Nipissing-Parry Sound Catholic District School Board	PRIVACY BREACH POLICY AND PROTOCOL	AG 38.0

Policy Section **Administration - General**	*Original Approval Date* **2018 08 29**	*Revision Date(s)*	*Review Date(s)*

POLICY STATEMENT

The Nipissing-Parry Sound Catholic District School Board ("the Board") is committed to maintaining an effective Privacy and Information Management (PIM) program, including a protocol for dealing effectively with a privacy breach, should one occur.

POLICY SCOPE

This policy and protocol applies to personal information in all records within the custody or under the control of the Board and addresses all aspects of Board operations, including all records made or received in the day-to-day business operations of the school or Board, regardless of the medium in which those records are stored and maintained.

PURPOSE

The protocol attached to this policy is intended to assist the Board with containing and otherwise responding to incidents involving the loss, theft or unauthorized access, use and/or disclosure of personal information.

Everyone has a role and responsibility to assist in the containment of a privacy breach.

DEFINITIONS

In this Policy and Protocol:

"FOI Coordinator" means the person designated by the Board to oversee its compliance with MFIPPA and/or its privacy program;

"IPC" means the Information and Privacy Commissioner of Ontario (who enforces compliance with MFIPPA) and his office;

"institution" means an organization to which MFIPPA applies;

"personal information" means recorded information about an identifiable individual as more particularly defined in Municipal Freedom of Information and Protection of Privacy Act ("MFIPPA");

"privacy breach" means any collection, access, use, disclosure or destruction of personal information in contravention of MFIPPA.

GUIDELINES

Privacy Breaches

The Board is an institution, responsible for managing personal information in its custody or under its control in compliance with MFIPPA.

A privacy breach may occur in any number of ways. Some 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 personal information being sent by mistake to an unintended recipient (e.g. to the wrong fax number or email address, etc.) They may also be intentional, such as when individuals view personal information for purposes outside of those for which the information was collected, including as a matter of curiosity or to advance their own interests. In today's environment in which technology increasingly facilitates information exchange, privacy breaches can be wide-scale, such as when a change or upgrade to software is not carried out properly and causes the personal information of many individuals to be comprised.

The following are some examples of privacy breaches:

	Student Records	Employee Records	Business Records
Inappropriate disclosure / use of personal information	Two teachers discussing a student by name in the local grocery store. Student's report card mailed to the wrong address. With certain exceptions, digital images of individuals taken and displayed without consent. Hard-copy psychological assessments kept in file cabinets that are not secured or controlled and are in openly accessible areas. Confidential student health records inadvertently blown out of a car trunk and scattered over a busy street.	Employee files containing social insurance numbers left in unlocked boxes in an open/accessible area. Budget reports (containing employee numbers and names) found in unsealed recycle bins and garbage bins. Theft from a car of a briefcase containing a list of home addresses of teaching staff.	A list of names and bank account numbers left on the photocopier. Personal information disclosed to employees/trustees who did not need it, for example to decide a matter.

	Student Records	Employee Records	Business Records
Technology / computer error	Lost memory key containing student personal information. Theft of a teacher's laptop containing Special Education student records on the hard drive. Sharing files or folders electronically with staff or members of the public who do not require access.	Sending very sensitive personal information to an unattended, open area printer. Password written on a sticky note stuck to a monitor creates a security breach which may result in a privacy breach if someone uses the password to access private student or employee information. Resumes faxed or emailed to a wrong destination or person.	Stolen or misplaced laptop containing names and addresses of permit holders. Personal information scanned and not cleared from multifunctional office machine. Disposal of equipment with memory capabilities (e.g., memory keys, disks, laptops, photocopiers, fax machines, or cell phones) without secure destruction of the personal information it contains.

Roles and Responsibilities in Responding to Privacy Breaches

It is essential that privacy breaches get reported to the appropriate personnel as soon as they are detected. The following personnel may need to be involved when the Board responds to a privacy breach. Some of the following roles and responsibilities may be undertaken concurrently.

Individuals	Roles	Responsibilities
Employees	All Board employees need to be alert to the potential for personal information to be compromised, so that they can recognize a breach, notify the appropriate personnel and take steps to contain the breach.	All Board employees have the responsibility to: • notify their supervisor immediately, or, in his/her absence, their school board's FOI Coordinator upon becoming aware of a breach or suspected breach;

Individuals	Roles	Responsibilities
	Employees dealing with student, employee and/or business records that contain personal information need to be particularly aware of how to identify and respond to a privacy breach.	• contain, if possible, the suspected breach by suspending the process or activity that caused the breach.
Senior Administration, Managers, and Principals	Senior administration, managers, and principals are responsible for alerting the FOI Coordinator of a breach or suspected breach and will work with the FOI Coordinator or Privacy Officer to implement the five steps of the response protocol found in Appendix B.	Senior administration, managers and principals have the responsibility to: • alert the FOI Coordinator and provide as much information about the breach as is currently available; • obtain all available information about the nature of the breach or suspected breach, and determine, to the extent possible, what happened; • work with FOI Coordinator to undertake all appropriate actions to contain the breach; • Accurately complete Appendix B – FOI Coordinator Privacy Breach Checklist & Reporting Form in conjunction with FOI Coordinator.
FOI Coordinator	The FOI Coordinator plays a central role in the response to a breach by ensuring that all five steps of the response protocol are implemented (see Appendix B for more details).	The FOI Coordinator will follow the following five steps (see Appendix B for more details): Step 1 – Respond to the privacy breach report

