CATHOLIC DISTRICT SCHOOL BOARD OF EASTERN ONTARIO
www.cdsbeo.on.ca

BOARD ADMINISTRATIVE PROCEDURE

ADMINISTRATIVE PROCEDURE

1006 Privacy Breaches

DIRECTIONAL POLICY

1000 Positive Communications

Title of Administrative Procedure:

Privacy Breaches

Date Approved:

May 2025

Projected Review Date:

May 2030

Directional Policy Alignment

This administrative procedure aligns with directional policy 1000 Positive Communications and establishes parameters within the Board regarding its duties to comply with all legislative requirements under the provisions of the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), as well as the Personal Health Information Protection Act (PHIPA).

Alignment with Multi-Year Strategic Plan:

The Privacy Breaches administrative procedure supports the Board's Multi-Year Strategic Plan through its commitment to the protection of privacy, and obligation to adhere to relevant privacy legislation. The Board is committed to the safety and well-being of all its student and their families and will ensure that Board employees are aware of their professional obligation to adhere to the privacy requirements outlined in the Education Act, MFIPPA, Bill 194, and PHIPA.

CDSBEO Strategic Plan 2025-2030

Purpose and Action Required

The Catholic District School Board of Eastern Ontario (CDSBEO) and its employees have a duty to ensure that the personal information of employees and students that is in their custody is protected from unlawful disclosure. The Board is committed to the protection of personal and confidential information under its custody and to an individual's right of privacy regarding personal information that is collected, used, retained, and disclosed in the school system. While protection of personal information is paramount, the board recognizes that breaches may occur. This Privacy Breach Response Administrative Procedure allows for a prompt, reasonable and

coordinated response when personal information is compromised; that is, when it is collected, accessed, used, disclosed, retained, or destroyed in a manner inconsistent with privacy legislation.

With this procedure, the CDSBEO seeks to:

a) make its employees aware of the potential for privacy breaches;

b) implement a standardized and consistent response to privacy breaches.

1. Examples of Privacy Breaches

Student Records:

a) digital image of a student taken and displayed without consent;
b) psychological assessments kept in openly accessible file cabinets;
c) documents containing student personal information left unattended on photocopier;
d) memory key/jump drive containing student data left in public area;
e) theft from teacher's car of a laptop containing student records on hard drive.

Employee Records:

a) budget reports containing employee numbers and names found not shredded in recycling and garbage bins;
b) theft from car of a briefcase containing a list of home addresses of teaching staff;
c) sending sensitive personal information to an unattended, open area printer;
d) password written on a sticky note stuck to a monitor;
e) resumes faxed or emailed to wrong destination or person;

Business Records:

a) list of names, including credit card numbers, left unattended on photocopier;
b) tender information scanned and not cleared from multi-functional office machine;
c) disposal of equipment with memory capabilities (e.g. electronic storage devices, laptops, photocopiers, fax machines, or cell phones) without secure destruction of the personal information it contains.

2. Responding to a Privacy Breach

All CDSBEO employees shall:

1. Notify their supervisor or, in his/her absence, the Privacy Officer immediately if:

    a) personal information is lost or suspected of being lost;
    b) personal information is disclosed or suspected of being disclosed to unauthorized

parties;
c) passwords or other system access control mechanisms are lost, stolen, or disclosed or are suspected of being lost, stolen, or disclosed;
d) they become aware of any unusual systems behaviours, such as missing files, frequent system crashes, or misrouted messages;
e) they become aware of any other privacy breach or suspected privacy breach.

2. Contain, if possible, the breach or suspected breach by suspending the process or activity that caused the breach.

Senior administrators, managers, and principals shall:

1. Obtain all available information about the nature of the breach or suspected breach;
2. Alert the Privacy Officer and provide as much information about the breach as is available;
3. Work with the Privacy Officer to undertake all appropriate actions to contain the breach;
4. Ensure details of the breach and corrective actions are documented.

The Privacy Officer shall:

1. Ensure that the CDSBEO's Breach Response Protocol is initiated as soon as a privacy breach or suspected breach has been reported.
2. Ensure that those whose personal information has been compromised are informed as required.
3. Collect all details of the breach and submit a report to the Information and Privacy Commissioner.

The Director of Education:

Is the key decision maker in responding to privacy breaches. The Director has the responsibility to:

1. Brief senior management and trustees as necessary and appropriate;
2. Review internal investigation reports and approve required remedial action;
3. Monitor implementation or remedial action.

Response Protocol

Unauthorized disclosure of personal information is the defining characteristic of a privacy breach, regardless of whether it was intentional, accidental or the result of a theft or malicious intent. All privacy breaches or suspected privacy breaches must be reported to the principal or supervisor, or in their absence, to the appropriate superintendent or Privacy Officer. Once reported, the supervisor or superintendent will contact the Privacy Officer and the following response steps will be implemented.

