

PERSONNEL

Privacy

Adopted under the Privacy Policy

1.0 Objective

- 1.1 The Privacy Procedure (the “Procedure”) is adopted under the Privacy Policy of the Durham District School Board (the “DDSB” or “Board”) to:
 - 1.1.1 Support the proper Collection, Use, retention, Disclosure of Personal Information held by the DDSB in accordance with applicable legislation; and
 - 1.1.2 Support the process for accessing information under MFIPPA and PHIPA.
- 1.2 This Procedure is to be interpreted and applied in accordance with the DDSB’s commitment to promoting and upholding Indigenous rights and human rights in all of its learning and working environments. This includes anti-colonial, anti-discriminatory and anti-racist approaches and actions to provide services and employment that are safe, welcoming, respectful, inclusive, equitable, accessible and free from discrimination and harassment consistent with the DDSB’s [Human Rights, Anti-Discrimination and Anti-Racism Policy](#), the [Indigenous Education Policy](#), the [Safe and Respectful Workplace and Harassment Prevention Policy](#).

2.0 Scope

- 2.1 This Policy applies to DDSB employees, service providers, volunteers, trustees, and other individuals acting on behalf of the DDSB.
- 2.2 This Policy applies to all information in the Custody or under the Control of DDSB, including but not limited to the Personal Information of DDSB students, parents, and staff.

3.0 Definitions

In this Procedure,

- 3.1 “**Collect**” means to gather, acquire, receive, or obtain the information by any means from any source, and “Collection” and “Collected” have a corresponding meaning.
- 3.2 “**Control**” means the power or authority to make a decision about the creation, use or disclosure of a record.
- 3.3 “**Custody**” means the keeping, care, watch, preservation or security of a record for a legitimate business purpose. While physical possession of a record may not always be necessary to establish custody, physical possession may be an element of the evidence of custody.
- 3.4 “**De-Identification**” means to remove any information that identifies the individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other

information, to identify an individual. De-identified data is any information that identifies the individual removed.

- 3.5 “**Disclose**” means to make the information available or to release it to another person, but does not include to Use the information, and “Disclosure” has a corresponding meaning.
- 3.6 “**Education Act**” is the *Education Act*, R.S.O. 1990, c. E.2 and its regulations, as amended.
- 3.7 “**Freedom of Information Request**” or “**FOI Request**” is a request under MFIPPA or PHIPA for access to information that is in the custody or control of the DDSB.
- 3.8 “**Information Lifecycle**” refers to the various stages that Records go through, from their creation or acquisition to their final destruction or archiving. Access and privacy laws apply to records at any stage of their lifecycle. The life cycle includes creation, collection, use, maintenance, and disposition (destruction or archiving).
- 3.9 “**Information and Privacy Commissioner of Ontario**” or “**IPC**” is an independent officer of the Ontario Legislature with the powers and duties prescribed by legislation, including MFIPPA and PHIPA. The office of the IPC is an independent body tasked with upholding and promoting open government and the protection of personal privacy in Ontario. The IPC has the authority to conduct investigations, issue orders, enforce fines and review disclosure decisions.
- 3.10 “**Least Privilege**” means the principle of allowing users or applications the least number of permissions necessary to perform their intended function.
- 3.11 “**MFIPPA**” is the *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M.56 and its regulations, as amended.
- 3.12 “**Need to Know**” means the principle that the user has a legitimate reason to access something.
- 3.13 “**Personal Information**” or “**PI**” means recorded information about an identifiable individual and includes personal health information. As defined by MFIPPA this may include, but is not limited to:
- Information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual, 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,
 - Any identifying number, symbol or other particular assigned to the individual,
 - The address, telephone number, fingerprints or blood type of the individual,
 - The personal opinions or views of the individual except if they relate to another individual,
 - 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,
 - The views or opinions of another individual about the individual, and/or
 - The individual’s name if it appears with other PI relating to the individual or where the Disclosure of the name would reveal other personal information about the individual.

3.14 **“Personal Health Information”** or **“PHI”** has the meaning set out in s. 4 of PHIPA. Specifically, it is “identifying information” about an individual that:

- Relates to the physical or mental health of the individual,
- Relates to the provision of health care to the individual,
- Is a plan of service under the *Connecting Care Act, 2019, S.O. 2019, c. 5, Sched. 1*;
- Relates to payments or eligibility for health care or eligibility for coverage for health care,
- Relates to the donation of any body part or bodily substance of the individual or that is derived from the testing or examination of any such body part or bodily substance,
- Is the individual’s health number, and/or
- Identifies an individual’s substitute decision-maker.

PHI also includes identifying information about an individual that is not PHI listed above but that is contained in a record that includes PHI listed above. Information is “identifying” when it identifies an individual or when it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify the individual.

3.15 **“PHIPA”** is the *Personal Health Information Protection Act, 2004, S.O. 2004, c. 3* and its regulations, as amended.

3.16 **“Privacy Breach”** occurs when personal information is compromised; that is, when it is collected, used, disclosed, retained, or destroyed in a manner inconsistent with privacy legislation.

In the event of a privacy breach, please refer to the [Privacy Breach Protocol](#).

3.17 **“Privacy Incident”** means a real or suspected privacy breach.

