HALTON CATHOLIC DISTRICT SCHOOL BOARD

Procedure No. VI-51

Security Breach Procedure

Adopted:	Last Reviewed/Revised:
December 17, 2018	December 6, 2021
Next Scheduled Review: 2024-2025	

Associated Policies & Procedures:
I-07 Protection of Privacy Policy
VI-81 Privacy Procedure
I-30 Video Surveillance
VI-83 Video Surveillance Procedure
I-43 Use of Technology and Digital Citizenship
VI-62 Use of Technology and Digital Citizenship

Purpose

The Halton Catholic District School Board (HCDSB) is committed to 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 Documents Act,* and any other applicable legislation.

Application and Scope

This procedure applies to all HCDSB employees, Trustees, and third-party service providers.

A security breach occurs when confidential information is compromised, that is, when it is 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, which can then lead to a personal information breach.

HCDSB is committed to treating all information collected/reported in response to security incidents as highly confidential. Internal deliberations about the cause of an incident or the risks to third parties caused by an incident are particularly sensitive.

All individuals with knowledge of information reported under this Procedure and generated by HCDSB during its response to security events must keep it confidential and share it internally only in accordance with this Procedure.

References

Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)

Personal Health Information Protection Act (PHIPA)

Personal Information Protection and Electronic Documents Act (PIPEDA)

Principles

Confidentiality, Integrity and Availability: The HCDSB's Security Breach Procedure will be constructed in a manner that treats all information reported under this Procedure and generated by the HCDSB during its response to security events as highly confidential and shared internally only with those who have a need to know.

Requirements

Information can be compromised in many ways. Some breaches have relatively simple causes and are contained, while others are more systemic or complex. Security breaches are often the result of human error, such as an individual's personal information being sent by mistake to another individual (e.g., fax number, email address, etc.). In today's environment in which technology increasingly facilitates information exchange, sometimes a security breach can be more wide scale, such as when an inappropriately executed computer programming change causes the personal information of many individuals to be compromised.

Internal Reporting Duty

Employees, students, trustees and third parties must:

- report promptly all problems and concerns that relate to a possible or potential breach of information security.
- not attempt to assess or remedy a problem. Any possible breach or threat must be reported right away.
- make reports to the Privacy Office (privacy@hcdsb.org) and IT Services (helpdesk@hcdsb.org). Refer to Appendix A.

Response Protocol for a Security Breach

Step 1 – Respond & Contain

Assess the situation to determine if a breach has occurred.

Report the breach to IT Services, your immediate supervisor, and the Manager of Privacy and Information Management. For breaches not involving technology, report directly to the Manager of Privacy Records Information Management.

- Identify the scope of the breach and contain it:

- retrieve the hard copies of any personal information that has been disclosed,
- determine if the breach would allow unauthorized access to any other personal information [e.g., electronic information system],
- change passwords and identification numbers
- temporarily shut down the system

- Document the breach and containment activities in detail

Step 2 - Assess

Once the security breach is contained:

- Investigate with the involvement of other parties as necessary:
  - Identify and analyze the events that led to the security breach;
  - Evaluate what was done to contain it; and
  - Recommend remedial action so future breaches do not occur.
- Document the results of internal investigation using the Security Breach Report – Appendix A

Step 3 – Notify

Determine if notification is required based on the extent and circumstances surrounding the breach.

The method of notification shall be guided by the nature and scope of the breach and in a manner that reasonably ensures that the affected individual will receive it.

The department associated with the breach will notify the impacted individual. For example, where the breach is for student information, the Principal of the school shall be responsible for providing notification; where the breach is for staff information, Human Resources shall be responsible for providing notification.

Notification will include:

- description of the incident and timing;
- description of the information involved;
- the nature of potential or actual risks or harm;
- what mitigating actions were/are being taken;
- a contact person for questions or to provide further information; and/or
- contact information for the Information and Privacy Commissioner, of Ontario

Step 4 – Implement Change and prevention

A prevention plan may address such issues as:

- Staff training
- Policy review or development

- Review of physical and/or technical security
- Review of relationships with third party service providers
- Audit to ensure that prevention plan has been fully implemented

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

Identification of Third Party (include contact name, title, facility address and work number/email)

Details of the Incident:

1. Description of the breach (include the cause, any technological issues involved, location and discovery).
2. Description of the type of personal information involved (name(s) of individuals, contact information, financial, medical, etc.). **Do not include the personal information in your response, stick to 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. What is the status of the individuals affected? Are they student, employees, trustees, others?
6. Do the parties know each other? (Co-workers, ex-spouses?)
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. Is there any other investigation related to this breach? (Security, criminal, insurance, other?)
11. Describe the measures taken to contain the breach.
12. Has the information been recovered? If not, please explain the steps you have or will be taking to obtain the records?
13. Have the affected individuals been notified of the breach and of their right to complain to the Information and Privacy Commission of Ontario? (Was it my letter, email, telephone, other?)
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 Office (privacy@hcdsb.org), cc Director of Education and appropriate Supervisory Officer.