Individuals	Roles	Responsibilities
	The FOI Coordinator may be authorized to obtain legal advice or other expert assistance as required, with permission from the Director of Education for such consultations.	Step 2 – Contain the breach Step 3 – Investigate the breach Step 4 – Notify the appropriate individuals if breach has occurred (See Appendix B) Step 5 – Implement any required changes identified through the investigation.
Director of Education	The Director of Education is responsible for making decisions arising from a privacy breach investigation, including breach notification and changes to policies or procedures.	The Director of Education has the responsibility to: • brief senior management and trustees as necessary and appropriate; • review internal investigation reports and approve any remedial action identified; • monitor implementation of remedial action; • ensure that any required notices are given.
Third Party Service Providers	Increasingly, Ontario school boards/ authorities use contracted third party service providers to carry out or manage programs or services on their behalf. Typical third party service providers are commercial school photographers, bus companies, external data	The third party service providers need to be required to: • inform the Board contact as soon as a privacy breach or suspected breach is discovered; • take all actions to contain the privacy breach as directed by the Board;

Individuals	Roles	Responsibilities
	warehouse services, outsourced administrative services (such as cheque production, records storage and shredding), external researchers and external consultants. Other third parties that may have a role in managing events or occurrences include the Children's Aid Societies (CAS), Public Health Units (PHU). It is important to note that these organizations are not 3rd party service providers "using" personal information on behalf of school boards, but rather 3rd party agencies to which personal information may be disclosed. Third party service providers, not the Board, are responsible for their use of personal information disclosed to them by the Board. In regard to personal information provided to third party providers, the Nipissing-Parry Sound CDSB retains responsibility for protecting the personal information while it is being used by suppliers. Therefore, contracts with third party providers need to clearly set out what the provider is entitled to do with personal information and that they do not acquire any ownership rights to the information by providing their services. Contracts MUST require the third party to comply with the requirements of	• document how the breach was discovered, what corrective actions were taken and report back; the Board may also undertake this step; • undertake a full assessment of the privacy breach in accordance with the third party service providers' contractual obligations; • cooperate with and assist the board in conducting such an assessment; • take all necessary remedial action to decrease the risk of future breaches; • comply with privacy legislation. Contracts MUST require the third party to comply with the requirements of MFIPPA.

Individuals	Roles	Responsibilities
	MFIPPA. The contracts should also include the duty to notify the Board if personal information they are using is compromised. All third party service providers must be contractually required to take reasonable steps to monitor and enforce their compliance with the privacy and security requirements in the contracts or service agreements, and to inform the Board of all actual and suspected privacy breaches.	

References and Related Administrative Procedures and Guidelines (APGs)

- Education Act Ontario
- Policy PB 10.0 NPS 5-9 Collection, Protection of and Access to Personal Information of Private Individuals and/or Board Employees
- Policy S 11.0 NPS 5-99 Protection of and access to Personal Information of Students including OSR's
- Policy AG 10.0 NPS 5-99 Access to General Information of the Board
- Policy AG 28.0 Records Management
- Adapted from a model created by the PIM Taskforce

Appendices

A. APPENDIX A – RESPONDING TO A SUSPECTED PRIVACY BREACH

This appendix may be used (in the form of a poster or posted on an intranet) to promote and raise the awareness of responsibilities in the event of a privacy breach.

B. APPENDIX B – FOI COORDINATOR PRIVACY BREACH CHECKLIST & REPORTING FORM

This appendix is a management tool for the Board's Freedom of Information (FOI) Coordinator or designates to use in the event of a privacy breach.

RESPONDING TO A SUSPECTED PRIVACY BREACH GUIDANCE DOCUMENT

RESPONDING TO A SUSPECTED PRIVACY BREACH

PRIVACY is...	**...**the **right to control** access to your personal information, and the **right to decide** what and how much information you give to others, who it is shared with, and for what purposes.
A PRIVACY BREACH occurs when...	**...personal information** that is collected, used, disclosed, retained or destroyed in a manner **that does not meet privacy requirements** set out in federal and provincial privacy legislation. ***Examples*** *of privacy breaches may include, but are not limited to: memory key/jump drive left in a public area containing student data; laptop lost or stolen containing student records on the hard drive; documents containing student or employee personal information left unattended on a photocopier; reports containing employee personal information found unshredded in recycle bins or garbage bins; confidential documents left in public view on an employee's desk or other publicly accessible area.*
If you suspect a PRIVACY BREACH has occurred, YOU are encouraged to...	**...notify** your Supervisor immediately, or, in his/her absence, your School Board's Freedom of Information (FOI) Coordinator Anna Marie Bitonti at 705-472-1201 ext. 31243; **...contain**, if possible, the suspected breach by delaying or stopping the process or activity involving the exposure or mishandling of student or employee personal information. Following your report of the suspected breach, the FOI Coordinator may contact you to confirm details about the suspected breach. No further action is required on your part unless further directed by your Supervisor and/or the Board's FOI Coordinator.

