



## Administrative Procedures Memorandum

#: APC023

### Student Personal Information Collection/Use/Disclosure

**Date of Issue:** September 2002  
**Reviewed/Revised:** December 2002, May 2009, May 2011, May 2013, May 2014, April 2015, April 2016, October 2017, May 2018

**Memo To:** All Staff

**From:** Director of Education

---

#### ACCESSIBILITY:

To request this file in large print, please email [aoda@wcdsb.ca](mailto:aoda@wcdsb.ca) or call (519) 578-3660.

#### PURPOSE:

The Waterloo Catholic District School Board (WCDSB) is committed to the protection of personal information under its control & custody, and to the right of privacy with respect to student personal information that is collected, used, disclosed, and retained in the board.

The WCDSB adheres to all applicable provisions 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 as it relates to privacy.

#### REFERENCES:

- IV 002 Board Policy Treatment of Public
- IV 003 Board Policy Treatment of Students
- Education Act and Regulations
- Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)
- Personal Health Information Protection Act (PHIPA)
- Occupational Health and Safety Act
- The Health Protection & Promotion Act, 1990
- The Immunization of School Pupils Act, 1987
- Copyright Act, 1985
- Ontario College of Teacher Act, Reg. 437/97
- Ethical Standards for the Teaching Profession
- Child and Family Services Act
- Youth Criminal Justice Act
- Ontario Student Record Guideline
- AP Memo APS020 Suspected "Child in Need of Protection" Reporting

## FORMS:

- APC023-02F: [Student Image, Video or Voice Recording Including Media Use, Consent](#)
- APC023-03F: [Specific External Organization Event Photographs & Recordings, Consent, Waiver and Release](#)
- APC014-03F: [Release of Information to Third Parties, Parent/Guardian Consent](#)

## REPORTS:

- N/A

## APPENDICES:

- Appendix A: [Student Personal Information Collection/Use/Disclosure Notice](#)

## COMMENTS AND GUIDELINES:

The information collected during the school registration process is personal information and is collected pursuant to the provisions of the Education Act and Regulations and maintained in compliance with Municipal Freedom of Information and Protection of Privacy Act (MFIPPA). It is our practice to include a notice statement on forms used to collect personal information to advise you how we will use and disclose the information.

## Definitions

1. **Personal information** refers to information about an identifiable or potentially identifiable individual and includes, but is not limited to, personal health information and opinions about the individual.
2. **Personal health information** is information about an individual that pertains to health care, including information about an individual's physical or mental health.
3. **Privacy** is the right or interest of an individual to control the collection, use, and disclosure of his/her personal information. Privacy is a legislated right and school boards are required to comply with provincial privacy laws.
4. **Confidentiality** is a duty imposed on an organization or individual by laws or professional and ethical standards to restrict access to or disclosure of certain information, which may include personal and/or business information.
5. **Security/Control** refers to measures designed to protect personal information regardless of media.

## Legal Framework

### Municipal Freedom of Information and Protection of Privacy Act

The Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) requires the WCDSB to protect the privacy of individuals with respect to personal information about themselves held by the WCDSB and to provide individuals with a right of access to their own personal information.

The protection of privacy includes the appropriate collection, use, retention and disclosure of personal information, including the use of appropriate security measures to protect information from unauthorized access.

### Education Act

The Education Act sets out the authority of a school board to collect and use personal information of students for the provision of educational services to students. Personal information is collected in accordance with Section 265(1)(d) of the Education Act, which states that information may be collected in accordance with the Act, Regulations or Guidelines issued by the Minister.

Additionally, Section 266 of the Education Act provides for the establishment of the student's Ontario Student Record (OSR) in accordance with the OSR Guideline. Section 266 of the Education Act requires that every person shall preserve secrecy in respect of the content of an OSR that comes to the person's knowledge in the course of his or her duties or employment, and no such person shall communicate any such knowledge to any other person except:

- As may be required in the performance of his or her duties; or
- With the written consent of the parent or guardian of the student where the student is a minor; or
- With the written consent of the student where the student is an adult.

## **Ontario College of Teachers Act - Professional Misconduct**

The Ontario College of Teachers Act, Regulation 437/97 defines the following as professional misconduct: Releasing or disclosing information about a student to a person other than the student or, if the student is a minor, the student's parent or guardian.

The release or disclosure of information is not an act of professional misconduct if, the student (or if the student is a minor, the student's parent or guardian) consents to the release or disclosure, or if the release or disclosure is required by law.

