Hamilton-Wentworth Catholic District School Board
Believing, Achieving, Serving

Policy Manual – Administration

A.17 – Privacy Breach - PROCEDURES

PROCEDURES

1. Employees dealing with student, employee and/or business records need to be particularly aware of how to identify and address a privacy breach.

   All Board employees have the responsibility to:

   - notify their supervisor immediately, or, in his/her absence, the Board's Freedom of Information (FOI) Coordinator upon becoming aware of a breach or suspected breach; and,
   - contain, if possible, the suspected breach by suspending the process or activity that caused the breach.

   Appendix A contains a list of privacy breach examples.

   The Privacy Breach Protocol is outlined in Appendix B.

2. Senior administration, managers/supervisors, and principals are responsible for alerting the FOI Coordinator of a breach or suspected breach and will work with the coordinator to implement the steps of the response protocol.

   Senior administration, managers/supervisors, and principals have the responsibility to:

   - obtain all available information about the nature of the breach or suspected breach, and determine what happened;
   - alert the FOI Coordinator and provide as much information about the breach as is currently available;
   - work with FOI Coordinator to undertake all appropriate actions to contain the breach;
   - ensure details of the breach and corrective actions are documented; and,
   - complete the Privacy Breach Report (Appendix C).

3. The FOI Coordinator plays a central role in the response to a breach by ensuring that all steps of the response protocol are implemented. The FOI Coordinator will:

   Step 1 – Respond;
   Step 2 – Contain;
   Step 3 – Investigate;
   Step 4 – Notify; and,
   Step 5 – Implement Change

4. The responsibility for protecting personal information affected by a privacy breach shall be assigned to the Director of Education, an accountable decision maker.

   The Director of Education shall be the key decision maker in responding to privacy breaches.

   The Director of Education, as the accountable decision maker, has the responsibility to:

   - brief senior management and trustees as necessary and appropriate;
   - review internal investigation reports and approve required remedial action;
   - monitor implementation of remedial action; and,
   - ensure that those whose personal information has been compromised are informed as required.

5. The Board, at times, makes use of contracted third party service providers to carry out or manage programs or services on its behalf. In such circumstances, the Board retains responsibility for protecting personal information in accordance with privacy legislation. It is incumbent upon the Board that all third party contracts or service agreements entered into ensure compliance with privacy policies and legislation.

   [Typical third party service providers are commercial school photographers, bus companies, external data warehouse services, outsourced administrative services (such as cheque production, records storage and shredding), Children's Aid Societies (CAS), Public Health Units (PHU), external researchers, and external consultants.]

   Third party service providers need to know their roles and responsibilities if a privacy breach occurs when they have custody of personal information for which the Board is responsible.

All third party service providers must take reasonable steps to monitor and enforce their compliance with the privacy and security requirements defined in the contracts or service agreements, and are required to inform the Board of all actual and suspected privacy breaches

The third party service providers have the responsibility to:

- inform the Board contact (FOI Coordinator) as soon as a privacy breach or suspected breach is discovered;
- take all necessary actions to contain the privacy breach as directed by the Board;
- document how the breach was discovered, what corrective actions were taken and report back;
- undertake a full assessment of the privacy breach in accordance with the third party service providers' contractual obligations;
- take all necessary remedial action to decrease the risk of future breaches; and,
- fulfill contractual obligations to comply with privacy legislation and Board policy.

Appendix A

PRIVACY BREACH EXAMPLES

Personal information can be compromised in many 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 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 privacy 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.

