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

ADMINISTRATIVE PROCEDURE

1. Purpose:

Pursuant to the *Municipal Freedom of Information and Protection of Privacy Act (*MFIPPA*),* 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 so as to ensure that the privacy of the individual to whom the information relates is not breached.

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.

2. 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:

a. 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;
b. discloses another employee's personal information when the disclosure is not required for purposes related to that employee's employment with the CDSBEO;
c. 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:

a. information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation, marital or family status of the individual;
b. 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;
c. any identifying number, symbol or other particular assigned to the individual;
d. the address, telephone number, fingerprints or blood type of the individual;
e. the personal opinions or views of the individual except if they relate to another individual;
f. 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;
g. the view or opinions of another individual about the individual;

h. 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.

3. 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.

4. Procedures for responding to Privacy Breaches

All CDSBEO employees shall:

1. Notify their supervisor or, in his/her absence, the Freedom of Information Coordinator 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:

a. obtain all available information about the nature of the breach or suspected breach;
b. alert the Freedom of Information Coordinator and provide as much information about the breach as is available;
c. work with the Freedom of Information Coordinator to undertake all appropriate actions to contain the breach;
d. ensure details of the breach and corrective actions are documented.

The Freedom of Information Coordinator shall:

a. ensure that the CDSBEO's Response Protocol is initiated as soon as a privacy breach or suspected breach has been reported.

The Director of Education:

1. Is the key decision maker in responding to privacy breaches. The Director has the responsibility to:
   a. brief senior management and trustees as necessary and appropriate;
   b. review internal investigation reports and approve required remedial action;
   c. monitor implementation or remedial action;
   d. ensure that those whose personal information has been compromised are informed as required.

5. Response Protocol

The following steps shall be initiated by the Freedom of Information Coordinator as soon as a privacy breach or suspected breach has been reported:

Step 1 - Respond
Step 2 - Contain
Step 3 - Investigate
Step 4 - Notify
Step 5 - Implement Change