Niagara Catholic District School Board

PRIVACY BREACH PROTOCOL

OBJECTIVE

Every person acting on behalf of the Niagara Catholic District School Board shall make a reasonable effort to protect personal information in their custody or control, and to immediately notify their Supervisor, upon becoming aware of a breach or suspected breach and contain a privacy breach through a prompt, reasonable and coordinated effort as outlined in this procedure.

DEFINITIONS

Privacy Breach

A Privacy Breach is any event causing personal information to be compromised when it is collected, used, disclosed, retained or destroyed in a manner inconsistent with applicable privacy legislation, and the Niagara Catholic District School Board's Privacy Policy.

IT Security Breach

An incident that results in unauthorized access of data, applications, services, networks and/or devices by bypassing underlying security mechanisms. This is also known as a security violation. Examples of incidents that can result in a security breach include phishing emails, ransomware attacks, brute-force attack (guessing passwords) and malware.

Person

An employee, a volunteer, or a Trustee of the Niagara Catholic District School Board, or a third-party service provider who is in possession of personal information collected or held by or on behalf of the Board.

Personal Information

The *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) defines 'personal information' as any recorded information about an identifiable individual, including:

- Information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual;
- Information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or relating to financial transactions in which the individual has been involved;
- Any identifying number, symbol or other particular assigned to the individual;
- The address, telephone number, fingerprints or blood type of the individual;
- The personal opinions or views of the individual except if they relate to another individual;
- Correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence;
- The view or opinions of another individual about the individual;
- The name of the individual if it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

Personal Health Information

Information about an individual that pertains to health care, including information about an individual's physical or mental health, receipt of health care services.

Third-Party Service Providers

These are contracted third parties procured for the purpose of carrying out or managing programs and/or services on behalf of the Board. For the purpose of privacy breach reporting third party includes all contractors that receive personal information from the Board, or collect personal information on behalf of the Board. Examples include: school photographers, bus companies, external data warehouse services and outsourced administrative services such as external researchers and consulting services.

EXAMPLES

Personal information can be compromised in many ways. Some privacy breaches have relatively simple causes and are contained, 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 (e.g., fax number, e-mail address, etc.). In today's environment in which technology increasingly facilitates information exchange, sometimes a privacy breach can be more widespread, such as when an inappropriately executed computer programming change causes the personal information of many individuals to be compromised.

Privacy beaches may be relatively obvious while others may not be as apparent. A privacy breach has occurred when there is an inappropriate collection, disclosure, use, retention, disposal or security of personal information.

Examples of potential privacy breaches include:

- Lost or misplaced personal information, such as a misplaced student assessment, report card or Ontario Student Record (OSR) or a lost USB stick containing student marks or employee contact information;
- Stolen technologies or equipment such as laptops, iPads or smart phones that may contain personal information;
- Disclosure of personal information to an unauthorized person or group, such as student information forms given to the wrong students or personal information disclosed to a Board member or employee who did not need it to effectively decide on a matter;
- Deliberate disclosure of personal information to an unauthorized person or group for fraudulent or other purposes;
- Inappropriate disclosure of personal information, such as two employees discussing and identifying a student in a grocery store, or a similar conversation on a cell phone in a public place;
- Information used for the purpose not consistent with the reason it was collected, such as sharing of staff or parent contact information for the purpose of sales or marketing or providing personal student information for a third party sponsored contest, without informed consent; and
- Disposal of equipment with memory capabilities, such as USB sticks, laptops or photocopiers, or paper records containing personal information in a non-secure manner.

ROLES AND RESPONSIBILITIES IN RESPONDING TO A PRIVACY BREACH

All employees are responsible for:

- Being alert to the potential for personal information to be compromised, and therefore potentially playing a role in identifying, notifying, and containing a breach;

- Notifying their Supervisor immediately, or, in their absence, the appropriate Superintendent or the Privacy and Risk Advisor, upon becoming aware of a breach or suspected breach; and
- Containing, if possible, the suspected breach by suspending the process or activity that caused the breach.

Principals, Managers, Supervisors and Senior Administration are responsible for:

- Alerting the Privacy and Risk Advisor of a breach or suspected breach and working with the Privacy and Risk Advisor to implement the five steps of the response procedure;
- Obtaining all available information about the nature of the breach or suspected breach, and determining what happened;
- Working with the Privacy and Risk Advisor , to undertake all appropriate actions to contain the breach; and
- Ensuring details of the breach and corrective actions are documented.

The Board's Privacy and Risk Advisor is responsible for:

- Ensuring that all five steps of the response procedure are implemented;
- Supporting the Principal, Manager, Supervisor and Senior Administration in responding to the breach; and
- Notifying the Office of the Information and Privacy Commissioner of Ontario where appropriate.

Director of Education or designate is the accountable decision-maker responsible for:

- Briefing Senior Administration and Board members as necessary and appropriate;
- Reviewing internal investigation reports and approving required remedial action;
- Monitoring implementation of remedial action; and
- Ensuring urgent notification to those whose personal information has been compromised.

Cyber Security Incident Response Team (CSIRT) is led by the Chief Information Officer (CIO) and is responsible for:

- Reporting to Senior Administration and Board members when required; and
- Activating the incident response plan, to investigate and respond to cyber security incidents.

Communications Officer is responsible for:

- Ensuring that internal/external stakeholders, customers, and the public are informed of an incident when required, and in a timely fashion.

