RCDSB
Renfrew County District School Board

INSPIRE. EMPOWER. ACHIEVE.

FORM F182 SECTION: GENERAL ADMINISTRATION	
Adopted/Original Date of Issue	2019
☒ Last Reviewed ☒ Revised	2023
Next Review Date	2028
Contact	**Corporate Services**

PRIVACY BREACH REPORT

Response Protocol

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 privacy breach or suspected privacy breach. Privacy breaches or suspected privacy breaches must be reported to the Principal or Supervisor, or in their absence, the Office of the Superintendent of Business - Corporate Services who is the Freedom of Information Coordinator. 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 Principal/Supervisor/Superintendent the incident is reported to in consultation with the FOI Coordinator. **(The FOI Coordinator completes Steps 3, 4 and 5.)**

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, retrieved copies, etc.).

Step 3 – Investigate

Analyze/determine who was affected (e.g., employees, parents/guardians, 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 a 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

The following were notified (as deemed appropriate).

☐ individual(s) whose privacy was breached	☐ police or other authority (FCS)	☐ Senior Administration
☐ department(s)	☐ union / employee group(s)	☐ Board members
☐ Office of the Privacy Commissioner	☐ third / other party	☐ other

Step 5 – Implement Change

a) Steps taken to correct the problem.
- ☐ Develop, change, or enhance policies and procedures.
- ☐ Ensure strengthening or 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 District policies and procedures.

_____ _____
Name/Title Signature

_____ Report No.: _____
Date

Form History

Approved:	May 2019; June 2023
Revised:	
Reviewed:	June 2023