Privacy and Information Management (PIM) of Personal Information

#400.13

Adopted:	June, 2023
Last Reviewed/Revised:	N/A
Responsibility:	Director of Education
Next Scheduled Review:	June, 2024

POLICY STATEMENT

The Brant Haldimand Norfolk Catholic District School Board (BHNCDSB) is committed to the protection of privacy and complies with the Education Act, the Municipal Freedom of Information and Protection of Privacy Act, (MFIPPA), the Personal Health Information Protection Act (PHIPA), the Personal Information Protection and Electronic Documents Act (PIPEDA) and any other applicable privacy legislation. It is the policy of the BHNCDSB to collect, use, retain and dispose of personal information while meeting its statutory duties and responsibilities. The BHNCDSB is committed to the protection of privacy of individuals with respect to personal information that is in its custody and/or under its control.

APPLICATION AND SCOPE

This policy applies to all Brant Haldimand Norfolk Catholic District School Board (BHNCDSB) staff who collect, use, retain, and disclose personal information related to students and BHNCDSB employees, and to operations and procedures in all facilities within the Brant Haldimand Norfolk Catholic District School Board.

All Board staff are responsible for the protection of personal, confidential, and sensitive information entrusted to them. They must ensure that personal information in their care and control is secured and protected from unauthorized access, disclosure and inadvertent destruction by adhering to safeguards appropriate to the sensitivity of the information and as described in this policy and procedure.

REFERENCES:

- Municipal Freedom of Information and Protection of Privacy Act
- Personal Health Information Protection Act
- Education Act and Regulations
- Child and Family Services Act
- Children's Law Reform Act
- Youth Criminal Just Act
- Records and Information Management 400.13
- Video Surveillance Policy and Procedure (under construction)
- Privacy Breach Protocol
- Ontario Student Record (OSR) Guideline
- Routine Use and Disclosure of Student Personal Information
- BHNCDSB Generic Records Retention Schedule
- BHNCDSB Managing Email and Records

FORMS:

- Consent for Release of Student Information Form – Adult Student (student over 18 years)
- Notice of Collection and Consent for the Use of Personal Information Consent Form
- Notice of Collection and Consent for the Use of Personal Information Consent Form - Limited.
- Disclosure of Information Form

APPENDICES:

- N/A

DEFINITIONS

Board - the Brant Haldimand Norfolk Catholic District School Board.

Confidential Record: A record containing information deemed by the Board or a third party to be of a confidential nature and requiring protection against unauthorized access or disclosure.

Confidentiality: The duty to protect records and information deemed confidential.

Express Consent: Consent given explicitly, either orally or in writing. Express consent is unequivocal and does not require any inference on the part of the organization seeking consent.

Implied Consent: Situations where consent may be reasonably inferred from the action or inaction of the individual.

Informed Consent: The requirement that the person consenting understands the exact nature of the information for which consent is sought, understands the potential consequences of signing the consent form, and is given the right to revoke the consent at any time. Students 18 or older must sign the consent form. If a student is less than 18 years of age, and has not withdrawn from parental control, the parent or guardian must provide informed consent.

Notice: The requirement to advise an individual or third party of intended use of personal or confidential information in the Board's custody and/or control.

Parent/Guardians: The biological or adoptive parent of a child, or a person other than the biological/adoptive parent who has lawful custody.

Personal Health Information: Recorded information about an individual's physical or mental condition including intellectual ability, cognitive and language skills, behaviour and emotional functioning.

Personal Health Information Custodians: Health care practitioners, including those defined under the Regulated Health Professions Act (psychologists, psychological associates, and speech-language pathologists), members of the Ontario College of Social Workers and Social Service Workers (social workers and attendance counselors), and those people "whose primary function is to provide health care for payment" (child and youth counselors, communication disorder assistants).

Personal Information: Recorded information about an identifiable individual, including but not limited to:

- Personal contact information;
- Biographical information;
- Financial information; and
- Employment information.

Examples include:

- 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 unique identifier assigned to the individual;
- The address, telephone number, fingerprints, or blood type of the individual;
- The personal opinions or view 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
- The individual's name if it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

Privacy: The rights and obligations of individuals and organizations with respect to the collection, use, disclosure and retention of personal information; however recorded, whether in printed form, on film, by electronic means or otherwise.

