



POLICY P.128.GOV

TITLE: ACCESS TO INFORMATION AND PRIVACY PROTECTION

Date Authorized: 12 February 2010

Last Revised:

Last Reviewed: XXXXXX

COMMITMENT TO INDIGENOUS RIGHTS, HUMAN RIGHTS, AND EQUITY

The Board recognizes its responsibility to ensure that this policy and associated procedures promote and protect Indigenous rights, human rights, and equity. The Board will strive to address and eliminate discrimination and structural and systemic barriers for students, staff, and community.

1.0 OBJECTIVE-RATIONALE

To ensure public transparency through access to information in the custody of the OCDSB, and to ensure the protection of Personal Information in the custody of the OCDSB in accordance with the requirements of the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)*, the *Personal Health Information Protection Act (PHIPA)*, and other privacy legislation as applicable.

2.0 DEFINITIONS

Please refer to Appendix A for a list of definitions of terms used in this policy.

3.0 GUIDING PRINCIPLES

- 3.1 The OCDSB acknowledges its responsibility to collect, use, retain, ~~and~~ disclose, and destroy Personal Information in accordance with ~~the statutory duties and responsibilities provided in the~~ *Education Act*, the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)*, the *Personal Health Information Protection Act (PHIPA)*, and ~~any~~ other applicable legislation.
- 3.2 ~~The Board recognizes that~~ Every individual has the right to access information in the OCDSB's control, including ~~their~~ the individual's own Personal Information. Every individual also has the right to challenge the ~~its~~ accuracy and completeness of their Personal Information and to be notified of all requests for access to their Personal Information from other individuals in accordance with the law..
- 3.3 The Board recognizes ~~the need to balance the right of a student to an expectation of confidentiality and the rights of parents/guardians and others to disclosure of~~

~~confidential communications between students and staff.~~ that it must balance a student's right to privacy with the rights of parents/guardians and others to know certain information shared between students and staff in accordance with the law.

- 3.4 Employees have a duty to report child protection concerns to the Children's Aid Society of Ottawa, and this duty supersedes the privacy protections in *MFIPPA* and *PHIPA*.
- 3.5 ~~Individuals have the right to address or challenge compliance with these principles through an appeal process in accordance with the *MFIPPA*.~~ The Board's privacy decisions are subject to an appeal to the Information and Privacy Commissioner of Ontario
- 3.6 Under *MFIPPA* many privacy decisions must be made by the "Head" of the OCDSB. *MFIPPA* allows the Board to designate a person to be the Head to make those privacy decisions. ~~The Board delegates the authority relative to the *MFIPPA* to the Director of Education/Secretary of the Board or designate to be accountable for compliance with all privacy legislation.~~ designates the Director of Education as the Head for the purposes of *MFIPPA*. The Director of Education may delegate this authority to a member of staff.
- 3.7 For the purposes of *PHIPA*, Records created by health care practitioners employed by the District, including psychologists, social workers, and speech language pathologists, with respect to the provision of services to students, the OCDSB is the Health Information Custodian.
- 3.8 ~~The Board recognizes that students should be advised that while staff members are willing to discuss personal issues with students, staff cannot guarantee that the information will not be disclosed to anyone; the staff member may have a professional and/or legal obligation to disclose the information to the student's parents or other appropriate authorities.~~ The Board recognizes that when students choose to interact with staff about personal issues, staff might have legal or professional obligations to disclose that information to parents/guardians, or others depending on the circumstances. Staff should be aware of these limits on confidentiality, and where applicable should make students aware of these limits.

4.0 SPECIFIC DIRECTIVES

Awareness

- 4.1 The Director or designate shall ensure that all policies, procedures, manuals, and guidelines relating to the management of Personal Information are ~~made~~ readily available to the public.
- 4.2 The District shall provide training opportunities to staff, as required, with respect to the obligations under the applicable privacy legislation, this policy, and associated procedures.

