Northeastern Catholic District School Board

BREACH OF PERSONAL INFORMATION

Administrative Procedure: APP025

POLICY STATEMENT

The Northeastern Catholic District School Board (NCDSB) is committed to protecting the personal information under its care and control. The *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)* establishes rules to follow to ensure the protection of individual privacy.

REFERENCES

Education Statutes and Regulations of Ontario
Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)
Personal Health Information Protection Act (PHIPA)
Personal Information Protection and Electronic Documents Act (PIPEDA)
Ontario School Record (OSR) Guideline 2000
NCDSB Policy Personal Information Management
NCDSB Personal Information Management Procedure

DEFINITIONS

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.

Personal information can be compromised in many ways. Some breaches have relatively simple causes, 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, a privacy breach could be more wide-scale.

PROCEDURES

1.0 GENERAL INFORMATION

1.1 Board staff upon learning of a breach or suspected breach, shall immediately take the following actions:

- 1.1.1 Contain the breach to stop any more information from being revealed;
- 1.1.2 Assess the extent of the breach;
- 1.1.3 Notify the immediate supervisor and the individual responsible for Freedom of Information, Privacy and Records Information Management; and
- 1.1.4 Complete a Privacy Breach Summary Report.

2.0 ASSESS

2.1 The Principal or Manager shall assess the breach by asking the following two questions. If the answer to **both** questions is yes, then it can be assumed that a breach has occurred.

2.1.1 Is there personal information involved? *Refers to information about an identifiable or potentially identifiable individual and includes, but it not limited to, personal health information and opinions about the individual.*

2.1.2 Has an unauthorized collection, use, disclosure or retention or personal information occurred? *Unauthorized disclosure is the defining characteristic of a privacy breach. Regardless of whether it is intentional, accidental, or the result of theft or malicious intent, an unauthorized disclosure constitutes a privacy breach.*

3.0 CONTAINMENT

3.1 The first step in responding to a privacy breach is to stop the inappropriate flow of data. This may include such actions as:

3.1.1 Taking down a website;

3.1.2 Retrieving items from garbage bins;

3.1.3 "Unsending" an email, if possible;

3.1.4 Recovering records;

3.1.5 Revoking or changing computer access codes or correcting weaknesses in physical or electronic security.

3.2 The main goal is to alleviate any consequences for both the individual(s) whose personal information was involved and the Board.

3.3 The Principal and/or Manager shall document all containment activities or attempts to contain.

4.0 INVESTIGATE

4.1 Once the privacy breach is confirmed and contained, the Principal or Manager shall conduct an investigation to determine the cause and extent of the breach by:

4.1.1 Identifying and analyzing the events that led to the privacy breach;

4.1.2 Evaluating if it was an isolated incident or if there is risk of further exposure of information;

4.1.3 Determining who was affected by the breach; e.g. student or employees and how many were affected;

4.1.4 Evaluating the effect of containment activities;

4.1.5 Evaluating who had access to the information;

4.1.6 Evaluating if information was lost or stolen; and,

4.1.7 Evaluating if the personal information has been recovered.

5.0 NOTIFICATION

5.1 Notification helps to ensure that the affected parties can take remedial action, if necessary, and to support a relationship of trust and confidence. The Principal or Manager shall consult with the Superintendent of Education and the Privacy Information Officer to determine what notifications are required. Considerations may include:

- 5.1.1 The affected individual's reasonable expectation of notification shall be considered.
- 5.1.2 Is the recipient of the personal information bound by professional duties of confidentiality or members of colleges that may be sanctioned if confidentiality is breached, i.e. a teacher is who is a member of the College of Teachers?
- 5.1.3 Is there a risk of identity theft or other fraud? How reasonable is the risk? It is a concern if the breach included unencrypted information such as name in conjunction with social insurance number or license numbers.
- 5.1.4 Could the loss or theft of information lead to hurt, humiliation, or damage to an individual's reputation? This type of harm can occur with the loss or theft of information such as mental health records, medical records or disciplinary records.
- 5.1.5 Could the loss of theft of information result in damage to an individual's reputation, affecting his/her business or employment opportunities?

5.2 Notification to authorities or organizations could include police if theft or other crime suspected; insurers; Information and Privacy Commissioner (IPC); credit card companies; financial institutions; unions or other employee groups or staff.

5.3 Affected individuals shall be promptly notified. Depending on the nature and scope of the breach and status of the investigation, notification may occur in stages. For instance, the Principal or Manager can make an initial notification directly along with updates as required and a report of the findings upon completion of the investigation.

5.4 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(s) will receive it. Direct notification by telephone, letter, and email or in person is preferable and shall be used where the individual is identified. If, for example, it is a system breach containing student information, posted notices, media releases, website notices or letters to all students or staff shall be considered.

5.5 Ideally, the individual(s) shall be notified by the department associated with the breach. 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 Resource Services shall be responsible. The Privacy Information Officer may be referred to as a contact for questions.

5.6 Notification shall include:

- 5.6.1 Description of the incident and timing.
- 5.6.2 Description of the information involved.
- 5.6.3 The nature of potential or actual risk or harm.
- 5.6.4 What mitigating actions were/are being taken.
- 5.6.5 Appropriate actions for individuals to take in order to protect themselves against harm; and

5.6.6 A contact person for questions or to provide further information and/or contact information for the Information and Privacy Commissioner (IPC).

6.0 PREVENTION OF FUTURE BREACHES

6.1 Once the breach has been resolved, the Privacy Information Officer shall work with the Principal, Manager or Superintendent to develop a prevention plan or take corrective actions, if required. The extent of the response shall be determined by the significance of the breach and whether it was systemic or isolated. Responses could include, audits, review of policies, procedures and practices; employee training; or review of delivery partners.

Director of Education: *Tricia Stefanic Weltz*

Date: April 2019

383 Birch Street North, Timmins ON P4N 6E8
[T] 705-268-7443 [F] 705-267-3590 [W] www.ncdsb.on.ca