Record: Any record of information however recorded, whether in printed form, on file, by electronic means or otherwise and includes:

- Correspondence, a memorandum, a book, a plan, a map, a drawing, a diagram, a pictorial, or graphic work, a photograph, a film, a microfilm, a sound recording, a videotape, a machine-readable record, any other documentary material, regardless of physical form or characteristics, and any copy thereof; and
- Subject to the regulations, any record that is capable of being produced from a machinereadable record under the control of an institution by means of computer hardware and software or any other information storage equipment and technical expertise normally used by the institution (document).

Student Personal Information: 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.

ADMINISTRATIVE PROCEDURES

PRIVACY PRINCIPLES

1. **Accountability**: The Director of Education is accountable for the action taken and decisions made under MFIPPA and ensures there is oversight of and compliance with this privacy policy.
2. **Identifying Purposes**: The BHNCDSB only collects personal information when it is necessary for providing education for students and/or the employment of school board employees, or as required and authorized by law.
3. **Consent**: The BHNCDSB will seek consent, if required, for the use or disclosure of personal information and/or personal health information at the time of collection.
4. **Limiting Collection, Use Disclosure and Retention**: The BHNCDSB will only collect personal information to that which is needed for the purposes identified by the BHNCDSB as well as for fair and lawful purposes. The BHNCDSB will restrict the use of personal information for the purpose for which it was collected. Personal information will be retained for as long as required to serve those purposes as defined in the BHNCDSB's Records Retention Schedule.
5. **Accuracy**: The BHNCDSB will ensure that personal information is accurate and complete and will routinely engage stakeholders to update personal information so that it can satisfy the purposes for which it is to be used.
6. **Safeguards**: The BHNCDSB is responsible for the protection of personal information under its control and custody and is committed to employing appropriate security measures relative to the sensitivity of the information entrusted to it.
7. **Openness**: The BHNCDSB will ensure that it will make detailed information about its policies and practices relating to the management of personal information publicly and readily available through routine disclosure and active dissemination of information for general BHNCDSB information. Access to information may also be handled through the formal Freedom of Information request process.
8. **Individual Access**: An individual has the right to personal privacy with respect to records in the custody and/or control of the BHNCDSB.
9. **Challenging Compliance**: An individual can address or challenge compliance with the above principles to the Director of Education and the Office of the Information Privacy Commissioner.

REQUIREMENTS

- Personal information will not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law.
- Personal information will be disposed of when it is no longer needed in accordance with the BHNCDSB Records Retention Schedule.
- Adhere to the BHNCDSB's Privacy Principles.

RESPONSIBILITIES

Director of Education

- Ensuring there is a Privacy program that complies with the principles of the Municipal Freedom Information Protection Privacy Act.

Manager of Information Technology Services

- Ensuring IT staff follow the Security Breach Procedure and for establishing and maintaining an IT triage and escalation process.

Manager of Communications and Community Relations | Privacy Officer.

- All aspects of the BHNCDSB's Privacy program, including policy development and maintenance, training and awareness.

Administrators, Managers, Superintendents

- 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 Board policies, procedures and guidelines; and
- Ensuring that agreements with service providers contain privacy protection provisions with regard to the protection, collection, use, retention and disclosure of personal information.

Staff (including all Employees, Trustees, Volunteers and Third Parties)

- Complying with legislation, professional standards, Board 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; and
- Participating in training regarding their obligations to protect personal information.

SCHOOL VOLUNTEERS AND STUDENT PLACEMENTS

It is the responsibility of the school Administrator to ensure volunteers and those participating in a student placement are aware of the policies and procedures, and BHNCDSB expectations with respect to privacy and the management of personal information.

Volunteers and individuals participating in a placement at a school or other location where personal information may be collected and/or used are required to read and acknowledge their responsibilities for the protection of privacy and sign a confidentiality statement.