Credit to:

FOI COORDINATOR PRIVACY BREACH CHECKLIST & REPORTING FORM

BREACH REPORT # _____

You must take immediate action when you have been advised of a suspected privacy breach. Many of the steps outlined below should ideally be carried out simultaneously or in quick succession. Steps 1 and 2 are completed based on the information received either directly from an employee, or from his/her immediate supervisor (by phone call, for example), or in written form (by email, for example).

Step 1 – Respond to Report

1. **Person Reporting Suspected Breach**:

   First name: _____ Last name: _____

   Job title: _____

   Location (school department): _____

   Name of immediate supervisor: _____

   Phone number: _____

2. **When Incident/Event Occurred**:

   Date: _____ **Time:** _____
   (mm/dd/yyyy) (indicate AM or PM)

3. **Incident/Event Details:**

   Number of individuals whose information was affected (NOTE: this may not be known until an investigation has been conducted):

   _____

   Type of personal information that was involved (health/medical information, student marks, biographical information (such as home address, phone numbers, names and contact information of family members), behaviour concerns etc.):

   To whom the personal information belongs (student, employee, third party (someone who is neither a student nor employee of the Board, such as a parent/guardian or volunteer)):

Step 2 – Contain the Activity Threatening the Security or Integrity of Personal Information

Who was involved and what did they do with the affected personal information:

Steps taken/efforts made to contain any privacy breach (suspending the process/activity that caused the breach, requesting the return or destruction of the personal information):

Step 3 – Investigate

Conduct an investigation of the event/incident to determine if a breach has occurred, and to fill in any of the details described in paragraphs 2 and 3 above. Note: Consultation with any or all of legal counsel, law enforcement agents, and forensic technology experts may be undertaken to assist in the investigation.

If a breach HAS NOT occurred: contact the person who reported the suspected breach **and** his/her immediate supervisor to advise him/her of your determination. No further action is required by the employee or supervisor.

Step 4 – Notify

If a breach HAS occurred: **notify** the following individuals, where affected individuals can take steps to prevent or mitigate any harm arising from the breach, or where the Office of the Information and Privacy Commissioner should be alerted that it may be receiving complaints from affected individuals.

☐ Individuals whose privacy was breached	☐ Legal counsel
☐ Accountable decision maker (Director of Education)	☐ IPC*
☐ Senior administration/managers/principals	☐ Other

*Note: At present, there is no requirement under MFIPPA to notify the IPC of breaches. The type and extent of the breach will influence your decision to notify the IPC [(1-800-387-0073) 2 Bloor Street East, Suite 1400, Toronto, Ontario, M4W 1A8]. It may be helpful to refer to the IPC's guidance documents on managing privacy breaches and more specifically:

- "Privacy Breach Protocol, Guidelines for Government Organizations" posted on the IPC's website at **https://www.ipc.on.ca/wp-content/uploads/Resources/Privacy-Breach-e.pdf;** and
- "Breach Notification Assessment Tool", posted at **https://www.ipc.on.ca/wp-content/uploads/Resources/ipc-bc-breach-e.pdf**.

Step 5 – Identify and Implement any Required Changes/Remediation

Steps taken to correct the problem/prevent a recurrence:
☐ Develop, change, or enhance policies and procedures including those on use of mobile devices and social media
☐ Enhance privacy training materials or the frequency of privacy training/refresher training
☐ Strengthen security and privacy controls through means such as annual agreements with staff, tracking of privacy training, restricting access, auditing access, pop-up notices on screens

Provide additional notices (as deemed appropriate):
☐ Advise IPC of investigation findings and corrective action
☐ Relevant third parties
☐ Consider public announcement
☐ Other Ontario school boards/authorities (for example, where shared responsibilities exist)

Prevent future breaches:
☐ As above, enhance employee training on privacy and security/notices of consequences of breaching privacy
☐ Enhance security safeguards
☐ Consider having an outside party review processes and make recommendations (security audit)
☐ Evaluate the effectiveness of remedial actions

The FOI Coordinator may wish to review Board policies, procedures, practices, and training materials to ascertain whether any revisions are required to ensure a clearer understanding of what can and cannot be done with personal information and how to respond to a suspected privacy or security breach.

Sign-off

Consider having the Director of Education or designate (e.g. FOI Coordinator) sign the checklist to formally acknowledge that the response to the notice of a breach or suspected breach was handled in accordance with the Board's policies and procedures.

_____ _____
Print Name/Title Signature

Sign-Off Date: _____
(mm/dd/yyyy)

Note: this form must be stored (or copied) in the Director's Office.