3.18 **“Record”** means a record of information, including data in any form, such as a record made, recorded, transmitted or stored in paper or digital form or in other intangible form by electronic, magnetic, optical or any other means, but does not include a mechanism or system for making, sending, receiving, storing, or otherwise processing information.

3.19 **“Safeguard”** refers to measures designed to protect Personal Information regardless of media.

3.20 **“Service Provider”** means a third-party contracted or otherwise engaged to provide services to the DDSB.

3.21 **“Use”** means to view, handle, or otherwise deal with the information, but does not include to Disclose the information, and “Use”, as a noun, has a corresponding meaning.

4.0 Legal Framework

The handling of Personal Information is governed by a legal framework of laws, regulations, standards, and guidelines. MFIPPA and the Education Act are the two main laws that guide access to information and privacy in Ontario's public and separate schools. This Procedure also refers to other applicable legislation, such as PHIPA and the *Child, Youth and Family Services Act*, 2017, S.O. 2017, c. 14, Sched. 1 (the "CYFSA"). These laws also permit or require school boards to Disclose limited Personal Information about students without consent in certain situations.

These laws may be subject to modification by prevailing laws in certain cases, such as the Ontario *Human Rights Code*, R.S.O. 1990, c. H.19 and the *Canadian Charter of Rights and Freedoms*.

4.1 MFIPPA and PHIPA

MFIPPA sets out the rules that school boards and other municipal institutions must follow regarding the Collection, Use, retention, and Disclosure of PI.

PHIPA sets out the rules for Collection, Use and Disclosure of PHI, and *may* apply when students receive health care in school.

4.1.1 Protection. MFIPPA and PHIPPA require that the DDSB protect the privacy of individuals with respect to PI about themselves held by the DDSB, and to provide individuals with a right of access to their own PI. The protection of privacy includes the appropriate Collection, Use, retention, and Disclosure of PI, including the use of appropriate security measures / safeguards to protect information from unauthorized access. Please refer Section 15 of this Procedure and to DDSB procedures on information classification and handling for more information with respect to securing Personal Information.

4.1.2 Access and Correction. MFIPPA also gives individuals a right of access to DDSB records, with some exceptions. PHIPA gives individuals a right of access to their PHI held by DDSB if it engages a Health Information Custodian to collect PHI on its behalf or is deemed to be a Health Information Custodian itself. Both MFIPPA and PHIPA also give individuals the right to correct their PI or attach a statement of disagreement.

4.1.3 Consent. Student PI may require the student and/or the student's parent or guardian to consent to its Use and/or Disclosure. Where a student is under 16, their parent or guardian may exercise the student's privacy rights on the student's behalf.

4.1.4 Staff handling of PI. Staff shall only access, Use and Disclose PI within the Custody and Control of the DDSB in performance of their professional duties.

4.1.5 PI of parents. While the focus of this Procedure is on access to and privacy of student PI, it is important to note that the rights and obligations set out in MFIPPA apply to *any individual's* PI. For example, where a school Collects, Uses or Discloses information about a student's parents, it must protect the privacy of this information.

4.1.6 IPC Complaints. If an individual feels their privacy has been compromised by the DDSB, they file a privacy complaint to the IPC:

The Information and Privacy Commissioner/Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8
Telephone: (416) 326-3333 or toll free 1-800-387-0073

4.2 **The *Education Act* and the Ministry of Education *Ontario Student Record Guideline***

The Education Act is the main law under which schools and school boards operate. It governs how education is delivered to students in Ontario's publicly funded school system. The Education Act contains a number of sections relevant to access and privacy, including rules about access to and the Collection, Use and Disclosure of information contained in the Ontario Student Record (OSR).

4.2.1 These rules may be subject to modification by MFIPPA in certain cases.

4.2.2 PI is Collected in accordance with section 265(1)(d) of the Education Act, which states that information may be Collected in accordance with the Education Act, its regulations, or guidelines issued by the Minister of Education.

4.2.3 Section 266 of the Education Act provides for the establishment of the student's OSR in accordance with the [Ministry of Education 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 their duties of employment, and no such person shall communicate any such knowledge to any other person except,

- a. as may be required in the performance of their duties; or
- b. with the written consent of the parent or guardian of the student where the student is a minor; or
- c. with the written consent of the student where the student is an adult, which the age of 18 or until they graduate from a secondary school, whichever comes first.

4.2.4 Reference should be made to the DDSB Human Rights Inclusive Design and Accommodation Procedure regarding requests for accommodation with respect to the OSR process.

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

The *Ontario College of Teachers Act*, Regulation 437/97 defines the following as professional misconduct for the purposes of section 30(2) of the Act:

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 or allowed by law.

4.4 **Ethical Standards for the Teaching Profession (Ontario College of Teachers)**

The Ethical Standards for the Teaching Profession represents a vision of professional practice. The standard of respect states: "Intrinsic to the ethical standard of Respect are trust and fair-mindedness. Members honour human dignity, emotional wellness and cognitive development. In their professional practice, they model respect for spiritual and cultural values, social justice, confidentiality, freedom, democracy, and the environment."

- 4.5 Other laws, regulations, standards, and guidelines may apply to other professionals, including but not limited to regulated health professionals.

