Administrative Procedure 1100

PRIVACY PROTECTION AND ACCESS TO INFORMATION

Responsibility: Freedom of Information, Privacy and Records Information Management Officer

Legal References:

Child, Youth and Family Services Act
Children's Law Reform Act
Divorce Act
Education Act
Municipal Freedom of Information and Protection of Privacy Act
Ombudsman Act
Personal Health Information Protection Act
Personal Information Protection and Electronic Documents Act
Workplace Safety and Insurance Act
Youth Criminal Justice Act

Related Resources:

- Board Policy 1014 – Privacy and Access to Information
  - Administrative Procedure 1102 - FOI Request Protocol
  - Administrative Procedure 1104 - Privacy Breach Protocol
- Board Policy 1015 - Records Information Management
  - Administrative Procedure 1110 - Records Information Management
  - Administrative Procedure 1050 - Ontario Student Record
- WRDSB General Uses of Student Personal Information
- Administrative Procedure 1070 - Access of Non-custodial Parents to Pupils and to Pupil Academic Records;
- Child Custody and Access Agreements Guidelines; Parent/ Guardian Assignment to Designate a Non-guardian with Access to a Student/Student Information (Day-to-day Activities) (IS-19-NG)
- Board Policy 4007 - Approval of Research Projects
  - Administrative Procedure 4340 - Approval of Research Projects
- Board Policy 4010 - Video Surveillance
  - Administrative Procedure 3100 –Video Surveillance
- Administrative Procedure 3550 - Employee Records
- Administrative Procedure 2190 - Student Withdrawal From Parental/Guardian Control
- Administrative Procedure 1390 - Police Interview with Students
- Administrative Procedure 4060 - Board Email Protocol
- Administrative Procedure 4070 - Responsible Use Procedure for Information, Communication and Collaboration Technologies
- Ministry of Education Ontario Student Record (OSR) Guideline
- Protocol between Family and Children's Services of the Waterloo Region and Waterloo Region District School Board
- Privacy Considerations and Best Practices When Using G-Suite for Education Guidelines for Using Online Educational Tools;
- External Online Tools /Parent/Guardian Consent (IS-17-00)
- WRDSB Privacy/Records Management Website Guide
- Information/Privacy Commissioner of Ontario - A Guide to Privacy and Access to Information in Ontario Schools
- Information/Privacy Commissioner of Ontario - Planning for Success: Privacy Impact Assessment Guide
- Adult Student Status Form (IS-18-BB)
- Release of Academic Information Form (IS-99-R)
- Student Media Release Consent Form (IS-19-L)

Effective Date: August 2020

Revisions:
Reviewed:

1. Preamble

The Waterloo Region District School Board recognizes the importance of establishing and maintaining a privacy sensitive culture in its schools and administrative facilities consistent with federal and provincial legislation. 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, use, disclosure and inadvertent destruction by adhering to safeguards appropriate to the sensitivity of the information and as described in this procedure.

Index

2. Privacy Impact Assessments

Ontario school boards must meet high standards of care and trust whenever collecting, using and disclosing personal and confidential information.

A Privacy Impact Assessment (PIA) is an organizational risk management tool used to identify the potential privacy risks of new or redesigned school board programs or services. It reviews how a school board protects personal information as it is collected, used, disclosed, stored and ultimately destroyed. PIAs also help eliminate or reduce identified risks to an acceptable level.

The Ontario Information/Privacy Commissioner's Office has developed a Privacy Impact Assessment Guide and related worksheets to assist Ontario school boards with this process.

3. Privacy Breaches

A privacy breach occurs when personal information is collected, used, disclosed, lost or stolen, retained, or destroyed in a manner inconsistent with privacy legislation. Personal information can be compromised in many ways. Some breaches have relatively simple causes and are contained, while others are more systemic or complex.

