

Privacy and the Management of Personal Information

INDEX

1.	Intent	1
2.	Definitions (Note: All defined terms will be capitalized when used in this document.) ..	1
3.	Objective of Procedure	3
4.	Roles and Responsibilities	5
5.	Collection And Access/Disclosure Of Student Personal Information	4
6.	Access to Students or Student Records by Parents/Guardians	5
7.	Access to Students or Student Records by Third Parties	6
8.	Disclosures Not Requiring Consent	7
9.	Displaying, Sharing Class Lists and/or Student Work or Achievement	9
10.	Disclosure of Student Health Information	10
11.	Security of Personal Information	12
12.	Retention and Destruction of Personal Information	14
13.	Videotaping, Video Conferencing, Voice Recordings and Photography	14
14.	Use of Cloud-Based Applications in the Classroom	18
15.	Communication and the use of Email, Instant Messaging, and Cloud-Based Applications	19
16.	Third Party Service Providers	21
17.	Privacy Breaches	23
18.	Privacy Impact Assessments	23
	APPENDIX A:	24

1. Intent

- 1.1. The Board recognizes the importance of establishing and maintaining a privacy sensitive culture in its schools and administrative facilities consistent with federal and provincial legislation.

2. Definitions (Note: All defined terms will be capitalized when used in this document.)

- 2.1. **Board** - the Thames Valley District School Board (TVDSB).
- 2.2. **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.

- 2.3. **Confidentiality** - the duty to protect records and information deemed confidential.
- 2.4. **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.
- 2.5. **Implied Consent** - situations where consent may be reasonably inferred from the action or inaction of the individual.
- 2.6. **Informed Consent** - 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 If a student is less than 18 years of age, and has not withdrawn from parental control, the parent or guardian must provide informed consent.
- 2.7. **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.
- 2.8. **Parent/guardians** – the biological or adoptive parent of a child, or a person other than the biological/adoptive parent who has lawful custody.
- 2.9. **Personal Health Information** – recorded information about an individual's physical or mental condition including intellectual ability, cognitive and language skills, behaviour and emotional functioning.
- 2.10. **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).
- 2.11. **Personal Information** - recorded information about an individual that renders that individual identifiable, including: name, address, phone number; race, ethnic origin, or religious or political beliefs or associations; age, sex, sexual orientation, marital status, or family status; any identifying number or symbol; fingerprints, blood type, or

inheritable characteristics; medical history; educational, financial, criminal, or employment history; personal views or opinions, except if they are about someone else; or anyone else's opinion about that individual.

2.12. **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.

3. Objective of Procedure

3.1. 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 procedure.

4. Roles and Responsibilities

4.1. Under the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), the Board is responsible for the personal information under its care and/or control. The Director of Education, and their designate, is responsible for the development and implementation of the Board's privacy policies and procedures.

4.2. Similarly, under the Personal Health Information Protection Act (PHIPA), health information custodians are responsible for personal health information and may designate an individual as an agent to assist with compliance with privacy legislation.

4.3. **Superintendents, Principals, Managers, and Supervisors** are responsible for:

- 4.3.1. complying with legislation, professional standards, Board directives, procedures and agreements when using personal information;
- 4.3.2. implementing security measures and safeguards to protect the personal information of students and staff;
- 4.3.3. ensuring staff are aware of and adequately trained in their responsibilities as set out in this document and other Board policies, procedures and guidelines; and
- 4.3.4. ensuring agreements with service providers contain privacy protection provisions with regard to the protection, collection, use, retention and

disclosure of personal information.

4.4. Employees are responsible for:

- 4.4.1. protecting personal information by following proper procedures and leading practices as outlined in this document and as directed by their supervisor;
- 4.4.2. ensuring records containing personal information are accurate, up-to-date and complete;
- 4.4.3. reporting any suspected privacy or security breaches of which they are aware;
- 4.4.4. taking reasonable steps to ensure the personal information within their custody and/or control is secured and protected; and
- 4.4.5. participating in training regarding their duties and obligations to protect personal information.