COLLECTION AND THE USE OF STUDENT PERSONAL INFORMATION

- Personal information will be collected directly from the student or his/her parent/guardian for the development and delivery of educational program and services.
- 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. The following Notice of Collection statement will be included on all Board forms requesting the personal information of a student:

  Information Collection Authorization

  Notice of Collection: The personal information you have provided on this form and any other correspondence relating to your involvement in our programs is collected by the Brant Haldimand Norfolk Catholic District School Board under the authority of the Education Act (R.S.O. 1990 c.E.2) ss. 58.5, 265 and 266 as amended and in accordance with Section 29(2) of the Municipal Freedom of Information and Protection of Privacy Act, (R.S.O. 1990 c.M.56) The information will be used to register and place the student in a school, or for a consistent purpose such as the allocation of staff and resources and to give information to employees to carry out their job duties. In addition, the 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. The information will be used in accordance with the Education Act, the regulations, and guidelines issued by the Minister of Education governing the establishment, maintenance, use,

retention, transfer and disposal of pupil records. If you have any questions, please contact the school principal and/or the Freedom of Information Officer, Brant Haldimand Norfolk Catholic District School Board, 322 Fairview Drive, Brantford, ON, N3T 5M8 (communications@bhncdsb.ca)

- 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.
- 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.
- 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.
- 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.
- A student who is 18 and over is considered an adult. The sharing of information with that individual's parent/guardian is triggered by the signing of a *Consent for Release of Student Information Form*. This provides any Parent/Guardian/Person of Authorization listed on the form access to the personal information of the Adult student. It does not, however, give the person listed decision-making capability on the Adult student's behalf. The intent of this form is to enable the school/board to provide copies of documentation and enable information to be verbally released to the listed person(s).

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.

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
2. Protection Act, 2004 and applicable professional standards. Personal health information will only be disclosed with appropriate consent.
3. 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).
4. 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.

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.

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.

With Consent
If the person to whom the information relates has identified that information 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.

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.

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:

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

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.

STUDENT EXPECTATION OF PRIVACY
In all BHNCDSB 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 (consent) of the person or persons being photographed or the principal or designate. Images/recordings taken as part of instruction or assessment share be retained and/or disposed of in accordance to the Board's Generic Records Retention Schedule (GRRS).

THIRD PARTY CONTRACTORS AND SHARING OF PERSONAL INFORMATION
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.

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.

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.

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.

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.

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.

ACCESS TO INFORMATION/COURT ORDERS
Access to OSR and non-OSR student personal information is governed as follows:

- 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;
- Access to other information not contained in the OSR is governed by MFIPPA;
- 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;
- 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;
- 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
- 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 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;
- 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.

THIRD PARTY REQUESTS FOR INFORMATION

- 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.
- 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 **will not**:

- 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;
- agree to participate in an interview with a parent's lawyer;
- complete testing or assessment reports that do not comply with established Board testing criteria; or
- provide assessments or opinions on matters other than a student's educational progress or educational needs.

RELEASE OF INFORMATION

Legal Authority
Personal information may be disclosed for the purpose of complying with legislation.

When a request is received for personal information or confidential records from the Ministry of Education, other Ministries, other Ontario school Boards/authorities, or private agencies, staff will verify the legal authority for the disclosure.

Local Medical Officer of Health
The school is authorized to provide the local medical officer of health with student information for the purposes of maintaining immunization records for the student (Ontario Regulation 645: Immunization of School Pupils Act). While information routinely is provided to health units by the Board office, the local health unit may contact an individual school should they be missing any required information.

Auditor(s)
The Board is authorized to provide records to an auditor appointed by the Board (Education Act, s. 253). If the institution does not employ the individual(s) performing the audit, an agreement stating they will abide by the privacy and records provisions of the Education Act and the Municipal Freedom of Information and Protection of Privacy Act is recommended.

At a minimum, the agreement should ensure that only personal information necessary to conduct the audit will be collected, and such information will be kept secure and not be disclosed to unauthorized persons.

Access to records does not mean the Board must forgo their policies and practices in this regard. For example, if OSRs are not shared by email by Board policy, then access to the OSR by the auditor would be by other means (i.e., an in-person visit to the school).

Personal information is to be redacted from records shared with Audit Committees.

Law Enforcement
Personal information may be shared with a law enforcement agency to aid an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result. In non-urgent matters, police shall provide a verbal or written statement that personal information is required for investigative purposes.

Video records may be released to law enforcement upon request in order to aid in an investigation. Refer to the Video Surveillance Policy and Administrative Procedure.

Health and Safety
Personal information may be disclosed in compelling circumstances affecting the health or safety of the individual. The imminence and reasonableness of the risk to health and safety must be considered and balanced with the right to privacy.

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:

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 Superintendents of Education via the Executive Assistants by calling 519-756-6505 Ext. 11237 or Ext. 11266.

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 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
- 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.