5.0 Responsibilities

- 5.1 The **Privacy Officer** is responsible for:

- 5.1.1 Overseeing the responsibilities of the DDSB's privacy program. These responsibilities include the management of Privacy Incidents, Privacy Breaches, privacy risks, privacy complaints, privacy inquiries, access and correction requests, and requests to implement consent directives.
- 5.1.2 Oversight of privacy impact assessments, privacy safeguards, privacy policies and procedures, privacy audit and compliance activities, and privacy training.
- 5.1.3 Supporting the Associate Director, Corporate Affairs with the privacy aspects of the DDSB information technology security program.
- 5.1.4 Providing the Director of Education and/or the Board of Trustees, as the Director of Education may deem appropriate, with relevant information on material privacy matters, including updates on the status of the privacy program, significant or high-risk Privacy Breaches, privacy audit reports, new privacy legislative, and regulatory and industry developments of note.

- 5.2 **Principals, Managers and Superintendents** are, within their sphere of authority, responsible for:

- 5.2.1 Implementing reasonable security measures and safeguards to protect PI.
- 5.2.2 Ensuring that staff are aware of and adequately trained in their responsibilities as set out in this Procedure, the Privacy Policy, and other supporting procedures and guidelines.
- 5.2.3 Ensuring that agreements with service providers contain, where appropriate, privacy protection provisions regarding the protection, Collection, Use, retention and Disclosure of PI.

- 5.3 **Staff** are responsible for:

- 5.3.1 Complying with the Privacy Policy, this Procedure, legislation, applicable professional standards, and DDSB procedures and agreements when using PI.
- 5.3.2 Reporting any suspected privacy breaches of which they are aware to the Privacy Officer.
- 5.3.3 Taking reasonable steps to ensure the PI within their Custody and Control is secured and protected, including following proper procedures and best practices as directed by their Manager/Principal, the Privacy Officer, and as outlined in this Procedure and DDSB information classification and handling procedures.
- 5.3.4 Participating in any mandatory DDSB training regarding their duties and obligations to protect PI.

6.0 Collection and Use of student Personal Information where consent is not required

6.1 School registration

Where student PI is Collected and Used for the provision of educational services in accordance with the Education Act for a student who has registered in the DDSB, consent of the parent/guardian/student is not ordinarily required. However, at time of Collection, individuals must be given notice of:

6.1.1 the legal authority for Collection,

6.1.2 the purpose(s) of its intended Use, and

6.1.3 the title and contact information of an individual who may respond to specific questions regarding the Collection.

6.2 Planning and delivering educational programs and services

In general, teacher(s), principal(s) and supervisory officer(s) may Collect, Use and Disclose a student's PI for the purpose of planning and delivering educational programs and services that best meet student needs.

Educational programs and services include ancillary services such as student transportation. For example, student addresses may be provided to the Durham Student Transportation Services and bus operators for the provision of home to school transportation.

Ordinarily, PI will be Collected directly from the student or parent/guardian for the purposes necessary for the creation and delivery of appropriate educational program(s) for the student or for the proper administration of any other lawfully authorized activity.

6.3 In performance of assigned duties

A student's PI may be Used by officers or employees of the DDSB who need the information, including access to a record, in the performance of their duties – i.e. student PI may be shared internally on a limited need-to-know basis. Use of PI for this purpose is in accordance with MFIPPA and the Education Act.

6.4 Annual Notice of the Collection and Use Student Personal Information

The DDSB shall publish annually a Notice of the Collection and Use Student Personal Information (**Appendix A**) which outlines student PI that is routinely Collected and Used for the provision of educational services to students. This notice statement shall be reviewed by the Privacy Officer and shall be posted on the DDSB websites and included within student handbooks. Consent to the Collection and Use of information as outlined in this notice statement is not required.

6.4.1 Parents/guardians/students are invited to communicate any concerns they may have regarding the Collection and Use of information outlined in this notice statement to their school principal. The principal may consult with their Superintendent of Education and/or the Privacy Officer in addressing concern.

7.0 Collection and Use of student Personal Information where consent is required

7.1 Use and Disclosure of student PI for a purpose other than planning and delivering educational programs and services that best meet student needs or in accordance with the specific exceptions outlined in MFIPPA and PHIPA will generally require written consent.

7.2 Purposes requiring consent including, but are not limited to:

7.2.1 Release of OSR Documents (Appendix B)

7.2.2 Collection and/or Release of Personal Information (Appendix C)

7.2.3 Photographs and Recordings (Appendix D)

7.2.4 Participation in Media or Promotional Activities (Appendix E)

7.3 Parental consent and age for student consent

The rules surrounding the age at which a person can provide consent are different under MFIPPA and the Education Act; both statutes may be subject to modification by prevailing laws in certain circumstances.

7.3.1 Under MFIPPA, an individual having lawful custody (for example, a parent or guardian) of a child under 16 years of age may provide consent on the child's behalf. The child may also provide consent. Once a student turns 16, their parent or guardian may no longer consent on their behalf.

7.3.2 Under the Education Act, the parent or guardian of a student under 18 may provide written consent for the Use or Disclosure of information from the child's OSR. Once a student is 18 or older, the student alone may provide the consent.

