Windsor-Essex Catholic District School Board

Section: Information Technology

ADMINISTRATIVE PROCEDURE:

PR IT:01F PRIVACY PROTECTION AND INFORMATION MANAGEMENT

NUMBER:	PR IT:01F
EFFECTIVE:	May 25, 2016
AMENDED:	Replaces H:17, H:18, SC:03
RELATED POLICIES:	See References
REPEALS:	
REVIEW DATE:	2019-2020

1.0 OBJECTIVE

1.1 To provide, as per legislation and Board Policy and Procedures, the right for the protection of individual's personal information.

2.0 GUIDELINES

2.1 The Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) regulates the privacy protection practices of all Ontario School Boards. MFIPPA sets out and provides direction on how we collect, use, disclose and destroy personal information while protecting the individual's right to privacy, however recorded, whether in printed form, on film, by electronic means or otherwise.

3.0 PROCEDURE

3.1 Everyone has the legislated right for the protection of their personal information.

3.2 The Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) regulates the privacy protection practices of all Ontario School Boards. MFIPPA sets out and provides direction on how we collect, use, disclose and destroy personal information while protecting the individual's right to privacy.

3.3 Staff is responsible for protecting personal, confidential and sensitive information entrusted to them in their professional role.

3.4 Staff must report any suspicions they may have of a privacy breach to their immediate supervisor and to the Board's Freedom of Information (FOI) Coordinator.

3.5 All electronic information of a sensitive or confidential nature should be protected from unauthorized access and only made available to individuals who require that access. (Refer to Procedures PR:01B User Access Management and PR:01C Passwords for Information Technology Resources).

3.6 The Freedom Information Coordinator for the Board shall ensure that reasonable measures respecting the records in the custody or under the control of the institution are developed, documented and put into place to preserve the records in accordance with any recordkeeping or records retention requirements, rules, or policies, whether established under an Act or otherwise, that apply to the institution. The Board shall retain personal

information in accordance with the Board's retention schedule.

3.7 All records will be efficiently and promptly disposed, when administrative, legal and fiscal values have ceased and all legislative requirements as they affect Board documents have been met, while preserving value due to archival, historical or vital reasons.

3.8 There are some business processes which require data to be exchanged with parties outside the Windsor-Essex Catholic School Board. When highly sensitive data is transmitted to external servers or vendors, a non-disclosure agreement must be in place with the vendor and extra security measures must be taken.

Data which resides with external vendors who provide services for the Board may require uploads of information in order to perform the contracted services. When this is necessary, consideration must be given to the sensitivity of the required data prior to any exchange of information. Following current privacy legislation such as the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), the contractual agreement with the vendor must include appropriate language to protect personal or confidential information.

3.9 Any transmission of confidential data or information must be conducted using encrypted channels (SSL, Secure FTP, etc.)

The Ontario Software Acquisition Program Advisory Committee (OSAPAC), in collaboration with the Ontario Information and Privacy Commissioner's Office, has created rigorous agreements with Google and Microsoft to provide a more secure cloud environment for school boards to use. The WECDSB has opted to use Google Apps for Education. Within this secure Google Apps for Education environment also referred to as MyTools2Go, it is acceptable to include personally-identifiable information about staff or students or other confidential corporate information in accordance with MFIPPA guidelines. It is not acceptable to include confidential information in other publicly available cloud applications or external tools such as but not limited to Dropbox, Facebook, Twitter, Evernote, Remind, etc. as they are not sanctioned by the Board.

3.10 The use of any type of mobile or portable device (iPhones, iPods, iPads, Android based phones, Blackberries or other smartphones, USB memory sticks, USB drives, flash drives, laptops) which hold or transport data need to have consideration given to the type of data which may be contained on the device. As a general rule do not store highly sensitive or confidential data on these devices unless you have the proper encryption and security in place.

Access requests under the Act(s) are administered by the Board's Record Management and Access/Privacy Administrator referred to as the Freedom of Information (FOI) Coordinator. If more detailed information or access is required, a correction of your record, have a concern about privacy or have a complaint about the handling of your privacy, contact the Board's Freedom of Information Coordinator.

For additional information refer to the Board's Privacy Policy (A:30), MFIPPA or contact the Board's Freedom of Information Coordinator.