Medical Officer of Health (including public health unit staff)
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 released by the Data Services Team (not school staff). 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. Information released to public health to support these programs can be on a case-by-case basis or on a schedule (Example: released on the first of every month). Annually, each area of public health must complete a Disclosure of Information form.

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).

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.

School Photographers
All required personal information (including student full name and grade) is released by the Data Services Team (not school staff). Annually, each area of public health must complete a Disclosure of Information Form.

MEDIA AT SCHOOL
Principals are responsible for ensuring each student in their school has provided a signed copy of the Notice of Collection and Consent for the Use of Personal Information Consent Form. If a 'general' form has been signed, the Student Information System will indicate. If a Notice of Collection and Consent for the Use of Personal Information Consent Form - **Limited** has been provided to the school, staff are expected to limit student exposure including media coverage.

In the event of 'good news', administrators will decide if the media will have access to the school, staff or students. When the media is present, students should not participate if:

- They have not provided a completed Notice of Collection and Consent for the Use of Personal Information Consent Form.
- They have provided a completed Notice of Collection and Consent for the Use of Personal Information Consent Form – **Limited**.

All access to students and all interviews must be conducted under the supervision of a staff member.

Communications Services 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.

PRIVACY BREACHES
A privacy breach occurs when personal information is lost, stolen, or subject to unauthorized access or disclosure, contrary to the Education Act, PIPEDA, PHIPA or the MFIPPA. This includes the loss of computers, personal devices or media that contain personal information. In accordance with privacy legislation, individuals shall be informed when their personal information is involved in a privacy breach.

If staff becomes aware of a privacy breach, they must immediately follow the Privacy Breach Protocol 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 supervisor or the Manager of Communications and Community Relations | Privacy Officer.

ONTARIO EDUCATION NUMBER (OEN)
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; and
- on applications made by the individual for enrolment in an educational program, school or institution; on pupil assessments, tests and evaluations of the individual.

HOW THE BHNCDSB 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 BHNCDSB:

- For the purpose for which it was obtained or a consistent purpose (a purpose consistent for the reason collected);
- 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
- 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 BHNCDSB may use and disclose student personal Information:

Student Instruction, Achievement, and Well-Being

- 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.

- BHNCDSB 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.
- Students may be recorded or photographed by staff in school or during school activities as part of their educational program and for assessment purposes.
- Contact information, marks and transcripts are shared with Ontario colleges and universities to support post-secondary applications.
- 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.
- Indigenous 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. Indigenous heritage information will also be reported to the Ministry of Education and the Education Quality Accountability Office (EQAO).

Health and Safety/Transportation

- Student demographic information and **life-threatening medical conditions** will be released to the Student Transportation Services and the contracted bus companies responsible for transporting students in order to administer the Board's contracted transportation program.
- 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.
- Phone numbers will be used on emergency telephone lists. Examples include emergency contact lists to facilitate contact with parents/guardians during school excursions.
- Student information may also be shared with emergency responders or the hospital in the case of a medical emergency.
- Student information may also be shared with the local Public Health Departments., Children's Aid Society or others as required by law.
- 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.
- 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

Contracted photographers will take individual and class photos of students. These photos will be used for administrative and archival purposes, in the Student Information System, in school yearbooks and will be offered to parents/guardians for purchase. School photographers obtain their class lists directly from BHNCDSB Data Services, not the school.

Student first and last names and/or photographs may be printed in school programs (Example: commencement or graduation programs, school plays and musical productions, student awards, academic and athletic awards and plaques, honour roll, and in school yearbooks (print & digital). Public social media posts (derived from the family, other, and/or media not connected to the school) may contain student first and last names and/or photograph and may be shared (retweeted or otherwise depending on the social media platform.)

Student and staff information shared on authorized/official Board/School/Classroom social media accounts and/or websites will be deidentified as much as possible. (Examples: image only (no first name/last initial). Staff must not share the full identity and/or location of students or other staff members. Staff must seek verbal consent from other staff members before posting and must have knowledge of the level of consent of any student being featured and comply with that level. (Limited consent student are not to be featured on social media or websites.)

Student work, including student's first name and last initial (only), 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.

If the student or staff member understand that their role is public, full names and images may be shared. Examples include the school administrator, a trustee, a student trustee, a senior staff member.

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. Staff must have knowledge of the level of consent prior to the event/activity.

Parents/guardians/students over age 18 should be aware that when students participate in school events on or off school grounds, the school administrator 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 administrator.