## **Responsibilities**

Principals/Managers and Superintendents are responsible for:

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

Staff are responsible for:

- Complying with legislation, professional standards, WCDSB administrative policies and procedures, when using personal information.
- Protecting personal information by following proper procedures and best practices as outlined in this document and as directed by your supervisor.
- Reporting any suspected privacy or security breaches of which they are aware.
- Taking reasonable steps to ensure the personal information within their custody and control is secured and protected.
- Participating in training regarding their duties and obligations to protect personal information.

## **Collection and Use of Student Personal Information**

1. Personal information will be collected directly from the student or his/her parent/guardian for the creation and delivery of appropriate educational program(s).
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 WCDSB who need the information, including access to a record, in the performance of their duties. Use of personal information for this purpose is in accordance with MFIPPA, and the Education Act.
4. The WCDSB shall publish annually a [Student Personal Information Collection/Use/Disclosure Notice](#), (APC023-AX: Appendix A), which outlines student personal information that is routinely collected and used for the purpose of providing educational programming. This notice statement shall be reviewed annually, included in student handbooks, and posted on the WCDSB website. Consent to the collection and use of information as outlined in the aforementioned notice is not required; however parents/guardians/students are invited to communicate any concerns they may have with their school principal.

5. Use and disclosure of student personal information for a purpose other than planning and delivering educational programs and services or in accordance with the specific exceptions outlined in MFIPPA and PHIPA will require written consent. See [Release of Information to Third Parties, Parent/Guardian Consent \(Form APC014-03F\)](#).
6. A student who is under 16 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.
8. Please note that when a student turns 18 years of age, he or she is considered to be an adult. According to the Education Act, the school must have written consent from the student before it can share information regarding his or her attendance or academic program.

## **Collection and Use of Student Personal Health Information**

The WCDSB 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.

The WCDSB collects personal health information from health professionals with the consent of the parent/guardian/student and only as necessary for the purpose of planning and delivering educational programs and services that best meet student needs. A signed consent form describing the purposed use of the personal health information is presented to the health professional authorizing the release of the record(s).

Personal health information received by WCDSB 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.

## **Disclosure of Personal Information**

MFIPPA sets out when the WCDSB may use or disclose personal information in its custody and control without the consent of the parent/guardian/student as follows:

### **1. 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.

### **2. 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 practice to have consent in writing with an original signature from the parent/guardian.

### **3. 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. Contact your Superintendent of Education or the Privacy and Information Management Officer with any questions related to disclosures of this kind.

### **4. 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, the Ministry of Community and Social Services Eligibility Review Officers. In non-urgent situations, police shall provide a written statement that personal information is required for investigative purposes.

The contents of the OSR may be made available to the police in the following circumstances:

- 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
- Through a warrant requiring the surrender of an OSR to the police

## 5. 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 and the Superintendent of Education must be consulted.

## Access to Information/Court Orders

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

### Parents

1. 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 or a separation agreement. It does not give rights to access personal information about the other parent or other individuals.
2. Access to other information not contained in the OSR (or on the way to being part of the OSR) is governed by MFIPPA.
3. 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, who can provide explanations about the records.
4. 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 until he/she turns 16 or 17 and removes him/herself from care and control of his/her parent/guardian.
5. Principals shall abide by court orders, however they are not responsible for enforcing the order and should problems arise, the parent must enforce the court order.
6. 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:

1. 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.
2. Custodial parents and non-custodial 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 or a separation agreement. Non-custodial parents with access have a right to information and may examine an OSR.

## Third Party Requests for Information

Information **must not** be disclosed to third parties, including the student's lawyer, without the consent of the parent/guardian/adult student. An executed release form which clearly identifies the information requested may be used as authority to release the information. If a consent form is required see [Release of Information to Third Parties, Parent/Guardian Consent](#) (Form APC014-03F).

Staff must take reasonable care to authenticate the request, which may include contacting the parent/guardian/adult student or requesting identification or credentials.

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

Staff must not:

- Provide letters supporting parenting capability or otherwise provide student information for the sole purpose of supporting a parent's litigation.
- Agree to participate in an interview with a parent's lawyer without a court order.
- Complete testing or assessment reports that do not comply with established WCDSB testing criteria.
- Provide assessments or opinions on matters other than a student's educational progress or educational needs.

## **Release of Information**

### **Government Agencies**

Government agencies or officials may request student personal information in the course of conducting their duties. WCDSB staff members shall take steps to ensure the request is properly authorized and that the legal authority is valid. If uncertain, WCDSB staff members shall consult with their Superintendent of Education or Privacy and Records Information Management Officer.

Such requests may include:

#### **1. Family and Children's Services**

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. See WCDSB AP Memo APS020 Suspected "Child in Need of Protection" Reporting.

