

# Protection of Privacy Policy Support Document

## Privacy and Information Management (PIM) of Personal Information



## Contents

A.	Responsibilities .....	2
B.	Definitions .....	2
C.	Collection and use of student personal information.....	3
D.	Collection and use of other personal information .....	3
E.	Collection and use of student personal health information .....	4
F.	Disclosure of personal information.....	4
G.	Student expectation of privacy .....	5
H.	Third party contractors and sharing of personal information .....	6
I.	Access to information/court orders .....	6
J.	Third party requests for information.....	7
K.	Release of information .....	8
L.	Media at school .....	10
M.	Privacy breaches .....	10
N.	Ontario Education Number (OEN).....	11
O.	How the OCSB collects, uses and discloses student personal information .....	11
P.	Best practices for protecting personal information .....	12

## See also

- [Notice of Collection Use and Disclosure](#)
- [Consent for the Use and Disclosure of Student Information](#)
- [Consent to Receive Copies of Information Contained in an OSR](#)
- [Student Registration Form](#)

## A. Responsibilities

**Principals/Managers and Superintendents** are responsible for:

- a. implementing reasonable security measures and safeguards to protect student personal information;
- b. ensuring that staff are aware of and adequately trained in their responsibilities as set out in this document and other Board policies, procedures and guidelines; and
- c. ensuring that agreements with service providers contain privacy protection provisions with regard to the protection, collection, use, retention and disclosure of personal information.

**Staff** is responsible for:

- a. complying with legislation, professional standards, Board administrative policies and procedures, when using personal information;
- b. protecting personal information by following proper procedures and best practices as outlined in this document and as directed by your supervisor;
- c. reporting any suspected privacy or security breaches of which they are aware;
- d. taking reasonable steps to ensure the personal information within their custody and control is secured and protected; and
- e. participating in training regarding their obligations to protect personal information.

## B. Definitions

1. “**personal information**” has the same meaning as in the Municipal Freedom of Information and Protection of Privacy Act, and includes all information about an identifiable individual, including but not limited to:
  - i. Personal contact information;
  - ii. Biographical information;
  - iii. Financial information; and
  - iv. Employment information.
2. “**student personal information**” means personal information about a student of the Board, and may include information within the student’s Ontario Student Record (“OSR”) and information outside of the OSR.

## C. Collection and use of student personal information

1. Personal information will be collected directly from the student or his/her parent/guardian for the development and delivery of educational program and services.
2. At the time of collection individuals must be given notice of the legal authority for collection, the purpose(s) of its intended use and the title and contact information of an individual who may respond to specific questions regarding the collection.
3. A student's personal information may be used by employees of the Board who need the information, including access to a record, in the performance of his or her duties. Use of personal information for this purpose is in accordance with MFIPPA and the Education Act.
4. The Board shall make available its Index of Personal Information Bank, which outlines student personal information that is routinely collected and used for the purpose of providing educational programming.
5. Use and disclosure of student personal information for a purpose other than planning and delivering educational programs and services, or a purpose reasonably consistent with that purpose, or in accordance with the specific exceptions outlined in MFIPPA and PHIPA will require written consent.
6. A student who is under 18 will generally have his or her privacy rights exercised by a parent/guardian, on the student's behalf without specific authorization.
7. When a student aged 16 or 17 withdraws from parental custody and has informed the Principal about such a withdrawal in writing, the student's sole consent for the collection, use and disclosure of his/her personal information shall be sufficient.

## D. Collection and use of other personal information

1. The Board may from time to time collect personal information other than student personal information in the course of fulfilling its mandate.
2. The Board will only collect personal information where it is reasonably related to the Board's mandate.
3. The Board will collect personal information directly from the individual to whom the information relates, except where an exemption under MFIPPA may apply.
4. The Board will advise the individual at the time of collection of the purpose for which the information is being collected.

5. Personal information in the board's custody will be used for the purposes for which it was collected, and for reasonably consistent purposes. If the Board is contemplating using personal information for a purpose which is not reasonably consistent with the purpose for which it was collected, or for another purpose permitted by MFIPPA, the Board will seek consent.