Third-party service providers are responsible for:

- Taking reasonable steps to monitor and enforce their compliance with the privacy and security requirements defined in the contracts or service agreements;
- Informing the Board contact or Privacy and Risk Advisor, of all actual and suspected privacy breaches;
- Documenting how the breach was discovered, what corrective actions were taken and report back;
- Undertaking a full assessment of the privacy breach in accordance with the third party service providers' contractual obligations;
- Taking all necessary remedial action to decrease the risk of future breaches; and
- Fulfilling contractual obligations (especially the right to audit clause) to comply with privacy legislation, including

RESPONSE PROCEDURE

All privacy breaches or suspected privacy breaches must be reported to the principal or supervisor, or in their absence, to the appropriate superintendent or the Privacy and Risk Advisor. Once reported, the

supervisor or superintendent will contact the Privacy and Risk Advisor, and the following response steps are to be implemented.

STEP 1 – RESPOND and ALERT

- Assess the situation to determine if a breach or potential breach has indeed occurred and what needs to be done.
- When a breach has been identified, contact the appropriate area to respond to the breach.
- Report the privacy breach to key persons in the Board (the Director, Privacy and Risk Advisor or Coordinator of Information Management/Privacy and Freedom of Information) and, if necessary, to law enforcement. In the event of a cyber-security, incident/breach please notify the Chief Information Officer.

STEP 2 – CONTAIN

- Identify the scope of the breach and contain it. Containment involves taking immediate action to put an end to the unauthorized access, where possible. For example, retrieving hard copies of any personal information that has been disclosed, revoking or changing passwords and identification numbers, temporarily shutting down the system/ device, or correcting weakness in physical or electronic security.
- Document the breach and containment activities.
- Develop briefing materials.
- Brief key persons on the privacy breach and how it is being managed.

STEP 3 – INVESTIGATE

Once the privacy breach is contained:

- Conduct an investigation with the involvement of other parties as necessary
- Identify and analyze the events that led to the privacy breach;
- Evaluate what was done to contain it; and
- Recommend remedial action so future breaches do not occur.

Document the results of internal investigation and use the privacy breach checklist for record keeping, including:

- Background and scope of the investigation;
- Legislative implications;
- How the assessment was conducted;
- Source and cause of the breach;
- Inventory of the systems and programs affected by the breach;
- Determination of the effectiveness of existing security and privacy policies, procedures, and practices;
- Evaluation of the effectiveness of the Ontario school board's/authority's response to the breach;
- Findings including a chronology of events and recommendations of remedial actions;
- The reported impact of the privacy breach on those individuals whose privacy was compromised.

STEP 4 – NOTIFY

Notification helps to ensure that affected parties can take remedial action if necessary to support a relationship of trust and confidence. The Privacy and Risk Advisor shall consult with the Director of Education to determine what notifications are required. A Privacy breach caused by Niagara Catholic staff will be reported to the Information and Privacy Commissioner of Ontario and the Ministry of Education. Depending on the nature of the breach other considerations may include notification to the

affected individual, the police, financial institutions or other parties that may be affected; other departments and employees; unions or employee groups and the Board members.

In determining if notification is required to the affected individual(s) the following shall be considered:

- **Risk of Identity Theft -** Is there a risk of identity theft or other fraud in your Ontario school board/authority? How reasonable is the risk? Identity theft is a concern if the breach includes unencrypted information such as names in conjunction with social insurance numbers, credit card numbers, driver's license numbers, personal health numbers, debit card numbers with password information, or any other information that can be used for fraud by third parties (e.g., financial).
- **Risk of Physical Harm -** Does the loss or theft of information place any individual at risk of physical harm, stalking, or harassment?
- **Risk of Hurt, Humiliation, or Damage to Reputation -** 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.
- **Risk of Loss of Business or Employment Opportunities -** Could the loss or theft of information result in damage to an individual's reputation, affecting his/her business or employment opportunities?

Notification should be done promptly, and shall include:

- A description of the incident and the information involved;
- The nature of potential or actual risks or harm;
- Containment steps taken;
- What mitigating actions the Board is taking;
- Appropriate action for individuals to take to protect themselves against harm;
- A contact person for questions or to provide further information; and
- Contact for the information privacy commissioner, if the office of the information and privacy commissioner (IPC) is investigating. Include an explanation of the individual's right to complain to the IPC.

STEP 5 – IMPLEMENT CHANGE

When determining what changes and remedial actions need to be implemented, consider whether it is necessary to:

- Review the relevant information management systems to enhance compliance with privacy legislation;
- Amend or reinforce the existing policies, procedures, and practices for managing and safeguarding personal information;
- Develop and implement new security or privacy measures, if required;
- Review employee training/awareness on legislative requirements, security and privacy procedures and practices to reduce potential or future breaches, and strengthen as required;
- Test and evaluate remedial actions to determine if they have been implemented correctly and if policies, procedures, and practices need to be modified; and/or
- Recommend remedial action to the Director of Education or designate.

REFERENCES

- ***Education Act and Regulations (R.S.O. 1990 c.E.2)***
- ***Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)***
- ***Office of the Information and Privacy Commissioner of Ontario (IPC)***
- ***Personal Health Information Protection Act (PHIPA)***

- ***Personal Information and Protection of Electronic Documents Act (PIPEDA)***
- ***Privacy and Information Management PIM Toolkit***
- ***Niagara Catholic District School Board Policies/Procedures/Protocols***
  - ***Privacy Policy (600.6)***
  - ***Records and Information Management Policy (600.2)***
  - ***Freedom of Information Request Procedure***