Procedure No. VI-51

Security Breach Procedure	
Adopted: [illegible]	Last Reviewed/Revised: December 6, 2021
Next Scheduled Review: 2024-2025	
Associated Policies & Procedures: I-[illegible] VI-81 Privacy Procedure I-[illegible] Video Surveillance VI-83 Video Surveillance Procedures I-43 Use of Technology and Digital Citizenship VI-62 Use of Technology and Digital Citizenship	

Purpose

[illegible] responding and recovering from data security incidents in a manner that minimizes its business and legal risks and complies with all legal obligations and relevant legislation, including the *Education Act*, the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA), the *Personal Health Information Protection Act* (PHIPA), the *Personal Information Protection and Electronic* and any other applicable legislation.

Application and Scope

This procedure applies to all HCDSB employees, T[illegible] third-party service providers [illegible]

A [illegible] collected, used, disclosed, retained, or destroyed in a manner inconsistent with privacy legislation or other legal obligations. Confidential information can be personal information, or it can be third-party information or technical information that, if exposed to unauthorized users, can lead to significant harm to HCDSB's technology infrastructure [illegible]

- [illegible]
- [illegible]
- [illegible]
- [illegible]

Document the breach and containment activities in detail

Review of physical and/or technical security

Review of relationships with third party service providers

APPROVED: Regular Meeting of the Administrative Council

AUTHORIZED BY: _____

Director of Education and Secretary of the Board

Appendix A

Security Breach Report

Date of Incident

Name of School/Dept/Business:

Contact information (include contact name, title, facility address and work number/email)

Third Party reporting the Breach

Coordinates of other contacts if applicable

Details of the Incident:

1. Description of the breach (include the cause, context, relevant dates, length of time, and discovery).
2. Description of the personal information involved (name(s) of individuals whose personal information was breached, financial, medical, etc.) **Do not include the personal information in your response, just the types of information that was breached)
3. If the breach involved the loss or theft of a computer, tablet, USB stick, was it password protected or encrypted and if so, what is the procedure for implementing the protection?
4. How many individuals are affected?
5. [illegible]
6. [illegible] workers, ex-
7. Does the breach involve paper or electronic records?
8. How broadly has the personal information been disclosed?
9. Has any other organization (such as law enforcement) been notified of the breach? If so, when were they notified?
10. Security, criminal, regulatory, or other investigations related to this breach? (insurance, other?)
11. Describe the measures taken to contain the breach
12. How the information has been secured? If not, please explain the steps you have or will be taking to obtain the records?
13. [illegible] insight to the complaint to the
14. Describe the measures contemplated or being taken to prevent a recurrence of this incident? Please include details of the training, new policies or procedures, other actions you will be taking?
15. Submit report to the Privacy Officer (privacy@hcdsb.org), cc Director of Education and appropriate