Privacy breaches are often the result of human error; such as an individual's personal information sent by mistake to another individual. A breach can be more wide-scale, such as when a computer program change causes the personal information of many individuals to be compromised through inadvertent distribution.

The Privacy Breach Protocol Procedure is designed to help schools/departments contain and respond to incidents involving unauthorized disclosure of personal information. The ability to address privacy breaches on a system-wide basis is greatly improved through this standardized, consistent management approach

Refer to Administrative Procedure 1104 - Privacy Breach Protocol for information on how to manage and report a Privacy Breach.

4. Employee Personal Information (including Health Information)

The following guidelines are to be followed to protect employee privacy:

- Take precautions in storing employee information;
- Only allow access to employee records to those who require the information to carry out their job;
- Do not disclose an employee's information to anyone (other than government agencies and benefits providers) without first securing the employee's permission.

Refer to Administrative Procedure 3550 Employee Records for guidelines on the proper management of employee personal information, including health/medical records.

5. Student Personal Information (including Health Information)

5.1 Collection

Authority to Collect - School boards collect personal information about students and staff and are required to follow federal and provincial legislation regarding the collection, retention, use and disclosure of this information. Student records collected by boards fall into two broad categories:

- **OSR records** - The Ontario Student Record (OSR) is the record of a student's educational progress through the schools in Ontario. The Ministry of Education Ontario Student Record Guideline sets out the types of records that are to be contained in the OSR. It contains both personal and education-related documents such as report cards. Additional types of records may be included in OSRs over and above the types of records set out in the Guideline. The basic criteria for the inclusion of records in the OSR is that the information is "considered to be conducive to the improvement of the instruction of the student." The Ministry OSR Guideline also sets out the criteria for managing OSR access, use, maintenance, transfers, retirement, retention, storage, correction, destruction, and removal of information. WRDSB OSR best practices can be accessed via the Single Source Resource on the staff website.

- **Non-OSR records** (retained outside of the OSR) include all other types of personal information that a board/school may collect about a student including, but not limited to, permission slips for students to attend field trips, class lists, records of marks for weekly tests, photographs of students including names, and honour rolls.

  A board/school may collect personal information directly from a parent/guardian or adult student if at least one of the following circumstances apply:
  - authorized by statute, such as the *Education Act, Personal Health Information Protection Act,* etc., such as through the Student Registration Form;
  - used for the purposes of law enforcement (e.g. police who interview students on school property – Administrative Procedure 1390 - Police Interview with Students);
  - necessary to the proper administration of a lawfully authorized activity (e.g. Safe Arrival Program)
  - the parent/guardian or adult student has expressly consented to the collection and use of their personal information.

Notice of Collection: A Notice of Collection must be added to all WRDSB forms that collect personal information directly from students, parents/guardians, or employees. Refer to the staff Privacy/Records Management Guide for sample Notices of Collection.

5.2 Use with Consent

Boards/schools are allowed to use a student's personal information if one or more of these circumstances apply:

5.2.2 **The parent/guardian or student, if 18 years of age or older, has signed a consent form.**

A Student Media Release Consent form (IS-19-L) is distributed to families at the start of each school year. Consent is required when students are filmed, photographed or recorded and these images are used along with student names and the school attended, grade levels, activities related to school or board events, activities, or sports. This information may then be displayed, published or distributed for the purpose of posting on the WRDSB/school websites or social media sites. The form also includes a section to obtain consent from parents/guardians for the collection by the media of these types of student information for use on media websites, on television or radio. **NOTE: The Student Media Release Consent form does not include the sharing of student personal information with any other third party individuals or organizations.**

5.2.4 **Use by third party individuals or organizations (excluding WRDSB/schools and the media)**

- A properly authorized written request, signed by the parent/guardian/adult student, shall be received before information is released to an outside organization or individual concerning a student, or former student, of the Waterloo Region District School Board.
- Many organizations have their own standard form for the release of information. As long as the form is signed by the parent/guardian/adult student, and specifies the information to be released, the form is considered acceptable.
- In the absence of a release form from the requesting organization, a signed letter of authorization or the Release of Academic Information Form (IS-99-R) is considered acceptable. It must be signed by the parent/guardian/adult student. The letter or form should indicate which documents are authorized for release.