7.3.3 Where school boards are required to seek consent for the Use or Disclosure of PI, they should make sure that the person consenting understands what information the DDSB is seeking consent to Use or Disclose, and the purposes for the Use or Disclosure.

7.3.4 Where consent to Collect, Use or Disclose PI is required, consent shall *ordinarily* be sought from a parent/guardian for students under the age of 16 and from the parent/guardian and the student for students 16 to 17. Consent will be sought from students 18 and older unless there are reasons to believe that the student is incapable of consenting on their own behalf (**Appendix C**).

7.3.5 A student who is under 16 will generally have their privacy rights exercised by a parent or guardian, on the student's behalf without specific authorization. Where the student is 16 or 17, both the parent and the student shall consent to the Collection, Use and Disclosure of PI, except in circumstances where the student is not capable to exercise their rights.

7.3.6 Students aged 16 and 17 may withdraw from parental custody. If a student aged 16 or 17 has informed their school principal about such a withdrawal in writing the student's sole consent for the Collection, Use and Disclosure of their PI shall be sufficient authority.

7.3.7 Reference should be made to the DDSB Human Rights Inclusive Design and Accommodation Procedure regarding requests for accommodation with respect to parental consent and age for student consent.

8.0 Disclosure of student Personal Information

8.1 With Consent

If the person to whom the information relates has identified specific information and has 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 and the minor, where the minor is 16 or 17. **(Appendix C)**

8.2 Without Consent

The DDSB may Disclose PI in its custody and control, including from the OSR, without the consent of the parent/guardian/student, in the following circumstances.

8.2.1 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.

8.2.2 In Performance of Assigned Duties

PI may be made available to an officer, employee, trustee consultant or agent of the DDSB who needs the record for the performance of duties within their scope of authority and if the information is necessary and proper for the discharge of the institution's functions.

Information shall be limited to that which is necessary for the required purpose.

Under the Education Act, supervisory officers, principals, teachers and designated early childhood educators may Disclose information in the OSR to improve the instruction and other education of the student.

8.2.3 Legal Authority

PI 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. MFIPPA prevails over the confidentiality provisions in the Education Act, including those related to OSRs. This means that the DDSB may Disclose a student's PI, including the OSR, if MFIPPA permits it.

Contact your Superintendent of Education; the Superintendent of Education / Employee Relations; or the Privacy Officer with any questions related to Disclosures of this kind.

8.2.4 Law Enforcement

Personal Information (that is not the OSR) may be Disclosed to an institution or a law enforcement agency in Canada to:

- (a) aid an investigation undertaken with a view to a law enforcement proceeding, or
- (b) from which a law enforcement proceeding is likely to result.

In non-urgent situations, police shall provide a written statement that PI is required for

investigative purposes. MFIPPA does not permit ongoing or informal arrangements for the automatic Disclosure of PI to law enforcement agencies.

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

- (a) 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
- (b) through a warrant requiring the surrender of an OSR to the police.

8.2.5 Health and Safety

PI may be Disclosed in compelling circumstances affecting the health or safety of an individual, if, upon Disclosure, notification is mailed to the last known address of the individual to whom the information relates.

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.

The Superintendent of Education and Privacy Officer must be consulted.

8.2.6 Compassionate Circumstances

When there is a need to notify a close relative, friend, or spouse of a parent/guardian of a student who is injured, ill or deceased, school boards may Disclose PI without consent in order to facilitate or enable contact.

For example, if a young student is ill and the student's parent cannot be reached, the school may decide it needs to Disclose this information to someone at the parent's workplace to help make contact with the parent. The information Disclosed by the school should be limited to only that which will "facilitate contact" – in this case, it means that the school could Disclose to the parent's workplace that the child was ill and needs to be picked up, but should not Disclose the nature of the illness or other details.

9.0 Collection, Use and Disclosure of student Personal Health Information

- 9.1 The DDSB utilizes the services of and employs health professionals (e.g., speech language pathologists, psychologists, social workers) who are required to treat PHI in accordance with PHIPA and applicable professional standards.
- 9.2 The health professionals will obtain consent from the parent/guardian/student, when required, prior to providing their services.
- 9.3 The DDSB Collects PHI from health professionals with the consent of the parent/guardian/student and only as is reasonably necessary for the purpose of planning and delivering educational programs and services that best meets student needs.
 - 9.3.1 A signed consent form describing the purposed Use of the PHI is presented to the health professional authorizing the release of the record(s).
 - 9.3.2 PHI may be used for the purposes identified in the consent form and may be shared only with certain DDSB employees and/or Service Providers if it is necessary for them to perform their duties. Ordinarily, these would be DDSB employees who are working

directly with or have responsibility for the student.

- 9.4 Where a student has been diagnosed with an illness, disease or disorder that may be transmitted through bodily fluids, the DDSB's requirement that all releases of bodily fluids require the implementation of Universal Precautions will protect students and staff, without requiring the release of that student's PHI.
- 9.5 Sharing student PHI with certain DDSB employees will only be necessary in limited and specific circumstances requiring the creation of a Student Safety Plan. Consultation with their Superintendent of Education will be necessary before a Safety Plan is created and the student's PHI is shared with staff.