## E. Collection and use of student personal health information

1. The Board utilizes the services of and employs health professionals (e.g. speech language pathologists, psychologists, social workers) who are required to treat personal health information in accordance with the Personal Health Information Protection Act, 2004 and applicable professional standards. Personal health information will only be disclosed with appropriate consent.
2. The Board collects personal health information from health professionals with the consent of the parent/guardian/student and only as necessary for the purpose of delivering educational programs and services that best meet student needs. A signed consent form describing the purpose use of the personal health information is presented to the health professional authorizing the release of the record(s).
3. Personal health information received by Board staff may be used for the purposes identified in the consent form and may be shared only with staff members if it is necessary for them to perform their duties – i.e. ordinarily to staff members who are working directly with or have responsibility for the student.

## F. Disclosure of personal information

MFIPPA sets out when the Board may use or disclose personal information in its custody and control without the consent of the individual to whom the information relates.

### a. Consistent Purpose

Information may be disclosed for the purpose for which it was obtained or compiled or for a consistent purpose provided that the individual about whom the information relates might reasonably have expected such a use or disclosure of the information.

### b. With Consent

If the person to whom the information relates has identified that information in particular

and consented to its disclosure, that information may be disclosed. When dealing with minors, it is a best to have consent in writing with an original signature from the parent.

#### c. Legal Authority

Personal information may be disclosed for the purpose of complying with an Act of the Legislature or an Act of Parliament, an agreement or arrangement under such an Act.

#### d. Law Enforcement

Personal information may be disclosed to an institution or a law enforcement agency in Canada to aid an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result. Examples include police, and the Ministry of Community and Social Services Eligibility Review Officers. The contents of the OSR may be made available to the police in the following circumstances:

- i. With the written permission of the parent or guardian of the student or, where the student is an adult, with the written permission of the student, or where the student is 16 or 17 years of age and has withdrawn from parental support; and
- ii. Through a warrant requiring the surrender of an OSR to the police.

#### e. Health and Safety

Personal information may be disclosed in compelling circumstances affecting the health or safety of an individual. When disclosing information under this section the imminence and reasonableness of the risk to health and safety must be considered and balanced with the invasion of privacy.

## G. Student expectation of privacy

In all OCSB locations, staff must be aware of a student's expectation of privacy. Any personal electronic device with image, video capture, and recording capabilities are absolutely prohibited in areas where there is an expectation of privacy (e.g. washrooms, change rooms). The recording and taking of photographic images of a person or persons, on school property is prohibited without the permission of the person or persons being photographed or the principal or designate.

## H. Third party contractors and sharing of personal information

1. The Board has entered into agreements with various service providers and contractors in relation to the development and delivery of educational programs and services, and in relation to the administrative operations required to support its mandate in that respect. For example, the Board has entered into agreements for the provision of software and related services which assist it in delivering services to students and managing the operations of its schools.
2. Depending on the nature of services provided by a contractor, it may be necessary for the contractor to have access to personal information in the Board's custody.
3. Personal information will be shared with a contractor where reasonably required to perform the services for which the contractor has been retained. Personal information will be used and disclosed in this way where the purpose for the use is the same or reasonably consistent with the purpose for which it was collected.
4. Where a contractor will have access to personal information in the Board's custody, the Board will ensure that it has agreements in place with the Contractor requiring the contractor to take all reasonable precautions to protect the personal information to which it has access from unauthorized access, use or disclosure.
5. The contractor will be required to undertake that any employee of the contractor who has access to personal information in the course of providing services to the Board will be required by the Contractor to execute a confidentiality agreement as a condition of having access to personal information in the custody of the Board.
6. The Board will remain at all times responsible for personal information in its custody or control, whether in the hands of the Board or in the hands of a third contractor.

## I. Access to information/court orders

Access to OSR and non-OSR student personal information is governed as follows:

- a. All parents/legal guardians have a right to examine the OSR, request corrections and request the removal of information, subject to the dispute resolution mechanisms outlined in the Education Act, until their child turns 18 unless this right is limited by a court order, custody or separation agreement. It does not give rights to access personal information about the other parent or other individuals;

- b. Access to other information not contained in the OSR is governed by MFIPPA;
- c. A person who has access rights to the OSR also has the right to receive a copy of anything in the OSR. A student has access to his/her OSR at any age and is entitled to receive copies; however, access shall occur in the presence of the Principal or designate, who can provide explanations about the records;
- d. In the absence of a court order or separation agreement, a parent who had legal custody continues to have access to the same information about the student's health, education and welfare until the student turns 18 or turns 16 or 17 and removes him/herself from care and control of his/her parent/guardian;
- e. Principals shall abide by court orders, however they are not responsible for enforcing the order and should problems arise, the parent must apply to the family court for enforcement; and
- f. All relevant staff shall be made aware of any custody orders regarding their students, which include any limitations on a parent's right to information about a student.