The following are some examples of privacy breaches:

	Student Records	Employee Records	Business Records
Inappropriate disclosure/use of personal information	Two staff members discussing (and identifying) a student in the local grocery store. Student's report card mailed to the wrong home address. Digital images of individuals taken and displayed without consent. Hard-copy psychological assessments kept in openly accessible file cabinets that are not secured or controlled. 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 near the open shipping/ receiving area. Budget reports (containing employee numbers and names) found in their entirety in recycle bins and garbage bins. Theft from car of a briefcase containing a list of home addresses of teaching staff.	A list of names, including credit card numbers, left on the photocopier.
Technology/ computer error	Lost **storage device** containing student data. Theft from teacher's car of a laptop containing Special Education student records on the hard drive.	Sending very sensitive personal information to an unattended, open-area printer. Password written on a sticky note stuck to a monitor. Resumes faxed or emailed to a wrong destination or person.	Stolen laptop containing names and addresses of permit holders. Tender information scanned and not cleared from multifunctional office machine. Disposal of equipment with memory capabilities (e.g., memory stick, storage devices**,** disks, laptops, photocopiers, fax machines, or cell phones) without secure destruction of the personal information it contains.

Appendix B

HAMILTON-WENTWORTH CATHOLIC DISTRICT SCHOOL BOARD

PRIVACY BREACH PROTOCOL

PURPOSE
It is the responsibility of the Hamilton-Wentworth Catholic District School Board (Board) to contain and respond to incidents involving unauthorized disclosure of personal information.

All employees have a role and responsibility to notify and assist in the containment of a privacy breach. Use the Privacy Breach Report in Appendix C in conjunction with this protocol.

The Benefits of a Privacy Breach Protocol are**:**

- quick and coordinated response;
- roles and responsibilities;
- effective investigation process; • effective containment process; and,
- easier remediation.

The Five Steps Implemented Concurrently by Tte Freedom Of Information (FOI) Coordinator.

The following steps are to be initiated as soon as a privacy breach or suspected breach has been reported.

STEP 1 – RESPOND

- Assess the situation to determine if a breach has indeed occurred and what needs to be done;
- When a privacy breach is identified by an internal or external source, contact the appropriate area to respond to the breach;
- Provide advice on appropriate steps to take to respond to the breach;
- Report the privacy breach to key persons within the Board (including the Director of Education or designate) and, if necessary, to law enforcement; and,
- Evaluate effectiveness of response to the breach and implement improvement as necessary.

STEP 2 – CONTAIN

- Identify the scope of the breach and contain it (e.g., 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 and/or temporarily shut down the system if necessary to contain the breach);
- Document the breach and containment activities;
- Develop briefing materials; and,
- Brief the Director of Education, senior management, and 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. Document the results of the internal investigation using Appendix C.

STEP 4 – NOTIFY

- Notify, as required, the individuals whose personal information was disclosed **immediately upon discovery of the breach or as soon as possible thereafter. The preferred method of notification is direct – by phone, letter or in person – to affected individuals. Indirect notification – website information, posted notices, media – should generally only occur where direct notification could cause further harm, is prohibitive in cost, or contact information is lacking. Using multiple methods of notification in certain cases may be the most effective approach. See Appendix D for sample letter.**

The purpose of providing notice of a privacy breach to the individuals whose personal information was involved in the incident is to provide them with information about:

- what happened;
- the nature of potential or actual risks or harm;
- what mitigating actions the board is taking; and,
- appropriate action for individuals to take to protect themselves against harm.

How to Determine if Notification is Required?

The following factors should be considered when determining whether notification is required:

- **Legislation requires notification**
  Are you or your organization covered by legislation that requires notification of the affected individual? If you are uncertain, contact the privacy commissioner (see contact information at the end of this publication).

- **Contractual Obligations**
  Do you or your organization have a contractual obligation to notify affected individuals in the case of a data loss or privacy breach?

- Risk of Identity Theft
  Is there a risk of identity theft or other fraud in the Board? 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?

If personal information that could lead to identity theft has been disclosed, affected individuals should be provided with information on steps they can take to protect themselves. If the office of the Information and Privacy Commissioner (IPC) is investigating the privacy breach, indicate that to the affected individuals. Give an

explanation of the individual's right to complain to the IPC about the Board's handling of their personal information, along with contact information for the IPC.