Class Lists

- Class lists may not be posted on external doors or windows of the school where the information would be available for the general public to see. They may be posted on the interior doors/walls on the first day of school in September if applicable.
- Class lists may be given to families (first name, last initial only) for celebratory purposes such as Valentine's Day, etc.
- Class lists may not be given to external community groups/services without written consent of the parent/guardian.
- Similarly, class lists may not be provided to local MPPs/MPs.

School Memorabilia/School Reunions
Student records that were prepared for the public such as brochures, newsletters, plaques and yearbooks may be provided for display at school reunions. Personal information otherwise is protected, under MFIPPA, until 30 years after one's death.

If school Administrators are instrumentally involved with alumnae/other in planning the event, use of class lists to facilitate contacting alumni of the school is permitted by school staff. Class lists should not be copied and distributed. School reunion committees are encouraged to use social media, word of mouth, and advertisement of the event in the local newspaper.

ACCESS TO STUDENTS OR STUDENT RECORDS (In addition to the previous section.)

Parents/Guardians
Parents/guardians of students under the age of 18 may have access to records contained in the OSR, unless otherwise indicated in a separation agreement or court order that is filed with the school in the OSR.

Parents/guardians are the biological or adoptive parent of a child, or a person other than the biological/adoptive parent who has lawful custody. This includes non-custodial parents and Crown Wards. This does not include a step parent, unless the child has been formally adopted.

A person who has custody of a child has the rights and responsibilities of a parent/guardian with respect to the child. They make important decision regarding day-to-day matters including what school the child attends and courses they take.

If named in a court order, the Children's Aid Society (CAS)/Family and Children's Services (FCS) assumes the rights and privileges of any legal guardian and they are the contact for significant school matters. With CAS/FCS consent, the foster parent/group home may be provided with information and/or flagged as an emergency contact.

Non-custodial parents have access rights to the student, unless otherwise stipulated in a separation agreement or court order that is filed with the school in the OSR.

Where a student chooses to live with a family friend, the family friend does not assume the role of parent/guardian.

Where a student under age 18 chooses to live with the non-custodial parent, the custodial parent retains responsibilities for decisions regarding school registration.

Records of Students Over Age 18
Records of students age 18 years or older may be discussed and shared only with the student unless written consent has otherwise been received from the student. Care must be taken not to leave telephone messages on the home phone unless there is an emergency and the number has been given as an emergency contact by the student. Refer to the *Collection and the Use of Student Personal Information*.

Confirmation of Registration/Attendance
Requests for a letter from a parent/guardian to confirm registration and/or attendance at the school may be provided by the current school or the last school attended. The letter is to be given to the parent/guardian directly and not to a third party. A copy of the Office Index Card or attendance summary is permissible as appropriate.

Verification Requests from Parents/Guardians (Often for the Canada Revenue Agency (CRA) or other)
Parents/guardians receive requests from the CRA to verify personal information. These requests arrive in writing (paper) and a short turn-around time is issued. Most often, the CRA is seeking to verify proof of address or proof of custody. Staff must follow the steps outlined by Communication Services in respect to content, process and distribution of verification documentation.

Access to Students or Student Records by Third Parties
Schools receiving requests for student records by third parties (i.e., CAS, legal firms, insurance companies, summons to witness/subpoena, police, etc.) are to forward the request to the school administrator who will determine, with assistance from the Superintendent of Education and/or Manager of Communications | Privacy Officer, the legal right of the individual making the request and determine requirements for consent.

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 generally will require consent.

The Board will seek consent for the use or disclosure of personal information at the time of collection. In certain circumstances, however, consent for use or disclosure may be sought after the information has been collected but before it is used (i.e., when the Board wants to use information for a purpose that was not previously identified and is not consistent with such purpose).

The purposes for which consent is sought must be clear to the individual.

Written consent generally is required. Any failure to return documents seeking consent to disclose student personal information must not be considered implied consent.

Subject to legal or contractual restrictions and reasonable notice, an individual may withdraw consent at any time. In such circumstances, Board staff should inform the individual of implications, if any, of such withdrawal.

HOW THE BHNCDSB COLLECTS, USES, AND DISCLOSES STUDENT HEALTH INFORMATION

Personal Health Information Disclosed During a Guidance Appointment
A guidance counsellor or educator receiving information from a student that is of a health-related nature is not required to share information with the parent/guardian; confidentiality of the student is to be maintained. The only exceptions compelling a guidance counsellor to share information with the parent/guardian or other authority is if the student was a danger to themselves or others or if there was a suspected case of child abuse or neglect.