5.3 Use without Consent - Consistent Purpose of Education

A public notice regarding General Uses of Student Personal Information is posted on the WRDSB public website. It outlines how the board or schools will use student personal information for a number of consistent purposes or to comply with legislation. These uses do not require written consent from parents/guardians or students. Where information is shared with external organizations, the organizations are covered by privacy legislation or specific privacy agreements with the school board. It is important for parents to understand how their personal information, or that of their child, is shared within the school system, for what purpose it will be used, and who will receive the information.

Student information may also be shared for the following purposes without notifying or receiving consent from students/ parents/ guardians;

- nominating students for an award or honour
- assisting in a law enforcement investigation.

5.4 Access/Disclosure (including Requests for Student Records)

Boards/schools must keep Ontario Student Records (OSRs) confidential. The following should be considered prior to disclosing student personal information from OSR records:

- information may only be examined by educational personnel such as supervisory officers, principals and teachers of the school for the purpose of improving the instruction of students;
- students of any age may examine their OSR;
- parents/guardians and students may examine the OSR and obtain a copy of its contents.

Non-OSR student personal information records may be disclosed if one or more of the following conditions exist:

- when consent has been obtained from the individual;
- to comply with legislation;
- to assist in a law enforcement investigation;
- for compelling circumstances affecting the health and safety of an individual;
- in compassionate circumstances to facilitate contact with the next of kin or a friend of an individual who is injured, ill or deceased.

The following subsections set out guidelines regarding access to student records by various groups or individuals:

5.4.1 **By Custodial Parents/Guardians of Minors (under 18 years of age) or Adult Students -**

- Requests may be received by schools for student proof of enrolment or proof of guardianship. Parents /guardians may require records in response to matters such as being audited by the Canada Revenue Agency (CRA) for child tax credit purposes. Refer to the Single Source Resource for more information on how to create Proof of Enrolment or Proof of Guardianship letters. Letters must be printed on letterhead, signed and, where possible, a school or board seal applied.
- An Office Index Card (OIC) can be produced upon request by parents/guardians for purposes such as Canadian Citizenship applications. Where possible, a school or board seal should be applied to the OIC.
- No fees are charged for student records related to such requests.
- Schools must not create letters of opinion about a student if requested to do so by a parent/guardian, student or lawyer for use in legal proceedings. This would include electronic mail messages.

5.4.2 **By Custodial Parents/Guardians of Adult Students** - Under the Education Act, parents/guardians have a right to access their child's OSR if the student is under 18; however, students reach adult status when they are 18 years of age in accordance with the *Ontario Age of Majority and Accountability Act*. If the student is 18 or over, the board/school must follow the privacy provisions of *MFIPPA* if it wishes to disclose personal information about the student to his or her parents/guardians. The student must provide written permission by signing Adult Student Status Form IS-18-BB to permit parents/guardians to obtain school-related information about the student such as academic progress, attendance and behaviour.

5.4.2 **By Custodial Parents/Guardians of Students who have Withdrawn from Parental Control** - Once it has been substantiated that a student has withdrawn from parental/guardian control, the parent/guardian loses all right to educational information, as well as any other information to which the school/Board may have access such as the student's address or phone number. For more information, refer to Administrative Procedure 2190 - Student Withdrawal From Parental/Guardian Control.

5.4.3 **By Non-Custodial Parents/Guardians** - Under the *Children's Law Reform Act* and the *Divorce Act*, the legal right of a non-custodial parent/guardian to have access to a student includes the right to make inquiries and to be given information concerning the child's health, education, and welfare, unless otherwise stated in a Court Order. For more information, refer to Administrative Procedure 1070 - Access of Non-custodial Parents to Pupils and to Pupil Academic Records and the related Child Custody and Access Agreements: Impact on Access to Students, Student Information & Education Decision-Making Guidelines.