The following points further clarify parental access to information:

- a. A non-custodial parent does not have access to the child at school unless it is specifically set out in the court order that access to the child at school shall be permitted;
- b. Custodial parents and noncustodial parents with a right of access to their child ("access parents") also have a general right to be given information concerning their children's health, education and welfare unless this right is limited by a court order, custody or separation agreement. Non-custodial parents with access have a right to information and may examine an OSR.

Access to other information will be in accordance with the rules and procedures set out in MFIPPA.

## J. Third party requests for information

1. Information will not be disclosed to third parties upon request, including legal counsel, without the consent of the parent/guardian/student, as applicable. An executed release form which clearly identifies the information requested may be used as authority to release the information.
2. Staff must take reasonable care to authenticate the request, which may include contacting the parent/guardian/adult student or requesting identification or credentials.

3. Consent forms for access to OSR records shall be retained in the OSR.

Staff will not:

- a. provide letters supporting parenting capability or otherwise become involved in a parent's litigation, beyond providing access to student personal information where permitted by these procedures;
- b. agree to participate in an interview with a parent's lawyer;
- c. complete testing or assessment reports that do not comply with established Board testing criteria; or
- d. provide assessments or opinions on matters other than a student's educational progress or educational needs.

## K. Release of information

### Government agencies

Government agencies or officials may request student personal information in the course of conducting their duties. Board staff members shall take steps to ensure the request is properly authorized and that the legal authority is valid. Such requests may include:

#### a. Ottawa Children's Aid Society

In accordance with the Child and Family Services Act, the Family and Children's Services may collect information about a student under 16 when investigating child protection cases. The Board liaison is the Chief Social Worker in the Special Education & Student Services Department.

#### b. Ministry of Education

In accordance with Section 8.1 of the Education Act, the Minister of Education may collect personal information directly or indirectly, for purposes related to the following matters, and may use it for those purposes:

- i. administering the Education Act and the regulations, and implementing the policies and guidelines made under the Education Act;
- ii. ensuring compliance with the Education Act, the regulations, and the policies and guidelines made under the Education Act;



iii. planning or delivering programs or services that the Ministry of Education provides or funds, in whole or in part, allocating resources to any of them, evaluating or monitoring any of them or detecting, monitoring and preventing fraud or any unauthorized receipt of services or benefits related to any of them; and

iv. implementing risk management, error management or activities to improve or maintain the quality of the programs or services that the Ministry of Education provides or funds, in whole or in part; conducting research and statistical activities that relate to education and are conducted by or on behalf of the Ministry.

#### c. Medical Officer of Health

Section 266(2.1) of the Education Act states that the following information is available, upon request, to the Medical Officer of Health serving the area in which the Board is located:

- the pupil's name, address and telephone number;
- the pupil's date of birth; and,
- the name, address and telephone number of the pupil's parent(s) or guardian(s).

The required information is normally requested through the appropriate school principal, Superintendent or Associate Director's Office and forwarded to the Medical Officer of Health. Personal information may also be required to support Mandatory Public Health Programs, e.g., communicable disease and oral health, under the Health Protection and Promotion Act.

#### d. The Office of the Children's Lawyer

Any school board information requested by the office of the Children's Lawyer or representative, will be provided directly to the custodial or access parent(s).

#### e. Youth Criminal Justice Act

The Youth Criminal Justice Act (YCJA) protects the privacy and identity of young persons involved in the criminal justice system. The provisions of the YCJA prohibit all persons, including police, youth courts and school board officials from disclosing the identity of a young offender.

Disclosure is allowed between police services and school authorities to ensure safety of

staff, students or other persons or when authorized by a court order. The YCJA also includes provisions that deal with the disclosure, security, storage and destruction of information pertaining to young offenders. The sharing of information must take into account a balance between the need to share information in a timely fashion, particularly when safety is a concern, and the need for personal privacy.