#### **2. 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:

- Administering the Education Act and the regulations, and implementing the policies and guidelines made under the Education Act
- Ensuring compliance with the Education Act, the regulations, and the policies and guidelines made under the Education Act
- Planning or delivering programs or services that the Ministry 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
- Implementing risk management, error management or activities to improve or maintain the quality of the programs or services that the Ministry 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.

#### **3. 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 WCDSB is located:

- Pupil's name, address and telephone number
- Pupil's date of birth
- Name, address and telephone number of the pupil's parent or guardian

The required information is normally requested through the appropriate Superintendent 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.

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

Information will be provided to the custodial or access parent(s) who may provide it to the Office of the Children's Lawyer representative. The only instance in which information would be provided directly to the Office of the Children's Lawyer or their representative, would be with a court order.

#### 5. 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.

### Media Coverage at School

Principals shall ensure that student interaction with the media is conducted in accordance with the guidelines outlined below.

Principals must validate the credentials of any member of the media before inviting him/her onto school grounds, and in doing so, must collect and record the following information:

- The name and nature of the media corporation the person represents
- The topic of the feature/story (e.g. student achievement, school closures, health education)
- The type of information the reporter would like to gather from the student (regardless of what will actually be publicized), e.g. team photo, name of students, and school, or individual student photo, opinion on school activity

If principals have any questions or concerns they should contact the WCDSB's Chief Managing Officer or their School Superintendent for further direction.

Principals must:

- Ensure that the [Student Personal Information Collection/Use/Disclosure Notice](#) (APC023-AX: Appendix A), is posted annually in the student handbook or sent home in early September. This notice will inform parents in writing regarding the possibility of media exposure and of the principal's inability to control or prevent media exposure when a school-sponsored activity occurs off school grounds or when a school-sponsored activity occurs on school grounds but is open to the general public.
- Schools must collect the [Student Image, Video or Voice Recording Including Media Use](#) (Form APC023-02F) from students in September as part of the registration process. This form must be signed by the parent/guardian or student age 18 and over.
- When a principal invites a member of the media on to school grounds to report on school related activities, he/she must ensure that a signed [Student Image, Video or Voice Recording Including Media Use](#) (Form APC023-02F) is on file at the school for each student who participates in interviews or is featured in an interview or photo session.
- As a courtesy parents/guardians should be notified prior to any such interview/media coverage.
- Students must not participate if there is no consent granted.
- Interviews must be conducted under the supervision of a staff member.

### Specific Event Photographs & Recordings Consent, Waiver and Release

The [Specific External Organization Event Photographs & Recordings Consent, Waiver and Release](#) (Form APC023-03F) is to be used for events outside of the regular school/classroom, that will be published internally/externally of the board. These events would not normally be thought of as school-related activities i.e.

local parishes, researchers, training videos, special promotions, joint board projects. Prior to the event occurring, this form should be used to seek specific consent for a child to participate in photographs, video or audio recordings for the specific event which is over and above normal classroom/school events.

## **Privacy Breaches**

A privacy breach occurs when personal information is lost, stolen, or inadvertently disclosed contrary to the Education Act or the MFIPPA. This breach includes the loss of computers, personal devices or media that contain personal information. In accordance with MFIPPA, individuals shall be informed when the security of their personal information is breached.

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.

For information about responding to a privacy breach, contact your Superintendent of Education or the Privacy and Information Management Officer.

## **Ontario Education Number**

- The Ontario Education Number (OEN) is a unique number assigned to each person who is enrolled in a school.
- 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.
- 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 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.
  - Applications made by the individual for enrolment in an educational program, school or institution; on pupil assessments, tests and evaluations of the individual.

## **Best Practices for Protecting Personal Information**

These best practices reflect WCDSB's commitment to protect personal information.

The following are some best practices for security measures to ensure that any personal information accessible to employees remains confidential and protected:

1. Access to confidential records should be restricted only 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 or mail boxes 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 intended recipient to confirm receipt of a FAX containing sensitive information.
9. When transporting confidential information (e.g. student assignments or exams home for marking) ensure secure transportation and that confidentiality is maintained.
10. Ensure records that are the property of the WCDSB, in particular student assignments and exams, are not removed from WCDSB 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 WCDSB 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 on your computer when you leave your desk. (CTRL, ALT, DEL) or ⌘ (Windows) L
14. Computer screens should be positioned to prevent unauthorized viewing.
15. Notify Information Technology Services if there is a change in an employee's employment status.
16. Do not disclose/share passwords with others.
17. Report any lost or stolen records to your immediate supervisor.
18. Use a file checkout procedure for Ontario Student Records and Personnel files. The file's temporary location/borrower's name, and date borrowed must be recorded, to easily locate files.
19. Complete a Third Party Confidentiality and Privacy Agreement with third parties when outsourcing services that involve the storage or access to personal information under the custody or control of the WCDSB.