5.4.4 **By Family and Children's Services**

- For the purposes of Pupil Records, the *Education Act* defines a "guardian" as including "a person, society or corporation who or that has custody of a pupil". Family and Children's Services (F&CS) is the official guardian for students who are its wards. The parent/guardian access is limited to the F&CS designate, which is likely the student's social worker. Only this individual has access to the OSR and other personal information.

- Foster parents do not have access to the OSR or other personal information. Information relating to attendance and school progress may be relayed to the foster parents as considered appropriate.
- In suspected abuse cases, the court can, under the *Child, Youth and Family Services Act*, order a principal to produce the student OSR.
- For more information, refer to the Protocol between Family and Children's Services of the Waterloo Region and Waterloo Region District School Board.

5.4.5 **By School Volunteers** - School volunteers do not have access rights to the student information system, the OSR or the Office Index Card. They must respect confidentiality and hold in confidence all situations related to staff and students.

5.4.6 **By Student Transportation Services of Waterloo Region** - The Student Registration Form completed by parents/guardians or adult students when registering to attend school, or the Data Verification Form they complete each September for returning students, identifies in the Acknowledgement section signed by parents/guardians/adult students that personal student information may be provided to Student Transportation Services of Waterloo Region for the purposes of providing transportation to and from school.
Note: The acknowledgement section on the registration and data verification forms does not provide permission for students to be transported for off- campus trips. A separate, signed form must be completed for each off-campus excursion— "blanket" permissions are not allowed. Refer to Administrative Procedure 1580 - Off-Campus - Categories I, II & III and Administrative Procedure 1581 - Category III - Out of Province and Out of Country Trips.

5.4.7 **By an individual or organization regarding Students who are Residents of Women's Crisis Shelters** - Refer to the Protocol for Students who are Residents in Anselma House or Haven House or Women's Crisis Services for direction in access or disclosure of student personal information.

5.4.8 **By an Education Verification company** - It is common for employers in North America to hire the services of an education verification company. Requests for education verification for employment purposes require a signed authorization from the adult student. No student records are to be released to these companies; therefore, no fees are charged. All such requests can be directed to the WRDSB Privacy/Records Office at records@wrdsb.ca

5.4.9 **By Students for Transcripts and Diplomas** -
- There may be times when a student may leave owing money to the school for textbooks not returned or other outstanding fees. While the school may request repayment of these debts, if the student requests a copy of a transcript, the school may not withhold the issuing of the transcript for non-payment.
- Active students (currently enrolled) or who have been out of secondary school for *less than one year* receive one complimentary (no charge) copy of their transcripts and diplomas from their secondary school Guidance Department.
- Inactive students who have been out of school for *more than one year* are to request certified copies of their transcripts (no maximum) or diploma (maximum one copy) from the WRDSB Privacy/Records Office. This can be done by submitting an order online through the WRDSB website or by contacting the office at records@wrdsb.ca Transcript fees are $15.00 for the first copy and $5.00 for each additional copy on the same order. Diploma fee (maximum one copy) is $25.00.

5.4.10 **By Law Firms (excluding subpoenas)** -
- All requests must be received in writing and must be accompanied by a consent form signed by the custodial parent/guardian of the student if under 18 years of age, or by the adult student if 18 years of age or older.
- If the request is related to an incident involving a student on school property or in connection to a school activity, the request is to be sent to the WRDSB Risk Management Department. Risk Management Staff will provide the request to a representative of OSBIE (Ontario School Board Insurance Exchange) who will then

respond directly to the law firm. OSBIE may contact the school to request copies of student records related to the request.

