1. Purpose:

The *Municipal Freedom of Information and Protection of Privacy* Act (MFIPPA) requires that the Catholic District School Board of Eastern Ontario (CDSBEO) and its employees protect the privacy of all individuals with respect to their personal information held by CDSBEO. The *Education Act* also contains rules which specifically govern the use and disclosure of information held in a student's Ontario Student Record ("OSR").

With this Procedure, CDSBEO seeks to:

a. make its employees aware of their responsibilities in regard to the security of the personal information of students and employees, and of other confidential CDSBEO information, which is in their care or custody, whether at the office, school or offsite;

b. ensure that its employees use CDSBEO-owned and personal electronic devices in a responsible and secure manner.

2. Legal Framework

Education Act

Pursuant to the Education Act, the information contained in a student's Ontario Student Record folder:

a. can only be used by CDSBEO's supervisory officers and the principal and teachers of a student if it is required for the improvement of instruction of that student;

b. is not to be shared with or disclosed to any other person unless it is required in the performance of that person's duties for improvement of instruction of that student or unless the written consent of the parent or guardian of a minor student or of the adult student is obtained.

MFIPPA

MFIPPA requires CDSBEO employees to ensure the protection of personal information of students or other employees that is in their care and/or custody so that their privacy is not breached. This applies to personal information in all formats, including but not limited to paper, computer storage, electronic storage devices, remote electronic storage, photos, drawings, and recordings.

MFIPPA also sets out rules regarding the disclosure of other confidential information in the care and/or custody of CDSBEO which does not necessarily include personal information. CDSBEO has designated a Freedom of Information Coordinator ("FOI Coordinator") to deal with any issues related to the release of confidential information held by the CDSBEO.

3. Definitions

"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;

c. relating to financial transactions in which the individual has been involved;

d. any identifying number, symbol or other particular assigned to the individual;

e. the address, telephone number, fingerprints or blood type of the individual;

f. the personal opinions or views of the individual except if they relate to another individual;

g. 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;

h. the view or opinions of another individual about the individual;

i. 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.

"Confidential information" may include but is not limited to recorded information that:

a. reveals the substance of deliberations of CDSBEO meetings held in the absence of the public;

b. reveals advice or recommendations of an officer or employee or consultant;

c. could reasonably be expected to reveal information CDSBEO has received in confidence from the Ministry of Education;

d. reveals financial or labour relations information;

e. was prepared by CDSBEO's legal counsel in giving legal advice or in contemplation of litigation.

"Electronic devices" include but are not limited to computers, electronic storage devices, remote electronic storage, handheld electronic devices, and digital cameras.

4. Procedures

All CDSBEO employees are expected to comply with the following Procedures. In the event that an employee suspects a privacy breach, please refer to administrative procedure: Privacy Breaches.

a. CDSBEO employees shall immediately return to all paper documents, software, and electronic devices belonging to CDSBEO upon termination of employment.

b. no records, information or data in the CDSBEO system shall be accessed by any individual unless he or she is authorized to do so in the course of his or her daily CDSBEO-related business, employment or educational activities;

c. personal information in the CDSBEO system shall not be disclosed to any individual, agency, organization or institution outside the CDSBEO except in accordance with CDSBEO Procedures. If in doubt, please refer to the FOI Coordinator;

d. confidential information in the CDSBEO system shall not be disclosed to any individual, agency, organization or institution outside the CDSBEO without written authorization of the FOI Coordinator;

e. paper records and electronic devices containing personal or confidential information should not be left unattended unless physically secured and should be stored out of sight when not in use;

f. if viewing personal or confidential information in any format at a location outside the school or office, ensure that it is not viewable by anyone else;

g. paper records and electronic devices containing personal or confidential information should never be left in a vehicle. If it absolutely cannot be avoided, the records or electronic device should be locked in the trunk before the start the trip;

h. when travelling by air, bus or train, personal or confidential information in any format should be transported as carry-on luggage.

Paper Documents

a. documents containing personal information or confidential information should never be discarded in a trash or recycling bin;

b. whenever practical, original documents should remain on-site and only copies should be removed from the school or office. Copies should be clearly identified as such and should be shredded when no longer needed;

c. whenever possible, only documents that are relevant or extracts or summaries should be removed from files, rather than removing the entire file from the school or office. If a file is removed, a sign-in/sign-out procedure should be used;

d. if they must be removed, records and documents should be returned to a secure environment as quickly as possible, for example, at the end of a meeting, the end of the day or upon return from a trip.

Electronic Devices

Teachers and staff members shall not share student data and student information (academic or behavioural) when using online educational learning platforms provided by private companies not licensed by the Ministry of Education or CDSBEO.

a. to the greatest extent possible, personal or confidential information should not be maintained or stored on mobile electronic devices;

b. CDSBEO employees shall not permit any unauthorized individual to obtain access to CDSBEO software or data;

c. CDSBEO employees shall not publicly disclose any internal CDSBEO information that may adversely affect CDSBEO's public relations or public image;

d. electronic devices containing personal information or confidential information should be destroyed, erased or otherwise processed to ensure that all data is permanently removed in a manner that prevents recovery before these devices are redistributed to another employee, disposed of, or returned to the vendor;

e. individual passwords must never be shared. If there is an issue that requires CDSBEO employees to do so, then the password should be changed immediately after the issue has been resolved. If a CDSBEO employee suspects a password has been compromised or a CDSBEO employee is unsure then the password should be changed immediately. Never use the “Remember Password” feature on any system;

f. CDSBEO employees who leverage internet based software services not licensed by the Ministry of Education or CDSBEO shall ensure compliancy with the Board Policy F2 Personal Information Management Freedom of Information and Protection of Privacy Act;

g. CDSBEO employees should structure their electronic communications and social networking sites in recognition of the fact that CDSBEO may, from time to time, examine, intercept or disclose the content of electronic communications and/or electronic data in order to;
   i. protect CDSBEO's electronic communications network;
   ii. resolve problems within CDSBEO's electronic communications network; or
   iii. aid an investigation into conduct which the Board suspects may constitute a breach of professional standards or may jeopardize the safety of CDSBEO students;

h. Board personnel shall not review the content of an individual CDSBEO employee's communications out of personal curiosity or at the request of individuals who have not obtained authorization from their Superintendent;

i. electronic messages or data which are no longer needed for the purpose for which they were created shall be purged by CDSBEO employees according to the Board's Record Retention Schedule;

j. in order to protect personal and confidential information;
   i. CDSBEO software shall not be installed, downloaded or copied onto non-CDSBEO electronic devices or placed on any publicly accessible computer or on the internet without the prior consent of the Info Tech Committee;
   ii. software from non-CDSBEO sources shall not be downloaded or installed onto CDSBEO owned electronic devices without the prior consent of the Info Tech Committee;
   iii. CDSBEO employees shall not establish external network connections that could allow non-CDSBEO employees to gain access to CDSBEO systems and information;
   iv. CDSBEO employees shall not attempt to alter or circumvent security measures put in place by CDSBEO;
   v. network devices such as but not limited to access points, routers, hubs, switches, repeaters or similar devices are strictly prohibited, as they create security holes and connectivity interference on the CDSBEO computer network infrastructure.

5. Failure to Comply

In the event employees suspect non-compliance of this procedure, they must notify their Supervisor immediately. Violation of this procedure may subject CDSBEO employees to disciplinary sanctions up to and including termination of employment.