9.6 Student Health Card Numbers

The DDSB may receive a student's health card number to facilitate emergency care during a field trip or co-curricular activity. In all such cases, the number shall only be recorded for the trip or activity at issue. The DDSB shall not require parents/guardians/students to provide a health care number as part of the registration process or as a condition of attending school or participating in a field trip or school-related event. Health cards numbers shall not be recorded in the student information system and shall be protected from unauthorized access.

10.0 Parental and student access to Personal Information

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

10.1 Student and parental access to OSR – Informal Requests

If a student, or their parent or guardian, wants to access the student's PI, they might choose to ask for the information informally – by asking the school/school principal for a particular record.

If an informal request is not appropriate, or the OSR records are numerous and lengthy, they may choose to make a formal access request under the Education Act.

10.2 Student and parental access to OSR under the Education Act

A child of any age has the right under the Education Act to examine their OSR.

Subject to the dispute resolution mechanisms outlined in the Education Act, and until the child turns 18 (unless this right is limited by a court order or a separation agreement), all parents/legal guardians have a right to, without the child's consent, at no cost:

- 10.2.1 examine their child's OSR at the school office;
- 10.2.2 request corrections to their child's OSR;
- 10.2.3 request the removal of information from their child's OSR; and
- 10.2.4 request to pick up from the school hard copies of records from their child's OSR (electronic copies and mailed hard copies will not be provided).

Where a student of 16 or 17 has withdrawn from parental control, this right of access would likely not apply and will require assessment of the facts by the Principal, who may consult with the Privacy Officer.

10.3 Student and parental access to Personal Information under MFIPPA

A child of any age has the right to exercise their access rights under MFIPPA. This includes requesting access to general records held by the school or school board and/or to their PI.

Until a child turns 16, anyone having lawful custody of the child has a right under MFIPPA to access the child's record of PI on behalf of the child, without the child's consent being required. If the record is in the OSR, the access rights of parents/guardians extend until the child is 18.

A charge of twenty cents per page may be charged for copies of records (in accordance with MFIPPA).

Principals may consult with their Superintendent or DDSB Legal Services regarding this process.

10.4 Parents' Access

Parents with decision-making responsibility and those with parenting time 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. This right exists until the student turns 18 or is 16 or 17 and has removed themselves from parental control. Parents may access an OSR in accordance with the [Ministry of Education OSR Guidelines](#) and other applicable laws.

See Section 11.3 of this Procedure for more information on custody and access orders and agreements.

10.5 Non-OSR information

Parents with decision making responsibility and those with parenting time have a general right to information and may be provided with:

- 10.5.1 an opportunity to attend parent-teacher interviews;
- 10.5.2 report cards, school newsletters, and other similar information; and,
- 10.5.3 other information about their children customarily given to parents.

11.0 Third Party Requests for student Personal Information

11.1 Parent's Lawyer and Litigation

Information shall not be Disclosed to third parties, including a parent's lawyer, without the express consent of the parent/guardian/adult student.

A duly executed release form which clearly identifies the information requested, and includes original or electronic signatures, may be used as authority to release the information to the parent's lawyer. **See Appendix B.**

Staff shall 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. **See Appendix B.**

The ***Request for Release of OSR By Way of SIGNED CONSENT (only) CHECKLIST*** (a copy of which may be obtained from the Privacy Officer) provides additional guidance for responding to OSR requests from law firms.

Staff shall not:

- 11.1.1 provide letters supporting parenting capability or otherwise provide student information for the sole purpose of supporting a parent's litigation;
- 11.1.2 agree to participate in an interview with a parent's lawyer (see section 11.4.4 of this Procedure for requests from the Office of the Children's Lawyer);
- 11.1.3 complete testing or assessment reports that have not been reviewed by DDSB psychological services or that do not comply with established DDSB testing criteria; or
- 11.1.4 provide assessments or opinions on matters other than a student's educational progress or educational needs.

11.2 External Health and Social Service Professionals and Paraprofessionals

When schools are working with external agencies for the provision of services by regulated health professionals, regulated social service professionals and paraprofessionals, school administrators must ensure that informed consent processes are followed as outlined in the as outlined in applicable DDSB policies and procedures for collaboration with external agencies for provision of services.

11.3 Custody and Access Orders and Agreements

- 11.3.1 ***Custodial parental rights.*** Except where limited by legislation, court order, separation agreement, or other legally binding agreement, parents have a right to make inquiries and to be given information as to the health, education, and welfare of the child.
- 11.3.2 ***Parents with Parenting Time.*** A parent with parenting time has the right to make inquiries and be given information as to education including report cards and attendance records, and meeting for a parent/teacher interview. However, School Administrators should be mindful of any limitations of this right that may apply, including requests for information that extend beyond the subject of the child's education.
- 11.3.3 ***Obtaining and Validating court/legal documents.*** School Administrators shall attempt to obtain court orders and/or agreements pertaining to child custody where there exists a reasonable belief that such documents exist. School Administrators shall exercise diligence to ensure that all court orders and agreements pertaining to custody and access are current, accurate, and complete. In the absence a final sealed court order, the Principal may contact both parents to confirm the validity of any court order or agreement between the parties.
- 11.3.4 ***Compliance with orders/agreements.*** School Administrators and staff shall use best efforts to comply with any court order or agreement that *sets out the rights of the parents*. However, neither the DDSB nor the school are responsible for the enforcement of a court order or agreement, nor are they responsible for mediating any dispute between the parties to these document.
- 11.3.5 ***School Records.*** Any court order or agreement, the existence of which the school has become aware, that describes a custody and access arrangement shall be included by the school principal in the OSR.
- 11.3.6 ***Staff access to orders/agreement information.*** 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.