- If the request is related to an incident that is not connected to the school or a school activity (e.g. motor vehicle incident), then the school or site (e.g. WRDSB Privacy/Records Office) that holds the OSR is responsible for responding to the request. If a school receives this type of request from a law firm and does not hold the OSR, the request should be sent to the WRDSB Privacy/Records Office for processing at records@wrdsb.ca
- If copies of the contents of an Ontario Student Record are requested directly by a lawyer for litigation or a doctor or clinic for medical purposes, a fee of 20¢ per page may be charged. These documents must be sent out by paid courier and there should also be a cost for paid courier added to the invoice.
- Schools must not create letters of opinion about a student if requested to do so by a parent/guardian, student or lawyer for use in legal proceedings. This would include electronic mail messages.

5.4.11 Subpoenas for Court or Legal Proceedings

- The *Education Act* states that pupil records cannot be used in any proceedings without the written permission of the parent or adult student. Principals must be provided with the written permission of parents or adult students to release OSR information for any provincially legislated matter. This includes cases such as motor vehicle accident claims and family law litigation. If parental permission is not obtained, the lawyers cannot require the school board to divulge the contents of the OSR.
- A judge can subpoena the principal to attend court with the OSR documents. Principals should make a photocopy (true copy) of the contents of the OSR, and initial each page. If the judge directs that the OSR be left with the court, principals should request that the copy be left with the court in place of the original OSR documents.
- The Education Act does not exclude the OSR in proceedings under the Criminal Code or any other federal statute, even if parental permission is not given. In criminal matters the police may produce a search warrant or the principal may be served with a subpoena to attend court with the documents.
- Schools should not create letters of opinion about a student if requested to do so by a parent/guardian, student or lawyer for use in legal proceedings. This would include electronic mail messages.
- Principals should advise their superintendent of any court proceedings.
- If a request for student records is received from a lawyer's office related to a student who no longer attends the school, send the request to the Privacy/Records Office at records@wrdsb.ca. The staff in that office will determine where the student is located and respond accordingly.

6. Security of Personal Information

6.1 Secure Mobile Devices

In recognition of the need to protect the privacy of students or staff or of other business information, the WRDSB requires that all mobile devices used for administrative purposes are password-protected and fully encrypted. Data encryption is the conversion of data into a form, called a cipher-text,that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood. When sensitive data is stored on a portable device (e.g. Board-issued smartphones, laptops, memory sticks/USB drives, external hard drives, etc.), data encryption is required at all times so that if the device is lost or stolen, the data contained on the device cannot be read by an unauthorized party.

6.2 Working at WRDSB Sites

All Waterloo Region employees are responsible for ensuring student and employee personal information is secured in a reasonable manner to prevent its loss or unauthorized use or disclosure. This applies to records and information in all formats (paper, computer, photos, drawings, recordings, etc.). All staff are encouraged to adopt the following strategies to ensure confidential and/or personal information is not openly accessible:

- Do not release student or employee personal information over the phone before confirming the identity of the caller.
- Use care when talking over the telephone or to others so that personal information cannot be overheard by co-workers or visitors to the school.
- Adopt a 'clean desk' model such that no personal, confidential, and sensitive information is left unsecured on your desk.
- Position your monitor so that casual observers cannot view the screen and/or add a monitor privacy screen.
- Use a password-protected screen saver; ensure it is set to turn on after 10 minutes of inactivity.
- Log off or apply a stand-by mode when leaving your desk.
- Log off or sign out of applications you are not using.
- Ensure documents containing confidential or personal information are not left at the photocopier or fax machine in an open area.
- Lock confidential information away at the end of the day.
- Files containing sensitive or confidential information sent to or from outside sources should use either an SFTP (Secure File Transfer Protocol) site or be encrypted first and then sent through a regular FTP channel.
- Secure web sites (designated by https) must be used when filling in forms containing highly sensitive personal or confidential data..