This does not preclude the guidance counsellor/educator from sharing information, as needed, to ensure the health and safety of the student as directed under *Disclosure Not Requiring Consent*.

Provisions of the Personal Health Information and Protection Act (PHIPA)

In addition to the privacy provisions set out by MFIPPA, the following are in accordance with PHIPA:

- Only a Health Information Custodian (HIC) or their designated agent may disclose personal health information. Written approval for disclosure must be given by the parent/guardian or student over the age of 16. There is an exception when it is necessary to contact a relative or substitute decision maker if the student is incapacitated.
- Care must be taken to ensure health information is not accessible when an OSR is requested to be viewed.
- Express consent is required for disclosure of a student's health information to non-HICs (i.e., to an employer or insurer). Consent may be implied between Health Care Custodians (HIC) for health care purposes.
- Care must be taken to ensure that student health information is not openly accessible, e.g. pinned to a bulletin Board in the main office, or the staff room where it may be read by visitors to the school. It is understood, however, that it may need to be readily available to assist in medical emergencies.
- Only life-threatening health information is to be shared with Student Transportation Services to facilitate safe transport to and from school or events. Non-life threatening health information is not to be shared.

DISCLOSURES NOT REQUIRING CONSENT
MFIPPA sets out when a Board may use or disclose personal information in its custody or control without the consent of the parent/guardian/student.

Performance of Job Duties
Staff may use and share a student's personal information for the purpose of planning and delivering educational programs and services. "Educational programs and services" include ancillary services such as student transportation. For example, student addresses may be provided to the Transportation Consortium and bus operators for the provision of home to school transportation.

Personal information may be made available to an officer, employee, volunteer, consultant or agent of the Board who needs the record for the performance of their duties and if the information is necessary and proper for the discharge of the Board's functions. Staff responsible for these records will assess what should be made available and to whom. Access should be minimized as much as possible to reduce risk of wrongful disclosure. Information may be limited to that which is necessary for the required purpose.

Consistent Purpose
Personal information may be disclosed for the purpose for which it was obtained or compiled or for a "consistent purpose".

A consistent purpose is how the individual, to whom the information relates, might reasonably expect their information to be used or disclosed. This is covered in the Notice of Collection and Use of Student Personal Information (General and Limited) and on the Board's website.

Legal Authority
Personal information may be disclosed for the purpose of complying with legislation.

When a request is received for personal information or confidential records from the Ministry of Education, other Ministries, other Ontario school Boards/authorities, or private agencies, staff will verify the legal authority for the disclosure.

EDUCATIONAL TECHNOLOGY
Students will be using educational tools in the classroom that may include; Brightspace (D2L) and other tools such as Microsoft Team chats, blogs, podcasts, video conferencing and surveys.

The BHNCDSB 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 BHNCDSB's custody. The use of these tools may result in personal information being stored on remote servers or cloud-based systems. The BHNCDSB will take all reasonable precautions to ensure that information is subject to the same standard of privacy protections whether it is on the BHNCDSB's own servers or stored on a remote or cloud-based server.

The BHNCDSB follows the guidance of the Ontario Information and Privacy Commissioner in its use of these tools and software.

REMOTE LEARNING AND/OR MEETINGS

Board staff may use Microsoft Teams or Brightspace (D2L) to provide:

- Instruction for students who are participating in remote, synchronous learning;
- Participate in remote meetings or parent/guardian events;
- Meet with other teams/staff for the purposes of executing daily tasks.

Staff will only use teaching tools that have been approved by the BHNCDSB for remote learning. Microsoft Teams and Brightspace (D2L) have been chosen because they are secure online platforms, approved by the Ministry of Education, that enable two-way live voice/video/text chat communication. These platforms have robust privacy policies as well as safety features for classroom use. Through these platforms, educators can create a secure virtual space for educators and students only, and staff can create online meeting/event spaces for invited participants.

BHNCDSB educators and district staff must receive training to use the Board approved platforms with instructional practices that respect the privacy of participants, both in the classroom setting and while participating remotely.

BHNCDSB uses the Microsoft Teams and the Brightspace (D2L) platform solely to facilitate the collection and sharing of student information for the purpose of instruction; assessment and evaluation of students who are participating remotely in the secure virtual classroom environment; and/or individuals participating in a meeting or event.

