Ontario 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 officer) is required to sign below to formally acknowledge that the breach was handled in accordance with privacy legislation and HPEDSB policies and procedures.

_____ _____

Name and title Signature

_____ Report No:

Date