- Notify appropriate managers/supervisors and employees within the Board of the breach; and,
- report the privacy breach to the IPC as appropriate. Contact information:

Information and Privacy Commissioner/Ontario
1-800-387-0073
info@ipc.on.ca
www.ipc.on.ca

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 on legislative requirements, security and privacy policies, 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,
- recommend remedial action to the accountable decision maker so future breaches do not occur.

SOURCES

i **Breach Notification Assessment Tool, December 2006 - Ipc.on.ca. (2019). [online] Available at: https://www.ipc.on.ca/wp-ontent/uploads/resources/ipcbc-breach-e.pdf[Accessed 15 Jan. 2019].**

ii **Privacy Breach Protocol, Guidelines for Government Organizations - Ipc.on.ca. (2019). [online] Available at: https://www.ipc.on.ca/wpcontent/uploads/resources/privacy-breach-e.pdf[Accessed 15 Jan. 2019].**

Appendix C

PRIVACY BREACH REPORT

REPORT # _____

Take immediate action when you have been advised of a suspected privacy breach. Many of the steps outlined below have to 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 orally through his/her immediate supervisor (e.g., phone call), or in written form (e.g., email).

STEP 1 – RESPOND

1. Person Reporting Suspected Breach:

   First name: _____ Last name: _____

   Job title: _____

   Location (school/department): _____

   Name of immediate supervisor: _____

   Phone number: _____

2. When Incident Occurred Date - _____ (mm/dd/yyyy) Time - _____ (a.m. or p.m.)

3. Assess the situation to determine if a breach has indeed occurred and what needs to be done? (Briefly outline)

   _____

   _____

   _____

4. Contact:

   Internal Source – (Identify) _____

   External Source – (Identify) _____

5. Identify steps to take to respond to breach.

   _____

   _____

   _____

6. Report privacy breach to:

- ☐ Director (or designate)
- ☐ Law Enforcement (if needed)
- ☐ Other: _____

STEP 2 – CONTAIN

1. Identify the scope of the breach and contain it. Describe background and scope of the breach.

2. Document the breach and containment activities.

3. Develop briefing materials and brief the Director of Education, senior management, and key persons on the privacy breach and how it is being managed. Indicate date and time briefing occurred.

Date - _____ Time - _____

(mm/dd/yyyy) (a.m. or p.m.)

STEP 3 – INVESTIGATE

Conduct an investigation with the involvement of other parties as necessary. For electronic information breach, contact the Chief Information Officer to assist in containment of breach.

1. Source and cause of the breach. Identify and analyze the events that led to the privacy breach.

_____

_____

_____

2. Number of individuals whose information was accessed without consent or authorization: _____

3. Type of personal information that was accessed without consent or authorization, e.g., health/medical information, student marks, biographical information (such as home address, phone numbers, names and contact information of family members), behaviour concerns, etc.

_____

_____

_____

_____

4. To whom the personal information belongs to and how many individuals were affected (e.g., student, employee, third party [someone who is neither a student nor employee of the board, such as a parent/guardian or volunteer]):

5. Who had unauthorized access to the personal information, and how that access was made?

6. Efforts made, if any, to contain the privacy breach (e.g., suspending the process/activity that caused the breach):

7. Inventory of the systems and programs affected by the breach:

8. Findings, including a chronology of events:

Legislative Implications of the Breach

Following a report of a suspected privacy breach, ensure that the activity/process has been contained if possible. Conduct an investigation of the information supplied in Steps 1 and 2 of this report in conjunction with current privacy legislation (MFIPPA, PHIPA, PIPEDA) and with local privacy policies and procedures to determine if the incident is, in fact, a breach. Note: You may wish to consult legal counsel to assist you in your 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 refer to "How to Determine if Notification is Required" in Appendix B.

Notify the following individuals as appropriate:

☐ Individuals whose privacy was breached.