4.5. School Volunteers and Student Placements

- 4.5.1. 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 TVDSB expectations with respect to privacy and the management of personal information.
- 4.5.2. 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.

5. Collection And Access/Disclosure Of Student Personal Information

- 5.1. In addition to the following procedures, information relevant to the collection, use, and disclosure of student personal information contained in the Ontario Student Record (OSR) may be found in the *Ontario Student Record (OSR) Guideline 2000 and TVDSB Procedures*.

5.2. Collection

- 5.2.1. The collection and use of personal information of a student registered with

the Board is limited to that which is necessary for the provision of educational services in accordance with the Education Act.

- 5.2.2. Ordinarily personal information will be collected directly from the student and/or their parent or guardian.
- 5.2.3. 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.
- 5.2.4. The following Notice of Collection statement will be included on all Board forms requesting the personal information of a student:

5.2.4.1. Notice of Collection: The personal information provided on this form and any other correspondence relating to involvement in Board programs is collected by the Thames Valley District School Board under the authority of the Education Act and Regulations (R.S.O. 1990 c.E.2) as amended and in accordance with the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA). The information will be used to register the student in a school, for the collection of applicable student/activity fees, as well as for any consistent purpose. Information is shared with employees such that they may carry out their job duties. In addition, the information may be used or disclosed to comply with legislation, for compelling circumstances affecting health and safety or discipline, as required in circumstances related to law enforcement matters, or in accordance with any other Act. For questions about this collection, contact the TVDSB Privacy Office, Thames Valley District School Board, 1250 Dundas Street, London, Ontario, N6A 5L1, Telephone: 519-452-2000, Email: privacy@tvdsb.ca .

6. Access to Students or Student Records by Parents/Guardians

- 6.1. 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.
- 6.2. 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 stepparent, unless the child has been formally adopted.

- 6.3. 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.
- 6.4. If named in a court order, the Children's Aid Society (CAS)/Family and Children's Services (FCS) assume 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.
- 6.5. 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.
- 6.6. Where a student chooses to live with a family friend, the family friend does not assume the role of parent/guardian.
- 6.7. Where a student under age 18 chooses to live with the non-custodial parent, the custodial parent retains responsibilities for decisions regarding school registration.
- 6.8. **Access to Records of Students over Age 18**
- 6.8.1. Records of students over the age of 18 may be discussed and shared only with the student unless written consent has otherwise been received from the student. This includes the student portal. 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.
- 6.9. **Confirmation of Registration/Attendance**
- 6.9.1. 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 sample letter is available in the electronic forms portal (Student Confirmation of Registration and/or Attendance). Including a copy of the Office Index Card or attendance summary is permissible as appropriate.

7. Access to Students or Student Records by Third Parties

- 7.1. Schools receiving requests for student records by third parties (i.e., CAS, legal firms,

insurance companies, summons to witness/subpoena, police, etc.) are to email the TVDSB Record Centre at records@tvdsb.ca.

- 7.2. Use and disclosure of student personal information for a purpose other than planning and delivering educational programs and services or in accordance with the specific exceptions outlined in Section 8 generally will require consent.
- 7.3. 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).
- 7.4. The purposes for which consent is sought must be clear to the individual.
- 7.5. Written consent generally is required. Any failure to return documents seeking consent to disclose student personal information must not be considered implied consent.
- 7.6. 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.

8. Disclosures Not Requiring Consent

- 8.1. 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.

8.2. Performance of Job Duties

- 8.2.1. 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.
- 8.2.2. 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.

8.3. Consistent Purpose

- 8.3.1. 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.
- 8.3.2. The Board shall maintain and publish to its website the resource: *Routine Use and Disclosure of Student Personal Information* which outlines for parents and students how their personal information is shared within the school system, for what purpose it will be used and with whom it may be shared. Consent to the collection and use of information as outlined is not required. However, parents/guardians/students are invited to communicate any concerns they may have to the school principal. Where a parent communicates a concern that does not affect the delivery of services to the student, the principal shall comply with their wishes. In all other cases, the principal shall consult the school Superintendent.