Step 1 - Respond

When a suspected privacy breach is identified by an internal or external source:

1. Contact the appropriate department to investigate
2. Assess the situation to determine if a breach has indeed occurred and what needs to be done
3. Provide advice on appropriate steps to take to respond to the breach
4. Report the privacy breach to key persons within the Board (including the Director of Education or designate, Superintendent, and/or CIO) and, if necessary, to law enforcement

Step 2 - Contain

Identify the nature and scope of the breach and what actions are required to contain it quickly:

1. Identify what personal information is involved
2. Take corrective action:
3. Retrieve the hard copies of any personal information that has been disclosed
4. Determine if the breach would allow unauthorized access to any other personal information and if so, immediately change passwords, shut down necessary systems, suspend staff access rights, or remove data from an affected server to contain the breach
5. Brief the accountable decision maker, senior management, and key persons on the privacy breach and how it is being managed

Step 3 - Investigate

Once the breach is contained, complete an investigation with the involvement of other parties as necessary:

1. An analysis of events that led to the breach – this may include discussions with multiple parties including CIO, superintendent, school principal, staff member (if human error)
2. Evaluate what was done to contain it
3. Review staff training for improvements that could have prevented the breach, if applicable
4. Review policies and practices for protecting personal information to determine whether changes/improvements are needed (ie; cybersecurity improvements)
5. If breach was the result of a systemic issue, review program-wide or institution-wide procedures
6. Take all necessary corrective action to prevent similar breaches in the future
7. Document the results of internal investigation, including background and scope of

the investigation, source and cause of the breach

Step 4 - Notify

Notify those affected as soon as reasonably possible if you determine that the breach poses a real risk of significant harm to the individual, taking into consideration the sensitivity of the information and whether it is likely to be misused. Notification should be direct, such as by telephone, letter, email or in person. Indirect notification can be used in situations where direct notification is not possible or reasonably practical, for instance, when contact information is unknown or the breach affects a large number of people.

Notification to affected individuals should include:

- an explanation of what happened, including details of the extent of the breach
- the nature of potential or actual risks or harm
- what mitigating actions were taken
- contact information for someone within your organization who can provide additional information and assistance, and answer questions

Report the privacy breach to the Office of the Information and Privacy Commissioner as appropriate.

How do you Determine if Notification is Required?

Consider the following factors when determining whether notification is required:

Risk of Physical Harm

Does the loss or theft of information place any individual at risk of physical harm, stalking, or harassment?

Risk of Identity Theft

Is there a risk of identity theft or other fraud as a result of the breach? 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 Hurt, Humiliation, or Damage to Reputation

Could the loss or theft of information lead to hurt or 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?

Legislative Requirements (PHIPA, Regulation 329/04)

Notice to Affected Individual: Under the Personal Health Information Protection Act, a Health Information Custodian (HIC), having knowledge that personal health information in their custody or control was lost, stolen or used/disclosed without authority, is required to:

- Notify the individual of the theft or loss or unauthorized use or disclosure of the individual's personal health information; and
- Include in the notice a statement the individual is entitled to make a complaint to the Information Privacy Commissioner

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 to reduce potential or future breaches, and strengthen as required
- Recommend remedial action to the accountable decision maker

Responsibilities

The Director of Education is responsible for:

- Authorizing decisions with respect to the release of information under MFIPPA
- Designate resources for ensuring the implementation of and compliance with this administrative procedure
- Provide the Privacy Officer with ready access to records and information responsive to a formal access request

The Privacy Officer is responsible for:

- Receiving and processing all requests for information under MFIPPA including appeals
- Report any privacy breaches to the Information and Privacy Commission of Ontario

- Provide consultation and support regarding access to information from staff and members of the public

Superintendents/Managers and Principals are responsible for:

- complying with MFIPPA, the Education Act, and other laws related to the privacy of and access to students' personal information, along with relevant guidelines and policies
- collecting personal information only when permitted under the law
- implementing reasonable security measures to protect student personal information
- ensuring that staff are aware of and adequately trained in their responsibilities
- ensuring that agreements with service providers and data protection agreements are in place with all third-party vendors and that these agreements contain provisions to protect the privacy and security of personal information as required under legislation

Staff are responsible for:

- complying with legislation, professional standards, guidelines, and school board policies when collecting, retaining, using, and disclosing personal information
- protecting personal information by following school policies and procedures
- reporting any suspected privacy or security breaches to the school principal
- participating in annual training regarding their duties and obligations to protect personal information

Progress Indicators

- Mandatory annual privacy training for all staff
- Statistics for breaches involving a theft, loss, or unauthorized use or disclosure of personal information submitted annually to the Information and Privacy Commissioner of Ontario

Definitions

"Privacy Breach" occurs when personal information is collected, used, disclosed, retained, or destroyed in a manner inconsistent with Ontario privacy legislation. Privacy breaches can arise when a CDSBEO employee:

- discloses or shares a student's personal information when the disclosure is not required for the purpose of improving the instruction of the student or for a consistent purpose;
- discloses another employee's personal information when the disclosure is not required for purposes related to that employee's employment with the CDSBEO;
- unintentionally discloses a student's or an employee's personal information by reason of

unauthorized access by a third party or by inadvertent loss or destruction.

"Personal information" is any recorded information about an identifiable individual, including:

- information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation, marital or family status of the individual;
- information relating to the educational, 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 individual's name 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.

"Recorded information" is any information however recorded, whether in printed form, on film, by electronic means or otherwise, and includes, but is not limited to:

a. correspondence, a memorandum, book, drawing, photograph, film, microfilm, sound recording, videotape;
b. any recorded information that is capable of being produced by means of computer hardware and software or any other information storage equipment.

References

- Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M.56
- Education Act, R.S.O. (199), O. Reg. 440/20
- Personal Health Information Protection Act, 2004, S.O. 2004, c.3, Sched. A
- 1002 Freedom of Information and Protection of Privacy
- F2:5 Secure and Responsible Use of Personal and Confidential Information