Recorded sessioins shall only be used for the purpose for which consent was provided and destroying in accordance to the Board's Records Retention System.

This type of activity is authorized under the Education Act and is in accordance with the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) s.28(2). 2

SCHOOL OR PUBLIC EVENTS

The administrator of the school has the authority to ask visitors to the school to refrain from using photo and/or video recording devices.

Where photography or video recording is permitted at extra-curricular activities or events where the public is invited or otherwise attends (i.e., field trips, school concerts, school teams), it is generally not possible for the school or Board to control the use of such recordings. This may result in photos or recordings being posted on social media sites.

It is important that when taking pictures, individuals are respectful of the privacy rights of anyone captured in their recording and to practice good digital citizenship by only posting photos involving other students with permission of the individual or their parent/guardian and of staff with verbal consent.

THIRD PARTIES

If a third party wishes to take photos or video recordings of students for their own use, consent is required. This may include, for example, a group or organization that is invited into the school/classroom, or it may be an organization/business/location that a group of students may be visiting as part of a field trip. The Parent/Guardian Consent for Release of Student Personal Information **does not provide for that consent**. Consent cannot be transferred from one organization to another. It is up to the third party to obtain written consent from families using their own forms and methods.

BEST PRACTICES FOR PROTECTING PERSONAL INFORMATION

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

- Do not release student or staff information over the phone without first identifying the caller and confirming that they are entitled to the information. This includes 'is XX at school today?' 'is XX teaching this afternoon', etc.
- Restrict access to those employees that require the records and information in the performance of their assigned duties.
- Ensure that sensitive and confidential information is not visible to the public including volunteers.
- Encourage a clean desk policy to reduce the risk of exposing confidential information to others.
- Lock doors and filing equipment when the of fice is not in use.
- Label filing cabinets, drawers, boxes, and other storage containers in a manner that maintains the anonymity of items in storage.
- Keep open filing equipment behind a counter or other physical barrier to the public.
- Locate FAX machines (if applicable) and printers in a secure area and/or retrieve sensitive documents immediately. Best practice is to assign a password to a print job that is sent to a centrally located printer.
- Ensure that secure confidentiality is maintained when transporting confidential information (e.g. student assignments or exams home for marking).
- 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)
- Know how long to retain personal information, and securely destroy it as per the BHNCDSB's Records Retention Schedule.
- Ensure confidential destruction of paper records by placing the records in one of the locked shredding boxes, shredding, or by arranging shredding services.
- Shut down programs or lock the device when leaving work area.
- Double-check the recipient in an email or Microsoft TEAMs communication.
- Position screens to prevent unauthorized viewing and do not disclose passwords.
- Notify the Human Resources Department if there is a change in an employee's employment status.
- Lost or stolen records are a Privacy Breach. Staff must follow the Privacy Breach Protocol.
- 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.

WORKING OUTSIDE THE OFFICE OR SCHOOL

- Employees are responsible to take additional care when working outside of the office or school. The following protections are to be in place when transporting or using personal and confidential information outside the worksite:
- Sensitive personal information should not be stored on mobile devices (laptop computers, USB keys, cell phones, PDAs).
- When working remotely, a secure work area should be designated as "office space." All paper and electronic records must be stored securely.
- Do not leave paper records, computers, or mobile devices containing personal information in your vehicle. If it absolutely cannot be avoided, lock them in your trunk before you start the trip, not in the parking lot of your destination or other visible location. They should never be left in open view in the vehicle.
- When making telephone calls from outside the office, staff must safeguard personal and confidential information; consider the physical setting to ensure that no one overhears a telephone conversation.
- While viewing personal information at locations outside the office, ensure that it cannot be seen by anyone else.
- Records containing personal or confidential information must never be discarded in a public or remote work location's trash/recycling bin.
- Records should not be left unattended and, where possible, should be physically locked away or secured.
- When travelling by bus, train or airplane, records in any format must be transported as carry-on luggage and not left unattended.
- Paper records and mobile devices should be discreetly and permanently marked as school Board property and indicate a method of return should they be lost or stolen.
- Minimize risks of taking documents off-site by only removing copies where practical, use a sign-in/sign-out procedure with a due-back date to monitor removed files, remove only relevant or required documents, and return records to a secure environment as quickly as possible.