8.4. Legal Authority

- 8.4.1. Personal information may be disclosed for the purpose of complying with legislation.
- 8.4.2. 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.
- 8.4.3. **Local Medical Officer of Health**
 - 8.4.3.1. 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.

8.4.4. Auditor(s)

8.4.4.1. 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.

8.4.4.2. 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).

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

8.4.5. Law Enforcement

8.4.5.1. 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 written statement that personal information is required for investigative purposes.

8.4.6. Health and Safety

8.4.6.1. 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.

9. Displaying, Sharing Class Lists and/or Student Work or Achievement

9.1. Class Lists

9.1.1. 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, and this generally is limited to the

first day of school in September.

- 9.1.2. 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.

9.2. Student Work and Achievement

- 9.2.1. Student work may be displayed in the classroom or in the school hallways or may be shared with the public through events such as science fairs, bulletin Board displays, writing/colouring/poster contests, community events, fairs, and similar events/locations outside of the school setting.
- 9.2.2. Students' names should be printed on the back of their work when posted in public areas. The first name and last initial is appropriate for work displayed in the classroom. Grades must not be printed on the front of any work that is displayed.
- 9.2.3. Do not post, publish, or read aloud student achievement grades without consent.

9.3. School Memorabilia/School Reunions

- 9.3.1. 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.
- 9.3.2. If school Administrators are instrumentally involved with the alumnae association in planning the event, use of class lists to facilitate contacting alumni of the school is permitted by the school. 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.

10. Disclosure of Student Health Information

10.1. Personal Health Information Disclosed During a Guidance Appointment

- 10.1.1. 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.

- 10.1.2. This does not preclude the guidance counsellor/educator from sharing information, as needed, to ensure the health and safety of the student as per Section 8.4.6 of this procedure.

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

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

- 10.2.1.1. Professional Student Services employees who are regulated healthcare providers are Health Information Custodians (HIC). Only a HIC, or their designated agent, may disclose personal health information.
- 10.2.1.2. Students can consent to the collection, use and disclosure of their personal health information if they can understand the information that is relevant to deciding whether to consent, and the possible consequences of that decision.
- 10.2.1.3. If a student is deemed not to have capacity to provide consent to disclose personal health information, a substitute decision-maker provides consent for services and makes privacy decisions about the collection, use and disclosure of their information.
- 10.2.1.4. There is an exception when it is necessary to contact a relative or substitute decision maker if the student is incapacitated.
- 10.2.1.5. Care must be taken to ensure health information is not accessible when an OSR is requested to be viewed.
- 10.2.1.6. 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.
- 10.2.1.7. 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.

10.3. Provisions of the Health Care Consent Act

10.3.1. It is the responsibility of TVDSB's Professional Student Services employees to ensure that healthcare services (example: Psychological Services, Social Work, Speech-Language Pathology, Behaviour Analyst, Audiology) are delivered in manner as set out by the provisions of PHIPA, and the Health Care Consent Act (HCCA).

10.3.1.1. Under the HCCA and the Child Youth and Family Services Act, 2017, students who have the capacity to provide informed consent about counseling and treatment are permitted to do so.

10.3.1.2. Students who do not have the capacity to provide consent about counseling or treatment require decision making by substitute decision-maker.

10.3.1.3. Students can consent to receiving healthcare services if they can understand the information that is relevant to deciding whether to consent, and the possible consequences of that decision. It is the responsibility of TVDSB's Professional Student Services employee to make this determination as per the provisions under the HCCA.

10.3.1.4. If a student is deemed not to have the capacity to make their own decisions about counseling or treatment, a caregiver provides consent for services and makes privacy decisions about the collection, use and disclosure of their information.

11. Security of Personal Information

11.1. All Thames Valley employees are responsible to ensure 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.).

11.2. All staff are encouraged to adopt the following strategies to ensure confidential and/or personal information is not openly accessible:

11.2.1. Do not release student or employee personal information over the phone before confirming the identity of the caller.

11.2.2. 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.

11.2.3. Adopt a 'clean desk' model such that no personal, confidential, and sensitive information is left unsecured on your desk.