6.3 **Working Outside of 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 unencrypted mobile devices (laptop computers, USB keys, cell phones, etc.).
- When it is necessary to work from home, a secure work area should be designated as "office space." All paper and electronic records must be stored securely.
- If a personal device is used to create documents that contain sensitive or confidential information (e.g. a home computer), the document should be stored directly onto an encrypted USB key and not on the personal device, or residual files must be removed from the personal device after transfer to the encrypted USB key. Student, staff or other confidential business information which is considered sensitive or confidential must never be stored on an unencrypted device, including personally-owned devices.
- Do not leave paper records 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 to avoid being seen moving them to the trunk 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 your physical environment 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 be shredded and never discarded in trash or recycling bins, particularly bins in an employee's home or in a public area.
- 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
    - using a sign-in/sign-out procedure with a due-back date to monitor removed files
    - removing only relevant or required documents
    - returning records to a secure environment as quickly as possible.

7. Retention and Destruction of Personal Information

Records are to be maintained in accordance with the Board's Retention Schedule. This applies to paper and electronic records, including emails, photos, and video/voice recordings. When appropriate, confidential records must be disposed of securely to ensure they are permanently destroyed or erased in an irreversible manner and by a method that ensures that the records cannot be reconstructed in any way. When disposing of confidential records and information, consider if duplicate copies of the documents were made for in-office use. These also must be destroyed. Refer to Administrative Procedure 1110 - Records Information Management for more information about record destruction.

8. Videotaping, Video Conferencing, Voice Recordings and Photography

The use of videotaping and photography involves the collection, use, and potential disclosure of personal information and as such WRDSB must comply with the rules set out by *MFIPPA*.

8.1 School Video Surveillance

For information on videotaping for the purposes of safety and security, see Board Policy 4010 and Administrative Procedure 3100 on Video Surveillance.

8.2 In the Classroom

Taking photos, videos, voice recordings, and participating in video conferencing (i.e., Google Hangouts, Skype, Adobe Connect) in the classroom for the purposes of delivering an education program and/or documenting student learning is permissible. While permissible in the classroom for delivering an educational program and/or documenting student learning, there are a number of responsibilities under privacy legislation for how photos, videos, and voice recordings are collected, used, shared, and stored/retained.

8.2.1 Collecting, Using, and Sharing Student Photos, Videos, and Voice Recordings

Photographs and video/voice recordings of students are considered to be personal information; consideration must be given to whether informed consent is required to take a photo/video/voice recording and how that photo/video/voice recording may be used and shared.

Generally, WRDSB staff may take a photo or video without consent if it is for educational purposes or if it is otherwise necessary to deliver education to students. When consent is not required for taking photos/videos/voice recordings:

- Photos/videos taken and used by the teacher for instructional purposes only.
- Photos taken for student identification.

Taking photographs and video/voice recordings outside of these purposes requires informed consent. Examples of where informed consent is required include:

- Sharing photos in a newsletter or posting photos in the school;
- Posting photos, videos, and/or audio recordings to the school website or to a secure website specifically accessed by your classroom parents;
- Sending home photos or video/voice recordings of classroom activities; and
- Participating in a video conference that is recorded (refer to Section 8.2.3 below).

Refer to Section 5 (Use with Consent) of this procedure for additional information.

8.2.2 Security, Storage and Retention

- Photos, videos, and voice recordings are Board records; they must remain at the school (securely stored) or in WRDSB approved cloud-based storage location that is password protected (i.e. WRDSB-assigned login).
- WRDSB staff may not store student photos, videos, or voice recordings on personal devices.
- Destruction of photos, videos, and voice recordings must follow the Board's retention schedule and as outlined in Section 7.0 of this procedure.
- Unless otherwise specified, retention is the current school year, plus one additional year.