## L. Media at school

1. Principals are responsible for ensuring each student in their school has a signed copy of the 2016 Consent for the Use and Disclosure of Student Information Form on file in the student's OSR.
2. Principals will decide if the media will have access to the school, staff or students. When the media is present, students should not participate if there is no consent granted on their 2016 Consent for the Use and Disclosure of Student Information Form. All access to students and all interviews must be conducted under the supervision of a staff member.
3. The Communications Department is available to give guidance and support for high-profile events. As a courtesy where possible, parents/guardians should be notified prior to any high profile interview/media coverage.

## M. Privacy breaches

1. A privacy breach occurs when personal information is lost, stolen, or subject to unauthorized access or disclosure, contrary to the Education Act or the MFIPPA. This includes the loss of computers, personal devices or media that contain personal information. In accordance with MFIPPA, individuals shall be informed when their personal information is involved in a privacy breach.
2. If staff becomes aware of a privacy breach, they must immediately notify their supervisor to ensure that immediate action can be taken to mitigate the impact/results of the breach.
3. For information about responding to a privacy breach, contact your Superintendent or the Board Freedom of Information Officer.

## N. Ontario Education Number (OEN)

1. The Ontario Education Number (OEN) is a unique number assigned to each person who is enrolled in a school.
2. The Education Act allows for the OEN to be collected, used, or disclosed for purposes such as the provision of educational services and for purposes related to education administration, funding, planning, research, and for providing financial assistance to students.
3. No person shall, collect, use, or disclose another person's OEN except as provided by the Education Act. The OEN is to be used only for educational purposes. The OEN will be used:
  - a. on pupil records that are compiled and maintained in accordance with the Education Act or under any policy, guideline or directive issued by the Minister relating to pupil records; and
  - b. on applications made by the individual for enrolment in an educational program, school or institution; on pupil assessments, tests and evaluations of the individual.

## O. How the OCSB collects, uses, and discloses student personal information

The information collected during the school registration process is personal information as defined in the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) and is collected pursuant to the provisions of the Education Act.

The Education Act sets out the duties and powers of the board and authorizes school boards to collect personal information for the purpose of planning and delivering educational programs and services which best meet students' needs and for reporting to the Minister of Education as required. It also requires that the school principal maintain an Ontario Student Record (OSR) for each student attending the school. The OSR is a record of a student's educational progress through school in Ontario and follows students when they transfer schools. Under the MFIPPA, personal information may be used or disclosed by the Ottawa Catholic School Board:

- a. for the purpose for which it was obtained or a consistent purpose (a purpose consistent for the reason collected);

- b. to board officers or employees who need access to the information in the performance of their duties if necessary and proper in the discharge of the board's authorized functions; and
- c. to comply with legislation, a court order or subpoena or to aid in a law enforcement investigation conducted by a law enforcement agency; and, in compelling circumstances affecting health or safety (providing notice of the disclosure is sent to the student's home).

The following are the purposes for which the OCSB may use and disclose student personal information:

### Student instruction, achievement, and well-being

1. The student's OSR will be used by school and board staff to support the classroom teacher in developing an educational program which best meets the student's needs. Staff working with the classroom teacher or directly with the student may include individuals working in areas such as Special Education, guidance counselling, student success, etc.
2. OCSB intermediate/secondary schools may receive information about registered Grade 6 or Grade 8 students in advance of the student attending the intermediate/secondary school to help plan an appropriate program for the student.
3. Students may be recorded or photographed by staff in school or during school activities as part of their educational program and for assessment purposes.
4. Contact information, marks and transcripts are shared with Ontario colleges and universities to support post-secondary applications.
5. Referrals to personal health services such as psychological assessments, speech and language assessments, social work and child and youth service consent requirements are in accordance with the Personal Health Information Protection Act (PHIPA). On referral, you will be advised of how personal health information is collected and used.
6. Aboriginal ancestry information of First Nation, Métis and Inuit students who chose to voluntarily self-identify will be used to allocate resources, improve student learning and student success, and to offer individualized supports and opportunities to students and families. Aboriginal heritage information will also be reported to the Ministry of Education and the Education Quality Accountability Office (EQAO).