- 11.2.4. Position your monitor so that casual observers cannot view the screen and/or add a monitor privacy screen.
- 11.2.5. Use a password-protected screen saver; ensure it is set to turn on after 10 minutes of inactivity.
- 11.2.6. Log off or apply a stand-by mode when leaving your desk.
- 11.2.7. Log off or sign out of applications you are not using.
- 11.2.8. Ensure documents containing confidential or personal information are not left at a photocopier or fax machine in open area.
- 11.2.9. Lock confidential information away at the end of the day.

11.3. Working Outside of the Office or School

- 11.3.1. 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:
 - 11.3.1.1. Sensitive personal information should not be stored on mobile devices (laptop computers, USB keys, cell phones, PDAs).
 - 11.3.1.2. 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.
 - 11.3.1.3. 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, not in the parking lot of your destination or other visible location. They should never be left in open view in the vehicle.
 - 11.3.1.4. 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.
 - 11.3.1.5. While viewing personal information at locations outside the office, ensure that it cannot be seen by anyone else.
 - 11.3.1.6. Records containing personal or confidential information must never be discarded in a public or employee’s home trash/recycling bin.
 - 11.3.1.7. Records should not be left unattended and, where possible, should be physically locked away or secured.

- 11.3.1.8. When travelling by bus, train or airplane, records in any format must be transported as carry-on luggage and not left unattended.
- 11.3.1.9. 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.
- 11.3.1.10 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.

12. Retention and Destruction of Personal Information

- 12.1. 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.
- 12.2. 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.
- 12.3. Personal, confidential, and sensitive information in paper format must be destroyed by shredding or placing them in the locked shredding bins provided on-site.
- 12.4. Personal, confidential, and sensitive information stored in the memory of electronic devices that are being discarded for permanent destruction (e.g., hard drives, printers, photocopiers, fax machines, CDs, USB keys, etc.) must be deleted permanently prior to their removal from the office/workplace.
- 12.5. Refer any questions regarding the Board's records Retention Schedule to the Privacy Advisor.

13. Videotaping, Video Conferencing, Voice Recordings and Photography

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

13.2. School Video Surveillance

- 13.2.1. For information on videotaping for the purposes of safety and security, see TVDSB's Video Surveillance Policy and Procedure.

13.3. In the Classroom

- 13.3.1. 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.
- 13.3.2. 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.

13.4. Collecting, Using, and Sharing Student Photos, Videos, and Voice Recordings

- 13.4.1. 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.
- 13.4.2. Generally, TVDSB 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 the student.
- 13.4.3. When consent is not required for taking photos/videos/voice recordings:
 - 13.4.3.1. Photos/videos taken and used by the teacher for instructional purposes only.
 - 13.4.3.2. Photos taken for student identification.
- 13.4.4. Taking photographs and video/voice recordings outside of these purposes requires informed consent. Examples of where you require informed consent include:
 - 13.4.4.1. Sharing photos in a newsletter or posting photos in the school;
 - 13.4.4.2. Posting photos, videos, and/or audio recordings to the school website or to a secure website specifically accessed by your classroom parents;

13.4.4.3. Sending home photos or video/voice recordings of classroom activities; and

13.4.4.4. Participating in a video conference that is recorded.

13.5. Security, Storage and Retention

13.5.1. Photos, videos, and voice recordings are Board records; they must remain at the school (securely stored) or in TVDSB approved cloud-based storage location that is password protected (i.e., GOTVDSB).

13.5.2. Care for the security of technology is required (see Section 11). TVDSB staff may not store student photos, videos, or voice recordings on personal devices.

13.5.3. Destruction of photos, videos, and voice recordings must follow the Board's retention schedule and as outlined in Section 12. Unless otherwise specified, retention is the current school year, plus one additional year.

13.6. Video Conferencing

13.6.1. 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. The use of headsets by students is not permitted as it does not allow for adequate teacher assistance or supervision.

13.6.2. 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.

13.6.3. Unless written permission has been received from parents of involved students, teaching staff using video conferencing tools in their classroom must notify the other party that no pictures or voice/video recordings of the students who are participating in the video conference are permitted. This agreement needs to be collected in written form prior to the video conference

session. A sample agreement is provided in Appendix A.

