Toronto District School Board

Operational Procedure PR676

Title: **FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY**

Adopted: **April 15, 2003**
Revised:
Reviewed: November 2012
Authorization:

1.0 OBJECTIVE

To establish a process concerning freedom of information and protection of privacy in accordance to Purpose: legislation

2.0 RESPONSIBILITY

Director of Education

3.0 DEFINITIONS

Municipal Freedom of Information and Protection of Privacy Act

The *Municipal Freedom of Information and Protection of Privacy Act* applies to municipalities, local boards, agencies and commissions. This may include information held by a city clerk, a school board, board of health, public utility or police commission.

The *Act* requires that local government organizations protect the privacy of an individual's personal information existing in government records. It also gives individuals the right to request access to municipal government information, including most general records and records containing their own personal information.

Privacy Protection

The *Act* creates a privacy protection scheme which the government must follow to protect an individual's right to privacy. The scheme includes rules regarding the collection, retention, use, disclosure and disposal of personal information in its custody or control.

If an individual feels his or her privacy has been compromised by a government organization governed by the *Act*, he or she may complain to the Information and Privacy Commissioner who may investigate the complaint.

[Excerpt from the Municipal Mini Guide]

The Information and Privacy Commissioner/Ontario has a Web site that provides comprehensive information about the *Acts* and specific information for schools and school boards.

The IPC's Web Site

IPC Home Page	http://www.ipc.on.ca
List of Education Resources	http://www.ipc.on.ca/index.asp?navid=58&fid2=2
Frequently Asked Questions: Access and Privacy in the School System – a resource for parents, teachers and administrators	http://www.ipc.on.ca/images/Resources/faq-e_2.pdf
A Guide to Ontario Legislation Covering the Release of Students' Personal Information	http://www.ipc.on.ca/images/Resources/educate-e.pdf
Guidelines for Protecting the Privacy and Confidentiality of Personal Information When Working Outside the Office	http://www.ipc.on.ca/images/Resources/wrkout-e.pdf

4.0 PROCEDURES

4.1. ACCESS AND PRIVACY: A BACKGROUNDER

In 1991, the Province of Ontario enacted the *Municipal Freedom of Information and Protection of Privacy Act.* This act applies to municipal institutions including towns and cities, school boards, police, boards of health, public libraries, etc. The Province of Ontario and provincial institutions are covered by a similar Act. At the Federal level, there are two pieces of legislation: one for access and one for privacy.

The *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) and the *Education Act* provide a strong framework within which to balance access and privacy within the Toronto District School Board. The following is a summary of the major points of MFIPPA within the context of the Board.

The provisions of MFIPPA are central to open, accountable and democratic government and government services in Ontario. The Board must provide access unless the information is exempt under the Act. And, the Board must protect the privacy of those it deals with—students, families, staff and community members.

The Act establishes a climate or culture that balances access and privacy. It does not deal only with requests that may make the statement "I request . . . under the Act." The access and privacy provisions set out in the legislation

apply as equally to a telephone question as they do to a three-page letter or a conversation between staff members.

The **purposes of MFIPPA** are **to provide a right of access** to information under the control of the TDSB, and to **protect the privacy of individuals** with respect to personal information about themselves and to provide individuals with a right of access to that information.

4.1.1 Access

With regard to **access** or the freedom of information part of MFIPPA, the part which helps to ensure open and accountable government:

- information should be available with very limited exceptions;
- there are ten particular exemptions to this general rule of availability; for schools, the most common are that the information is personal information, there is a threat to health or safety, and the information is available publicly or is soon to be published.

4.1.2 Privacy

With regard to **privacy** and MFIPPA, the first thing is to identify personal information.

Personal information is recorded information about an identifiable individual, including information about race ethnic or national origin, religion, sex, sexual orientation or marital or family status, education, medical or employment history, identifying numbers, address, telephone number, and the views or opinions of another individual about the individual.

Please note. The recording medium can be anything—paper, film, electronic, audio or video tape, etc. And, there are circumstances where personal information includes non-recorded information, that is, conversations.

It is clear that an enormous percentage of the records within a school or education office contain personal information about students, their families and staff.

There are three important points to remember when dealing with personal information—**collection, use** and **disclosure**. You must have the authority to collect information, to use it and to disclose it.

To collect personal information

- You must have the authority to collect the information, usually from a statute such as the *Education Act*, Section 265, which provides the authority for the collection of information for the pupil record or OSR

- As a rule, personal information must be collected directly from the individual or in the case of children, it may be collected directly from the parent or guardian
- You must notify the person of your authority and the principle purposes for which the information will be used and provide a contact person or position for questions

To use personal information

- You must have the consent of the individual or, if a child, the parent or guardian
- The information may be used for the purpose for which it was obtained or compiled (collected); this is where the notice at the time of collection is very important

To disclose personal information

- You must have the consent of the individual or, if a child, the parent or guardian
- The information may be disclosed for the purpose for which it was obtained or compiled (collected); again, your collection notice is important
- The information may be disclosed to an officer or employee of the Board who needs the record in the performance of his or her duties
- The information may be disclosed to the police to aid in an investigation
- The information may be disclosed in compelling circumstances affecting the health or safety of an individual, or in compassionate circumstances to facilitate contact with the next of kin or a friend of an individual who is injured, ill or deceased

4.1.3 General

Generally, MFIPPA requires the following:

- You must ensure that reasonable measures to **prevent unauthorized access** to records are defined, documented and put in place, taking into account the nature of the records to be protected. These measures must protect the information throughout its life—including destruction. Personal information should be shredded or, if electronic, deleted so that it cannot be reconstructed
- Personal information that has been used by an institution **must be retained after use** by the institution for the period prescribed by regulation (**minimum one year**) in order to ensure that the individual to whom it relates has a reasonable opportunity to

obtain access to it. After this minimum, the Board's retention policy should be followed
- You must take reasonable steps to ensure that information is not used unless it is **accurate** and up-to-date

In summary, within the details and exceptions set out within MFIPPA:

- **Personal information** must be **protected** and used and disclosed only in very specific circumstances
- **Non-personal** or general records or information should, generally, be made **available** to requestors
- **Use the provisions of the *Act* to your benefit.** Use it to give yourself time to make a well considered reply to a request for information, to put structure around large or vague requests, or to reflect on the implications of an answer--even, to encourage a requestor to make a formal request.

There are many resources available if you are interested in access and privacy issues. Of particular interest will be the Web site of the Information and Privacy Commissioner/Ontario as noted at the top of page 2. An excellent print resource is Brenda Stokes Verworn's book, *An Educator's Guide to Freedom of Information* (Aurora, Ont.: Aurora Professional Press Canada Law Book, 1999).

4.2 ACCESS AND PRIVACY PROTECTION: POINTS TO CONSIDER

Consider whether the medium of the record has an impact on access and privacy. For example, a letter or report card in a sealed envelope sent by Canada Post versus a letter or report card sent by e-mail; a traditional photograph pasted into the OSR or reproduced in the yearbook versus a digital photograph intended for a similar purpose; or a document mailed versus a document faxed.

In this increasingly technological world, give some thought to the idea that just because you are able to do something, does not mean it's a good idea.

When planning a project, consider whether there are privacy implications, and if there are, how they should be managed.

Remember that it is very difficult to get information back once you have released it. Consider the implications before you release information. If in doubt--don't.

When dealing with student information and situations, ask yourself, If this were my child . . . ?, or with personal information and situations, If this were my file . . .? before you make a decision.

Make use of the resources and support available to you. The internet is a fabulous resource for information on access and privacy issues. (See the top of page 2 of this procedure.)

Think about the challenges that technology poses to privacy. There are two ways to manage this. Either forego the use of the technology or embrace the technology and build in privacy protection and even privacy enhancement.

For example, voice mail and e-mail pose some real challenges to access and privacy protection. If you use these technologies to communicate personal or confidential information, be sure you have adequate security in place first. Some things to think about: use the password protections available to you; don't disclose your passwords or write them down and stick them on your phone or computer; change passwords frequently; when you send a confidential voice or electronic message, be certain it is being sent to the correct destination; and, don't presume that the destination is secure, find out—it could be a mail box shared by a group of employees or by a whole family.

4.3 SOME FREQUENTLY ASKED QUESTIONS AND GENERAL ANSWERS

4.3.1 *The police call and ask for information about a particular student. Are there any guidelines for me to follow in responding?*

Disclosure of personal information is permitted under a number of particular circumstances. One of these is disclosure to a law enforcement agency to aid in an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result. In other words, it is appropriate to give the police information if it is in relation to an investigation. It is not appropriate if they are just on a "fishing expedition."

4.3.2 *We sometimes get calls asking for a teacher's home address and/or phone number, or a student's. Often these are from former students who just want to keep in touch. What are the guidelines here?*

It is not acceptable to give the caller the information. Home address and phone number are definitely personal information and should not be disclosed. Tell the caller that you cannot disclose that information, but if they would leave their name and telephone number, you will forward it to the individual involved. Or, the caller could write to the individual in care of the school and you could offer to forward the letter.

4.3.4 *We are frequently asked to fax documents and we receive a lot of information by fax. How should we deal with personal and confidential information and faxing?*

Consider the practice of faxing personal information only if it is really necessary. If you can, remove the personal identifiers from the faxed copy and mail the original. Ensure that the fax is sent to the correct fax number. Confirm the destination fax before transmission. Use a cover sheet and clearly identify the sender and intended recipient, as well as the total number of pages sent and a contact telephone number. Check the transmission report to be sure the complete document was transmitted. Try to place your fax machine in a secure area. Establish procedures for collecting and distributing faxes. Avoid just leaving the faxes at the machine where anyone has access to the information.

4.3.4 *Are there any tips on making this easier? We have a lot of occasional workers and volunteers in the office and it is important that they know the basics.*

Make a list of the information it is okay to give out to the public. Make another list of the information that should never be given out and some suggestions on how to handle those calls. Make a third list of special circumstances, e.g. parents or police, and how to handle those calls. Remind staff that very few requests need to be answered instantly. Take a message and call back. If in doubt—don't.

IF YOU RECEIVE A FORMAL REQUEST FOR INFORMATION under the *Municipal Freedom of Information and Protection of Privacy Act,* you must call and forward it to the Board's FOI contact: Roula Anastasakos, Executive Superintendent, Board Services, 5050 Yonge Street, Toronto, ON, M2N 5N8, (416) 397-3288, **as soon as possible**. There is a 30-day (calendar days) time limit for the Board to prepare a response. All formal requests must be processed by R. Anastasakos' office and according to the provisions of the *Act.*