8.2.3 **Video Conferencing**

- Video conference sessions open a window to the classroom; therefore, staff must ensure connections are made only with trusted individuals and organizations to ensure activities are safe and appropriate for students.
- Students using video conferencing tools must at all times be appropriately supervised. Additionally, because videoconferencing technology may allow for recording of conference sessions, it is important that controls are put in place to ensure the conference is not recorded unless appropriate steps and measures have been put in place. Staff must ensure they are fully aware of any related security settings and operational features for the video conferencing tool chosen.
- If the other party involved in the video conference intends to retain photos and/or audio/video files, written permission must be received from parents of involved students. This agreement needs to be collected in written form prior to the video conference session. Refer to IS-19-VC for a sample agreement.
- Video conferencing will not be used in any way to upload, post, reproduce, or distribute information, software, or other material protected by copyright or any other intellectual property rights without first obtaining the permission of such right holder.

8.2.4 **School or Public Events**

- **The Principal 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.
- **Schools should include the following statement in school communications and on their school website**: *Our students and staff enjoy opportunities to share some of their activities with parents and the school community through teams, clubs and special events. Many of these are 'memory making' for families and as such, photographs are often taken. We ask that families exercise their discretion when taking photographs or videos at school events and consider the privacy of other students who may also be present in those pictures. We would appreciate it if families not upload images of students other than their own to the Internet (e.g. Social Media). Your cooperation is appreciated.*
- **Schools should also add the following message to the bottom of notices of events shared with families**: *Parents and students should be aware that those attending the event may take photographs or videos, which is beyond the control of the school or the Waterloo Region District School Board. Families are requested not to upload images of children other than their own to the Internet.*
- **Media:** The media, such as print, television or radio, may be invited by the Board or a school to attend an event for the purpose of reporting on newsworthy activities. Media reports may include only non-identifying photos of groups of students. Individual students will only be interviewed or otherwise identified with consent. A Student Media Release Consent Form (IS-19-L) is sent home each September to families for completion. They have the option of providing or withholding consent. Only students whose completed forms contain authorized consent may have their names, grade level, etc. shared with the media.
- **Third Parties other than Media:** Consent is also required if a third party wishes to take photos or video recordings of students for their own use, for example, a group or organization that is invited into the school/classroom, or an organization/ business/location that a group of students may be visiting as part of a field trip. The Student Media Release Consent Form (IS-19-L) does **not** provide for that consent. In these circumstances, contact the Freedom of Information, Privacy and Records Information Management Officer (privacy@wrdsb.ca) for assistance with developing a consent form specific to this purpose.

9. Use of Cloud-based Applications In the Classroom

WRDSB-owned or contracted applications/tools such as GSuite for Education have been vetted to ensure student information is safe, stored securely, and passwords and logins have been provided to limit access to information. Educators must ensure privacy and security is maintained by never sharing logins and passwords and encouraging students to do the same.

The use of non-vetted cloud-based tools in the classroom must be carefully considered and educators must understand their responsibilities under privacy legislation for how these cloud-based applications collect, use, share, and store/retain student personal information.
At minimum, the following steps must be taken: ‘

- Read and understand the Privacy Policy and Terms and Conditions of the tool/application carefully;
- Determine how student information will be depersonalized; and
- Determine if parental consent is required.

Many applications require parental consent for users under the age of 13. The Guidelines for Using Online Educational Tools provides additional information for educators and school administrators.
NOTE: This process is under review for the 2020-2021 school year.

10. Communication and the Use of Email, Instant Messaging, and Cloud-based Applications

The use of technology to support communication must carefully be considered as it pertains to student and staff personal information. There are a number of responsibilities under privacy legislation for how electronic communications such as email, instant messaging tools and cloud-based applications are used to collect, use, share, and store/retain student and/or staff personal information. Refer to Privacy Considerations and Best Practices When Using G-Suite for Education for guidelines on how to ensure personal and confidential student and staff information is protected.

10.1 Appropriate Responsible Use of Personal Information in Electronic Communications

The Board is required to ensure reasonable measures are in place to prevent unauthorized access to the records that are to be protected. It may be appropriate to include student and staff personal information in emails if the disclosure is made to an employee of the Board who needs the information in the performance of their duties and if the disclosure is necessary and proper in the Board's operations, for example, requesting an OSR transcript, forwarding an ESL assessment to a school, providing copies of applications to an interview committee.