13.6.4. Staff will notify their administration when engaging in video conferencing experiences with students (e.g., Google Hangouts).

13.6.5. 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 right without first obtaining the permission of such right holder.

13.7. Video Conferencing Recordings

13.7.1. Video conferencing sessions shall not be recorded in any way or in any medium without the written permission of all individuals involved and the awareness of the school Principal. Recorded information shall only be used for the purpose for which consent was provided.

13.7.2. Where TVDSB students are recorded in a video conference session, refer to Section 8.2.2 of this procedure for information on the security, storage, and retention of video conferencing recordings.

13.7.3. Further, and as per the retention schedule, the school must maintain the following:

13.7.3.1. A record of the informed consents received from students/parents;

13.7.3.2. The written agreement clearly stating how the recording will be used; and

13.7.3.3. A video conferencing session log to record when the session took place, who organized it, and who was involved, including their contact information.

13.8. School or Public Events

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

13.8.2. 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.

13.8.3. 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.

13.9. Media

13.9.1. 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. The *Parent/Guardian Consent for Release of Student Personal Information* may provide that consent.

13.10. Third Parties

13.10.1. 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* regarding release of student personal information, completed in the Parent Portal, does not provide for that consent.

13.10.2. The Privacy Office will assist with the development of required consents as needed and upon request.

14. Use of Cloud-Based Applications in the Classroom

14.1. TVDSB-owned or contracted applications/tools such as G Suite 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.

14.2. Educators must ensure privacy and security is maintained by never sharing logins and passwords and encouraging students to do the same.

14.3. 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:

14.3.1. Read and understand the Terms and Conditions of the tool/application carefully;

14.3.2. Determine how student information will be depersonalized; and

14.3.3. Determine if parental consent is required. Many applications require parental consent for users under the age of 13.

14.4. The *Approved Software and Websites* SharePoint page provides additional information for educators and school administrators.

15. Communication and the Use of Email, Instant Messaging, and Cloud-Based Applications

15.1. The use of technology to support communication must carefully be considered as it pertains to student and staff personal information.

15.2. 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.

15.3. Appropriate Use of Personal Information in Electronic Communications

15.3.1. The Board is required to ensure reasonable measures are in place to prevent unauthorized access to the records that are to be protected.

15.3.2. 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:

15.3.2.1. Password-protect documents containing personal, sensitive information.

15.3.2.2. Do not include student or staff names in the subject line of an email.

- 15.3.2.3. 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.
- 15.3.2.4. 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".
- 15.3.3. 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.
- 15.3.4. Ensure mobile devices are password protected.
- 15.3.5. Ensure the following confidentiality statement is included with all emails:
 - 15.3.5.1. **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 section 28 (2). In certain situations, it will be the practice of the Board to share personal or confidential information with board employees as a means of addressing any questions or concerns. If you do not consent to the sharing of this information, please notify the intended recipient immediately. 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. If you have any questions about the collection of information, please contact privacy@tvdsb.ca.

15.4. Appropriate Use of Cloud-Based Technologies

- 15.4.1. From time-to-time and in limited circumstances it may be appropriate to use approved cloud-based technologies (i.e., GOTVDSB) to communicate personal student and staff information for the purposes of ensuring a small group of identifiable TVDSB staff, in the performance of their duties, have access to the information they require. The following protections must be followed:

15.4.1.1. Only Board-approved apps may be used (i.e., GOTVDSB is approved).

15.4.1.2. No student or staff names may be used; non-identifying personal identifiers may be used (i.e., initials).

15.4.1.3. An administrator must be assigned to the shared record. It is their responsibility to ensure the appropriate security access rights have been put in place, and to ensure records are retained and then destroyed as per the Retention Schedule.

15.4.1.4. Records about students may be accessible under a Freedom of Information request; as such they must be producible.

15.5. Record Retention

15.5.1. 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.

15.5.2. As an electronic record 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 subject matter. Should there not be an established retention period, correspondence must be retained for one year after the matter has been completed. Where there is student or staff personal information contained in the correspondence, the correspondence must be kept for a minimum of one year unless the individual to whom it pertains consents to its earlier disposal.