Implementation

- 4.3 The District shall ~~be responsible for compliance~~ comply with the *MFIPPA*, the *PHIPA*, and other applicable privacy legislation ~~with respect to:~~

- a) ~~the collection, use, disclosure, retention, and protection of Personal Information in its custody;~~
 - b) ~~administering requests for access to information and or correction of Personal Information;~~
 - c) ~~defending decisions made under the MFIPPA at an appeal appeals to the Information and Privacy Commissioner;~~
 - d) ~~managing any Privacy Breaches; and~~
 - e) ~~any other responsibilities that may arise with respect to the District's obligations under the MFIPPA or other privacy legislation.~~
- 4.4 ~~For the purposes of Records created by health care practitioners employed by the District, including psychologists, social workers, and speech language pathologists, with respect to the provision of services to students, the OCDSB is the Health Information Custodian as defined by PHIPA.~~
- 4.5 ~~The District shall ensure that the purposes for which Personal Information is collected are specified and noted in conjunction with legal authority for the collection, and the coordinates of an individual who can answer questions about the collection.~~
- 4.6 ~~The Director or designate shall ensure~~ The District shall obtain an individual's informed consent is obtained for the collection, use, or disclosure of when collecting, using, or disclosing Personal Information, except where otherwise permitted by law. ~~Such exceptions are set out in the law and include where legal, medical, or security reasons make it impossible or impractical to seek consent.~~
- 4.7 The District shall accept all forms of consent, including written, verbal, in-person, electronic, implicit, explicit, or implied. Consent may be obtained ~~consent through~~ from the individual or their authorized representatives, ~~as appropriate in the circumstances.~~
- 4.8 ~~The Director or designate shall ensure Personal Information only be used or disclosed for the purposes for which it was collected, other purposes consented to, or as required or permitted by law. The District shall only use or disclose Personal Information for the purpose it was collected or for a consistent purpose unless otherwise permitted by law.~~
- 4.9 ~~The denial of access to Personal Information shall be limited, specific, and in accordance with the exemptions set out in the MFIPPA, with the ability for such decisions to be reviewed by an independent agency (i.e. the Information and Privacy Commissioner of Ontario appeal process).~~
- 4.10 The District shall only keep Personal Information ~~may only be kept for~~ as long as is necessary to satisfy the purposes for which it was collected, or as required or permitted by law. Record retention shall be ~~or~~ in accordance with the OCDSB's Records and information management policy-Policy P 027 GOV - Management of Official Business Records.

- 4.11 The ~~Director or designate~~ District shall ensure any Personal Information that is collected, used or disclosed ~~should be~~ is as accurate, complete, and up-to-date as is necessary to fulfill the specified purpose ~~for its collection, use, disclosure, and retention.~~
- 4.12 The District shall ensure ~~the protection of~~ Personal Information ~~from unwarranted~~ is protected against improper release, or misuse by implementing ~~Security~~ safeguards appropriate to the information's format and sensitivity. ~~Safeguards may be physical, organizational, or technological, contingency plans or measures for using Personal Information off-site.~~
- 4.13 When contracting with a Third-party Service Provider, the District shall, as best as it can given the circumstances, ensure through any applicable contract, that the Third-party Service Providers ~~is who have custody of Personal Information on behalf of the OCDSB~~ are held accountable for the required protection of ~~that information~~ the Personal Information, and that the Third-party Service Providers ~~are obligated~~ agrees to abide by the privacy principles outlined in OCDSB ~~privacy~~ policies, procedures, and practices.
- 4.14 The Director of Education/~~Secretary of the Board~~ is authorized to issue such procedures as may be necessary to support this policy.

5.0 APPENDICES

Appendix A: Policy Definitions

6.0 REFERENCE DOCUMENTS

Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, Chapter M.56

~~Regulation 372~~

~~Regulation 823~~

The Education Act, R.S.O. 1990, Chapter E.2

A Guide to Privacy and Access to Information in Ontario Schools. The Information and Privacy Commissioner of Ontario

Privacy Breaches Guidelines for Public Sector Organizations, The Information and Privacy Commissioner of Ontario

OCDSB Policy P.027.GOV: Management of Official Business Records

OCDSB Policy P.047.FAC: Video Surveillance

OCDSB Policy P.018.GOV: Electronic Meetings of the Board and Committees and Meeting Attendance