- 11.3.7 **DDSB Support.** School Administrators shall contact DDSB Legal Services and/or their Superintendent of Education for support with respect to any questions or concerns pertaining to the application, interpretation, and legal requirements contained within custody and access orders and agreements.

11.4 **Government Agencies or Officials**

Government agencies or officials may request student PI in the course of conducting their duties, and MFIPPA permits Disclosure for the purposes of complying with other legislation.

The following are examples of situations where it is mandatory to Disclose student PI, and where consent is not required. However, DDSB employees shall take steps to ensure the request is properly authorized and that the legal authority is valid. If uncertain, staff are to consult with their Superintendent or DDSB Legal Services.

11.4.1 **Children's Aid Society**

In accordance with the CYFSA, a children's aid society may Collect information about a student under 16 when investigating child protection cases.

The “**duty to report**” under the CYFSA states that if any person – including a teacher or principal – has reasonable grounds to suspect that a child under the age of 16 is in need of protection, they are required to immediately report the suspicion and the information on which it is based to a children's aid society. For more information on the duty to report, see the [DDSB Reporting Children and Youth in Need of Protection Procedure](#).

In accordance with ss.129(4-6) the CYFSA, outside of the duty to report, a person may also choose to report information to the society review team, which is a team each children's aid society establishes to recommend how a child can be protected. Despite the provisions of any other act, a person may Disclose information to this team even if the information is confidential or privileged. No legal action for Disclosing the information can be taken against the person unless they acted maliciously or without reasonable grounds to suspect that a child is in need of protection.

11.4.2 **Ministry of Education**

In accordance with section 8.1 of the Education Act, the Minister of Education may Collect PI, directly or indirectly, for purposes related to the following matters, and may Use it for those purposes:

- (a) Administering the Education Act and the regulations, and implementing the policies and guidelines made under the Education Act;
- (b) Ensuring compliance with the Education Act, the regulations, and the policies and guidelines made under the Education Act;
- (c) 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;
- (d) Planning or delivering extended day programs, allocating resources to them, evaluating or monitoring them or detecting, monitoring and preventing fraud or any unauthorized receipt of services or benefits related to them;

- (e) Providing for financial assistance related to extended day programs, evaluating or monitoring the provision of the assistance or detecting, monitoring and preventing fraud or any unauthorized receipt of benefits related to the assistance;
- (f) 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;
- (g) Risk management, error management or activities to improve or maintain the quality of extended day programs;
- (h) Risk management, error management or activities to improve or maintain the provision of financial assistance related to extended day programs; or
- (i) Research and statistical activities that relate to education and are conducted by or on behalf of the Ministry.

11.4.3 Local Medical Officer of Health

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

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

PI may also be required to support Mandatory Public Health Programs, e.g., communicable disease and oral health, under the *Health Protection and Promotion Act, R.S.O. 1990, c. H.7*. Staff shall comply with these requests in accordance with the DDSB [Communicable Diseases](#) procedure.

11.4.4 The Office of the Children's Lawyer

The Office of the Children's Lawyer ("OCL") is appointed by a court to act on a student's behalf as their lawyer. Upon receipt of the signed consent of the parent/guardian, the student's lawyer or their designate may examine an OSR in accordance with the Education Act, may interview staff about the child's academic progress and may interview the student at school if they request to do so.

Before participating in an interview with a lawyer, psychologist, or social worker from the OCL or providing a written assessment to the OCL, DDSB staff members shall seek input from DDSB Legal Services and/or their Superintendent.

DDSB staff members may provide the OCL with the same information that would ordinarily be provided to a parent, as outlined above, including a fair and accurate assessment of a child's educational progress or educational needs.

Teachers and administrators shall take reasonable care to ensure that all factual information conveyed is true and provides a fair, accurate and appropriate assessment of the student.

11.4.5 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 YCJA prohibit all persons, including police, youth courts and school board officials, from Disclosing the identity of a young offender.

However, 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 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.

11.4.6 Eligibility Review Officers

These officers may investigate eligibility for government payments under several acts, including the *Ontario Disability Support Program Act, 1997*, the *Ontario Works Act, 1997, S.O. 1997, c. 25, Sched. A*, and the *Family Benefits Act, R.S.O. 1990, c. F.2*.

Eligibility review officers may make a written demand to the DDSB for the production of records. If the officer makes such a demand, the school board or principal must comply and may seek guidance or assistance from DDSB Legal Services in that regard.

11.5 Media Coverage at School

Principals shall ensure that student interaction with the media is conducted in accordance with the [DDSB Handling of Media at the School Level Procedure](#), and with the following guidelines:

11.5.1 Notice

Students must receive written notice of 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. The required notice is included in the annual *Notification of the Collection and Use of Student Personal Information (Appendix A)* and may also be conveyed on the consent to participate form or sent home on a separate flyer. It may also be published in the student handbook, which is distributed at the beginning of every school year or semester to students.