15.5.3. 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.

15.5.4. See *Email Privacy Safeguards*, located on the Privacy Office SharePoint page, for additional information.

16. Third Party Service Providers

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

16.1.1. Vendors should be advised that when submitting an RFP or Tender their

name, title, and contact information will be made public on request.

- 16.1.2. Under MFIPPA, and as a record of TVDSB, the bid prices submitted and agreed to under contract with TVDSB 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 requestor in whole or part unless otherwise considered exempt from disclosure under MFIPPA.

16.2. Contracts and Agreements with Third Party Service Providers

- 16.2.1. The Board maintains its responsibility for protecting personal information in accordance with privacy legislation when contracting with a third party.
- 16.2.2. 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. TVDSB staff will ensure contracts and agreements completed with these third party providers, at minimum, include the following:
 - 16.2.2.1. a written confidentiality statement;
 - 16.2.2.2. acknowledgement of and adherence to the Municipal Freedom of Information and Protection of Privacy Act (or applicable privacy legislation);
 - 16.2.2.3. limitations for the collection, use, and disclosure of personal information;
 - 16.2.2.4. a description of the safeguards in place for the protection of personal information;
 - 16.2.2.5. a description of their 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
 - 16.2.2.6. a description of the retention period and disposal of personal information.
- 16.2.3. 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.

17. Privacy Breaches

- 17.1. A privacy breach occurs when personal information is collected, used, disclosed, lost or stolen, retained, or destroyed in a manner inconsistent with privacy legislation.
- 17.2. 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.
- 17.3. 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.

18. Privacy Impact Assessments

- 18.1. Staff responsible for developing, implementing, and/or managing projects are to complete a Privacy Impact Assessment (PIA). The assessment will identify and mitigate any privacy-related concerns and the actual or potential risks that a proposed or existing project, technology, document or program may have on the use of an individual's personal information. Conducting a PIA at the design stage will ensure that personal information is managed safely, securely and responsibly, and ensure compliance with privacy legislation to potentially avoid a privacy breach. Its purpose is to ensure that appropriate operational practices are applied throughout the information life cycle of records containing personal information collected by the users.

18.2. Completing the Privacy Impact Assessment

- 18.2.1. Forms are available through the Privacy Office. The staff lead for the initiative is responsible to complete the form in consultation with the Privacy Office and other key informants such as ITS.
- 18.2.2. Copies of the completed forms shall be submitted to the Privacy Office and maintained as per the retention schedule.

APPENDIX A:

Video Conferencing in the Classroom: Agreement with Video Conference Participants

Agreement Template 1: No Recording

It is understood that the Thames Valley District School Board (the “Board”) has arranged to conduct a video conference to facilitate instruction and student learning.

In order to ensure the Board protects the privacy interests of our students, it is agreed that neither party will record the video conference session (in either video or photo format).

Agreement Template 2: Recording (Video or Photo format)

It is understood that the Thames Valley District School Board (the “Board”) has arranged to conduct a video conference to facilitate instruction and student learning.

In order to ensure the Board protects the privacy interests of our students, it is agreed that (check applicable box):

- ☐ Only the Board will record the video conference session.
- ☐ Only the external party will record the video conference, subject to restrictions in this agreement set out below.
- ☐ Both parties will record the video conference session, subject to restrictions set out below.

Restrictions on Recording

Where either party has authorization from the other to record the video conference as set out above, use and disclosure of the record will be restricted as follows:

- Recordings will only be used for instructional purposes by each party.
- No copies of recordings will be permitted without express written consent of the other party.
- Images or other information from recordings will not be published or disseminated in any manner, including electronically or in print, without express written consent of the other party.
- Recording will be maintained in a secure manner so as to prevent theft or unauthorized access, use, or disclosure.
- Upon request by the other party, any recording will be destroyed.
- Each party will notify the other of any unauthorized access, theft, use, or disclosure.

As a condition of participating in the video conference, the parties agree to comply with the terms set out in this agreement.