OCDSB Policy P.074.IT: Information Technology Security

OCDSB Procedure PR.669.GOV: Privacy Breach

OCDSB Procedure PR.638.IT: Donation of Obsolete Computer Hardware

OCDSB Procedure PR.615.FAC: Video Surveillance

OCDSB Procedure PR.564.IT: Information Technology Security

OCDSB Policy P.100.IT: Appropriate Use of Technology

OCDSB Procedure PR.622.IT: Appropriate Use of Technology (Students)

OCDSB Procedure PR.702.IT Appropriate Use of Information Technology (Staff)

OCDSB Procedure PR.672.IT: Electronic Communications Systems

OCDSB Procedure PR.510.GOV: Official Access and Correction Requests under the MFIPPA

APPENDIX A: POLICY DEFINITIONS

In this policy,

Access means the authority or permission to consult Records or to obtain restricted information.

Collect means to gather, acquire, receive or obtain the information by means from any source.

Confidential Record means a Record containing certain information that requires protection against unauthorized access or disclosure.

Disclose means to make the information available or to release it to another institution or to another person, but does not include using the information.

Informal Access means oral requests for Personal Information should be granted if a head may give access to information under the MFIPPA.

Informed Consent means informed consent is provided when the person consenting understands the nature of the information for which consent is sought, understands the potential consequences of signing the consent form, and is given the right to revoke the consent at any time.

Notice means:

- a) before disclosing a Record, the head shall cause notice to be given to any person to whom the information in the Record relates, if it is practicable to do so;
- b) written notice to the applicant regarding an extension to respond to a MFIPPA request for information;
- c) written notice to the applicant and to any person to whom the information in the Record relates of the decision to disclose or refusal to disclose, including appeal procedures; and
- d) written notice regarding the legal authority for the collection, the principal purpose or purposes for which the Personal Information is intended to be used, and a contact individual who can answer questions regarding the collection.

Personal Information means recorded information about an identifiable individual, including,

- a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
- b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information 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 views or opinions of another individual about the identifiable individual, and
- 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.

Personal information does not include information about an individual who has been dead for more than thirty years.

Personal Information Bank means a collection of Personal Information that is organized and capable of being retrieved using an individual's name or an identifying number or particular assigned to the individual.

Privacy means the quality or condition of being secluded from the presence or view of others. The state of being free from unsanctioned intrusion: a person's right to privacy.

Privacy Breach means an infraction or violation with respect to the collection, use, disclosure, retention, or destruction of Personal Information that is inconsistent with amounts to a violation of the applicable privacy legislation.

Privacy Impact Assessment (PIA) means an assessment framework used to identify the actual or potential risks that a proposed or existing information system, technology, or program may have on an individual's privacy.

Privacy Standard means a set of rules, policies, procedures, guidelines, and characteristics that helps to foster a culture of privacy regarding the way the OCDSB collects, uses, disclosures, secures, retains, and disposes of Personal Information. It also ensures the right of individuals to have access to Personal Information about themselves and, as appropriate, to have it corrected.

Record means any Record of information however Recorded, whether in printed form, on film, by electronic means or otherwise, and includes,

- a) correspondence, a memorandum, a book, a plan, a map, a drawing, a diagram, a pictorial or graphic work, a photograph, a film, a microfilm, a sound Recording, a videotape, a machine readable Record, any other documentary material, regardless of physical form or characteristics, and any copy thereof, and
- b) subject to the applicable regulations, any Record that is capable of being produced from a machine readable Record under the control of an institution by means of computer hardware and software or any other information storage equipment and technical

expertise normally used by the institution.

Retention means the minimum amount of time to keep a Record as determined to be necessary by law or other authority. Original Records cannot be destroyed until the retention time has expired. Likewise, Records should not be retained longer than the retention time without good reason.

Security means the protection of Personal Information regardless of the format in which it is held and includes but is not limited to, physical measures such as locked filing cabinets and restricted offices; organizational measures such as limited access, and technological measures, such as the use of passwords and encryption.

Third-party Service Provider means any outside individual (such as a consultant), a business, or an organization that provides a service to, or acts on behalf of, the OCDSB.