Knowledge and acceptance of the possibility of media exposure at open events may be made a condition of participation in the activity.

11.5.2 Consent

Even if notice of media exposure has been given, specific consent of the parent/guardian/adult student must be obtained before a member of the media is permitted to photograph or speak to specific students for stories which are of an in-depth nature. (**Appendix D**)

Where it is not possible to get written consent of a parent in advance of a student interview, the principal may accept a verbal consent and shall note on the form that the parent has provided verbal consent.

11.5.3 **Validate media credentials.**

Principals must validate the credentials of any member of the media before inviting them onto school grounds by collecting and recording the following information:

- (a) the name and nature of the media corporation the person represents;
- (b) the topic of the feature/story (e.g., student achievement, school closures, health education);
- (c) 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, school, or individual student photo, opinion on school activity.

11.5.4 **Conduct of interviews.**

Interviews of students by the media shall be conducted under the supervision of a DDSB employee.

11.5.5 **Access denial.**

The Board may impose conditions for attendance by the media on school property. If media representatives breach such conditions, the Board may deny them access to school property, including future access.

12.0 Privacy in the networked classroom and the use of online educational services

- 12.1 The Board shall ensure that all applications are reviewed and approved prior to introduction into the classroom in accordance with the [Technology Approval Process](#).
- 12.2 The Board shall ensure that all application providers are subject to privacy protections at least as comprehensive as the Board is obliged to comply with when Collecting, Using, retaining or Disclosing PI.

13.0 Privacy Breaches

- 13.1 If staff becomes aware of a suspected or actual privacy breach, they must immediately notify their principal/supervisor to ensure that immediate action can be taken to mitigate the impact/results of the breach.
- 13.2 For information about responding to a privacy breach, contact your Superintendent and/or the Privacy Officer at foi.privacy@ddsb.ca. See [Privacy Breach Protocol Procedure 3106](#) for more information.

14.0 Ontario Education Number

- 14.1 The Ontario Education Number (OEN) is a unique number assigned to each person who is enrolled in or who seeks admission to be enrolled in a school.
- 14.2 The Education Act, section 266, 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.

- 14.3 No person shall, Collect, Use, or Disclose another person's OEN except as provided by the Education Act.

15.0 Security and Handling of Personal Information

- 15.1 Reasonable Safeguards must be applied according to the level of sensitivity throughout the Information Lifecycle. Controls can be administrative, physical and/or technical.
- 15.1.1 Administrative Safeguards examples may include: staff training; privacy and security policies procedures and standards; confidentiality agreements; and privacy impact assessments.
- 15.1.2 Physical Safeguards examples may include: controlled access to locations where PI is stored; identification, screening and supervision of visitors; door and cabinet locks; access cards and keys; paper shredders; and alarm systems.
- 15.1.3 Technical Safeguards examples may include: authentication and access controls; logging, auditing and monitoring; strong passwords, encryption, maintaining up-to-date software by applying the latest security patches; firewalls; hardened servers; intrusion detection and prevention; anti-virus; anti-spam; and/or anti-spyware software; protection against malicious and mobile code; threat risk assessments; screen savers with passwords; and access control lists.
- 15.2 PI must be released only on a Least Privilege, Need to Know basis consistent with DDSB policies and procedures.
- 15.3 Safeguards should be periodically reviewed to ensure they continue to be reasonable.
- 15.4 Many DDSB departments already have Safeguards in place for Personal Information. Such Safeguards must be reviewed to ensure they comply with the requirements in this Procedure.

Physical Information and Records

- 15.5 Records containing PI shall be always kept secure. To preserve the confidentiality, integrity and availability of Records:
- 15.5.1 Take Records containing PI off-site only when necessary and, whenever practical, the original record shall remain on-site and only copies removed. Original OSRs shall not be removed from the school unless they are being transferred to a new school and must remain at last school of attendance.
- 15.5.2 Copies of documents containing PI shall be clearly identified as such and destroyed when no longer needed. Original documents containing PI shall be destroyed in accordance with a records retention schedule approved by the Privacy Officer.
- 15.5.3 A sign-in/sign-out procedure including sign out date to monitor removed files shall be established.
- 15.5.4 Records containing PI shall be returned to a secure environment as quickly as possible, for example, at the end of a meeting or the end of the day.

- 15.6 All working copies of paper files containing PI shall be returned to the office or a secure environment for destruction. Such records shall never be discarded in an individual's office, home or a public trash or recycling bin.
- 15.7 Visitor access to areas where records containing PI is being worked on or is stored shall be controlled. Unknown persons seen in operational areas shall be questioned. (e.g., Can I help you? Are you looking for someone?)
- 15.8 Areas of the building where PI is stored shall be secured after normal business hours.
- 15.9 Keys and access to locked file cabinets and locked areas shall be controlled and monitored.