## Health and safety/transportation

1. Student demographic information and life-threatening medical conditions will be released to the Ottawa Student Transportation Authority and the contracted bus companies responsible for transporting students in order to administer the Board's contracted transportation program.
2. Surveillance equipment may be used in schools and on buses to enhance the safety of students and staff, to protect property against theft or vandalism, and to aid in the identification of intruders and of persons who endanger the health, wellbeing or safety of school community members.
3. Phone numbers will be used on emergency telephone lists. Examples include: emergency contact lists to facilitate contact with parents/guardians during emergencies (e.g. inclement weather).
4. Student information may also be shared with emergency responders or the hospital in the case of a medical emergency.
5. Student information may also be shared with the Ottawa Regional Health Dept., Ottawa Children's Aid Society or others as required by law.
6. Information may be used to deal with matters of health and safety or discipline and is required to be disclosed in compelling circumstances or for law enforcement matters or in accordance with any other Act.
7. Student accidents that take place during school or on school-sponsored activities may be reported to the Board insurer. Reports include the name of the injured student(s) and details about the incident as well as the name and contact information of witnesses to the accident.

## School events and activities

1. Birthday congratulations may be announced over the PA system and/or in the classrooms.
2. Contracted photographers will take individual and class photos of students. These photos will be used for administrative and archival purposes, on student cards, in school yearbooks and will be offered to parents/guardians for purchase.
3. Student first and last names and/or photographs may be printed in school programs (e.g. commencement or graduation programs, school plays and musical productions, student awards, academic and athletic awards and plaques, school brochures, honour roll and classroom assignments) and in school yearbooks (print & digital).

4. Student work, including student's first name, may be displayed in the classroom or in school hallways, or may be shared with the public through science fairs, school and board newsletters, social media, writing/colouring/poster contests, community events, fairs, and similar events/locations outside the school setting.
5. When the media are invited to schools and board sites to report on school/board events or activities, students may be photographed/recorded as part of a group, but only those students with appropriate consents will be interviewed and identified.
6. Parents/guardians/students over age 18 should be aware that when students participate in school events on or off school grounds, the school principal is unable to prevent any media exposure, photographs or recordings which may be posted online by a third party. If you have concerns about your child's participation in such forums, please speak to the school principal.

## Educational technology

1. Students will be using educational tools in the classroom that may include; Google APPS for Education (GAFE), Desire2Learn (D2L) and other tools such as wikis, blogs, podcasts, video conferencing and surveys.
2. The OCSB uses various technological tools and software to administer the operation of schools and the delivery of educational programs and services. These tools and software will, in some cases be used in conjunction with personal information in the OCSB's custody. The use of these tools may result in personal information being stored on remote servers or cloud-based systems. The OCSB will take all reasonable precautions to ensure that information is subject to the same standard of privacy protections whether it is on the OCSB's own servers or stored on a remote or cloud-based server. The OCSB follows the guidance of the Ontario Information and Privacy Commissioner in its use of these tools and software.

## P. Best practices for protecting personal information

These best practices reflect OCSB's commitment to protecting personal information. Employees are expected to follow these best practices in the course of their duties.

1. Restrict access to those employees that require the records and information in the performance of their assigned duties.

2. Ensure that sensitive and confidential information is not visible to the public.
3. Encourage a clean desk policy to reduce the risk of exposing confidential information to others.
4. Lock doors and filing equipment when the office is not in use.
5. Label filing cabinets, drawers, boxes and other storage containers in a manner that maintains the anonymity of items in storage.
6. Keep open filing equipment behind a counter or other physical barrier to the public.
7. Locate FAX machines and printers in a secure area, and retrieve sensitive documents immediately.
8. Phone the recipient to confirm receipt of a fax containing sensitive information.
9. Ensure that secure confidentiality is maintained when transporting confidential information (e.g. student assignments or exams home for marking).
10. Ensure records that are the property of the Board, in particular student assignments and exams, are not removed from Board control when an employment contract is terminated. (i.e. return all student assignments)
11. Know how long to retain personal information, and securely destroy it as per the **OCSB Records Retention Schedule**.
12. Ensure confidential destruction of paper records by placing the records in one of the locked shredding boxes for pick up by the shred vendor.
13. Shut down programs or use password protection when leaving work area.
14. Position screens to prevent unauthorized viewing and do not disclose passwords.
15. Notify the Human Resources Department if there is a change in an employee's employment status.
16. Report any lost or stolen records to your immediate supervisor.
17. Use a file checkout procedure for OSRs and Personnel files, the file's temporary location's name, and date borrowed must be recorded, to easily locate files.