Provide them with information about:

- what happened;

- the nature of potential or actual risks or harm;
- what mitigating actions the board is taking;
- appropriate action for individuals to take to protect themselves against harm; and
- If the office of the Information and Privacy Commissioner (IPC) is investigating the privacy breach, indicate that to the affected individuals. Give an explanation of the individual's right to complain to the IPC about the Board's handling of their personal information, along with contact information for the IPC.

☐ Director of Education
☐ Senior administration/managers/principals
☐ Legal Counsel
☐ Information and Privacy Commissioner/Ontario (IPC)
☐ Other

Report impact of the privacy breach on those individuals whose privacy was compromised.

_____
_____
_____
_____
_____
_____
_____
_____

NOTE: The type and extent of the breach will influence your decision to notify the Information and Privacy Commissioner's Office, Toronto (1-800-387-0073) 2 Bloor Street East, Suite 1400, Toronto, Ontario, M4W 1A8.

STEP 5 – IMPLEMENT CHANGE

Steps taken to correct the problem:

☐ Develop, change, or enhance policies and procedures.
☐ Ensure strengthening of security and privacy controls.
☐

Advise IPC of investigation findings and corrective action.

Provide additional notices (as deemed appropriate):

- ☐ Relevant third parties
- ☐ Consider public announcement (e.g., statement and/or apology)
- ☐ Other Ontario school boards/authorities (where shared responsibilities exist)

Prevent future breaches:

- ☐ Arrange employee training on privacy and security.
- ☐ Recommend appropriate and necessary security safeguards.
- ☐ Consider having an outside party review processes and make recommendations (e.g. auditing company).
- ☐ Evaluate the effectiveness of remedial actions.

The FOI Coordinator may wish to review Board's policies, procedures, practices, and training materials to ascertain whether any revisions are required to ensure a clearer understanding of what constitutes a privacy breach.

SIGN-OFF

The Director of Education or designate (e.g., FOI Coordinator) is required to sign below to formally acknowledge that the breach was handled in accordance with privacy legislation and with the Board's policies and procedures:

_____

_____

Print Name/Title Signature

Sign-Off Date*:* _____

(mm/dd/yyyy)

Appendix D [Print on Board Letterhead]

[Date]

[Name of person being notified]

[Address]

The protection of privacy and personal information for staff and students and diligence to our obligations under the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) is an ongoing priority for the Hamilton-Wentworth Catholic District School (HWCDSB). At this time, we are advising you of an incident …….

[Details of incident, list risks, information exposed, steps to mitigate] Example:
The Vendor has informed us that some of your personal information may have been at risk to unauthorized access within their support ticket system. The personal information that the Vendor reported as being potentially at risk of unauthorized access was your first name, middle name, last name, Ontario Education Number, date of birth, address, gender and student number from the -------- school year. The Vendor has advised us that immediately after they discovered the issue, they implemented the proper security measures to prevent any further potential exposure of this data.

At times, the HWCDSB must share student information with this vendor so that support issues with our Student Information System can be resolved. As a result of this incident, the Vendor is reviewing their internal practices regarding access rights provisioning, change control, data protection and additional security training for their employees. The HWCDSB will also continue to work with the Vendor to ensure that future events like this are prevented.

[if applicable - if financial information or information from government-issued documents are involved, include the following in the notice: As a precautionary measure, we strongly suggest that you contact your bank, credit card company, and appropriate government departments to advise them of this breach.]

As part of our protocol, we have also reported the incident to the Information and Privacy Commissioner of Ontario (IPC) to ensure that we are complying with appropriate obligations with respect to this incident. If you wish to file a complaint with the IPC the website is http://www.ipc.on.ca.

Thank-you for your understanding as the HWCDSB works through and learns from this incident. If you have any additional questions, you are welcome to contact the
[Freedom of Information Coordinator or Principal or Chief Information Officer or Other]

Regards,

[Freedom of Information Coordinator or Principal or Chief Information Officer or Other]