Computers, Emails and Electronic Information

- 15.10 Email messages shall not contain PI about an identifiable individual unless necessary. Where it is necessary to include such information in an email, consider using the individual's initials, symbols, or a code rather than a full name to help maintain anonymity of the individual.
- 15.11 Emails and documents containing sensitive PI shall be encrypted in transit and at rest.
- 15.12 Passwords for encrypted files must be communicated through an out-of-band method, e.g., phone, text, portal, in person, mail.
- 15.13 The following email protection options in Microsoft Outlook should be utilized according to the level of sensitivity:
 - (a) *Encrypt Only*: Encrypts the message without additional permissions.
 - (b) *Do not forward*: recipients can read the message but cannot forward, print, or copy the content. The Information Owner has full permission to their message and all replies.
 - (c) *Confidential / All Employees*: requires protection which allows all employees full permissions. Information owners can track and revoke content.
 - (d) *Highly Confidential / All Employees*: allows all employees to view, edit, and reply permissions to this content. Data owners can track and revoke content.
- 15.14 Where possible, computer monitors shall be positioned to minimize unauthorized viewing of the PI displayed on the monitors. Monitors displaying PI shall never be left unattended and password protected screen saver options shall be used during periods of inactivity. These measures shall also be taken while working remotely.
- 15.15 Computer hard drives and file storage media must be rendered unusable when disposed of.

Mobile Devices

- 15.16 Mobile devices include, but are not limited to, laptops/notebook computers, tablets, cellular phones, and removable media (flash drives, memory sticks, removable drives).
- 15.17 All mobile devices must be secured against improper access, such as password protection and/or encryption.

- 15.18 PI shall not be stored on laptop hard drives unless these hard drives are protected by encryption software. If it is necessary to store data containing PI on the hard drive of a laptop, password protect the file and maintain the anonymity of the individual by initials or codes, when and where possible. Staff are encouraged to save documents or files that contain PI to DDSB Network drives or DDSB issued cloud storage media such as OneDrive or Google drive.
- 15.19 PI may not be transmitted to any destination external to DDSB without encryption.

Verbal Communications

- 15.20 When communicating PI, consider the physical setting and try to ensure that no one overhears the conversation, i.e., hallways, main office, etc. public telephones, etc.
- 15.21 When the work environment is not conducive to privacy while collecting or communicating PI, end and reschedule the conversation or move to a more private environment.

16.0 Retention Personal Information

- 16.1 Retention of PI will be subject to legislation and the Board's records retention schedules.
- 16.2 In accordance with MFIPPA, PI that has been Used shall be retained for a minimum of one year. This includes, but not limited to information such as teacher mark records, common assessment data, Individual Education Plans, etc.

17.0 Reference Documents

17.1 DDSB Policies

[Human Rights, Anti-Discrimination and Anti-Racism Policy](#)
[Indigenous Education Policy](#)
[Privacy Policy](#)

17.2 DDSB Procedures

[Acceptable and Safe Use Procedure for Computing Technology Safety](#)

[Collaboration Agreement With External Agencies For Provision Of Services By Regulated Health Professionals, Regulated Social Service Professionals, And Paraprofessionals \(Ministry Of Education Policy/Program Memorandum #149\)](#)

[Communicable Diseases](#)

[Electronic Monitoring](#)

[Guidelines for E-Mail](#)

[Handling of Media at the School Level Procedure](#)

[Human Rights, Anti-Discrimination and Anti-Racism Procedure](#)

[Human Rights Inclusive Design and Accommodation Procedure](#)

[Human Rights Roles, Responsibilities and Accountability Framework](#)

[Privacy Breach Protocol](#)

[Reporting Children and Youth in Need of Protection Procedure](#)

[Staff Mobile Phones](#)

[Student/Family Human Rights Issue, Incident and Complaint Resolution](#)

[Technology Approval Process](#)

[Technology Approval Process \(Cloud Services\): Privacy and Security Assessment Guide](#)

[Video Surveillance System](#)

17.3 **Legislation**

[Anti-Racism Act, 2017, S.O. 2017, c. 15](#)
[Canadian Charter of Rights and Freedoms](#)
[Child, Youth and Family Services Act, 2017, S.O. 2017, c. 14, Sched. 1](#)
[Education Act, R.S.O. 1990, c. E.2](#)
[Family Benefits Act, R.S.O. 1990, c. F.2](#)
[Health Protection and Promotion Act, R.S.O. 1990, c. H.7](#)
[Human Rights Code, R.S.O. 1990, c. H.19](#)
[Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M.56](#)
[Personal Health Information Protection Act, S.O. 2004, c. 3, Sched. A](#)
[Occupational Health and Safety Act, R.S.O. 1990, c. O.1](#)
[Ontario Disability Support Program Act, 1997](#)
[Ontario Works Act, 1997, S.O. 1997, c. 25, Sched. A](#)
[Youth Criminal Justice Act \(S.C. 2002, c. 1\)](#)

17.4 **Other Documents**

Ministry of Education OSR Guideline:
<https://www.ontario.ca/page/ontario-student-record-osr-guideline>

Appendix:

Appendix A: Notification of the Collection and Use of Student Personal Information
Appendix B: Consent to the Release of OSR Documents
Appendix C: Consent to the Collection and/or Release of Personal Information
Appendix D: Photographs and Recording Consent, Waiver and Release
Appendix E: Consent to Participate in Media or Promotional Activities

Effective Date

2012-06-15

Amended

2023-09-19