The following protections are to be followed:

- Do not include student or staff names in the subject line of an email.
- Within the body of the email, where the student or staff member is known to the recipient, the initials should be used where there has been a previous conversation about the matter.
- Sensitive personal information should be avoided in emails/texts. When it is necessary to discuss a student or employee, staff should be encouraged to do so by telephone and confirm via email referencing, for example, "the individual we spoke of this morning".
- Emails that include personal information must be directed only to staff needing the information in the performance of their duties. Care must be taken to ensure they are not forwarded to unauthorized individuals either inside or outside the Board.
- Ensure mobile devices are password protected.
- Ensure the following confidentiality statement is included with all emails - *Confidentiality Warning: This message and any attachments are intended only for the use of the intended recipient(s) and may contain confidential or personal information that may be subject to the provisions of the Municipal Freedom of Information and Protection of Privacy Act. If you are not the intended recipient or an authorized representative of the intended recipient, you are notified that any dissemination of this communication is strictly prohibited. If you have received this communication in error, please notify the sender immediately and delete the message and any attachments.*

10.2 Electronic Record Retention

The responsibility for retention of electronic correspondence lies with the author of the record. Those who are copied on the communication are not required to retain a copy unless they respond to it or forward it on. In such cases, the normal retention period outlined below is required.
Electronic records providing evidence of a business decision, accountability, or

support for transparency must be retained for the period set out in the Board's Retention Schedule based on the record subject matter.
If the Retention Schedule does not set out a prescribed period, electronic records containing:

- general business information must be kept for one year after the matter has been completed;
- student or staff personal information must be kept for a minimum of one year unless the
- individual to whom it pertains consents to its earlier disposal.

It is not necessary to retain transitory communications once their purpose has been met. Transitory emails are records that hold no further value to the Board beyond an immediate or minor transaction, or records that may be required only for a very short time, e.g. until they are made obsolete by an updated version of the record, or by a subsequent transaction or decision.

Refer to Administrative Procedure 4000 - GSuite Communications Archiving for more information about retention of GSuite Communications, including email.

11. Third Party Service Providers

11.1 Freedom of Information and Requests for Proposals (RFPs)/Tenders

- Vendors should be advised that when submitting an RFP or Tender their name, title, and contact information will be made public on request.
- Under MFIPPA, and as a record of WRDSB, the bid prices submitted and agreed to under contract with WRDSB also will be made available through a Freedom of Information request.
- Vendors will be notified regarding requests for any other information submitted in a bid submission; information may be disclosed to a requester in whole or part unless otherwise considered exempt from disclosure under MFIPPA.

11.2 Contracts and Agreements with Third Party Service Providers

The Board maintains its responsibility for protecting personal information in accordance with privacy legislation when contracting with a third party.

Third party service providers may include commercial school photographers, school bus operators, external data warehouse services, outsourced administrative services (such as records storage and shredding), community organizations, external researchers, and external consultants.

Third party service providers who collect, use, retain, and/or disclose personal information on behalf of the Board are to do so only for specified purposes. Notice to individuals stating the purpose(s) for which the personal information is collected, used, and/or disclosed must be provided. WRDSB staff will ensure contracts and agreements completed with these third party providers, at a minimum, include the following:

- a written confidentiality statement;
- acknowledgement of and adherence to the M*unicipal Freedom of Information and Protection of Privacy Act* (or applicable privacy legislation);
- limitations for the collection, use, and disclosure of personal information;
- a description of the safeguards in place for the protection of personal information;
- a description of the third party's breach protocol including audit reviews, their commitment to containing the breach and making corrective actions, and notification to the Board of any actual or suspected breach; and a description of the retention period and disposal of personal information.