Keewatin Patricia DISTRICT SCHOOL BOARD	Procedure Section: **School Administration** Procedure Name: **Privacy and Information Management**	**300** **318**

PROCEDURE

Privacy and Information Management

Created: May 14, 2019

Respectfully submitted by:
Richard Findlay, Director of Business

Keewatin-Patricia District School Board (KPDSB) recognizes the importance of establishing and maintaining a privacy-sensitive culture in its schools and administrative facilities consistent with federal and provincial legislation.

KPDSB 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 by adhering to safeguards appropriate to the sensitivity of the information and as described in this procedure.

Index

Cross References
The Education Act
Human Resources Manual
MFIPPA: The Municipal Freedom of Information and Protection of Privacy Act
PHIPA: The Personal Health Information Protection Act
PIPEDA: The Personal Information and Protection of Electronic Documents Act
Policies
314, Video Security Surveillance in Schools
318, Privacy and Information Management
Procedure
314, Video Security Surveillance in Schools

Date Adopted: 14/05/2019

Review by: 2020

1. Accountability and Responsibility

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

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.

a) Superintendents, Principals, Managers, and Supervisors are responsible for:

- Complying with legislation, professional standards, Board directives, procedures, and agreements when using personal information;
- Implementing security measures and safeguards to protect the personal information of students and staff;
- 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
- Ensuring agreements with service providers contain privacy protection provisions with regard to the protection, collection, use, retention, and disclosure of personal information.

b) Employees are responsible for:

- Protecting personal information by following proper procedures and leading practices as outlined in this document and as directed by their supervisor;
- Ensuring records containing personal information are accurate, up-to-date, and complete;
- Reporting any suspected privacy or security breaches of which they are aware to the Superintendent of Business;
- Taking reasonable steps to ensure the personal information within their custody and/or control is secured and protected; and
- Participating in training regarding their duties and obligations to protect personal information.

2. Collection and Access/Disclosure of Student Personal Information

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 OSR Ministry Guidelines and KPDSB procedures.

a) Collection

The collection and use of personal information of a student registered with KPDSB is limited to that which is necessary for the provision of educational services in accordance with the Education Act.

Ordinarily, personal information will be collected directly from the student and/or their parent or guardian.

At the time of collection, individuals must be given notice of the legal authority for the 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.

b) Access to Students or Student Records by Parent(s)/Guardian(s)

Parent(s)/Guardian(s) of students under the age of eighteen (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.

Parent(s)/Guardian(s) are the biological or adoptive parent(s) 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.

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 decisions regarding day-to-day matters, including what school the child attends and the courses they take.

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

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

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

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

i) Records of Students over the age of eighteen (18)
Records of students over the age of eighteen (18) may be discussed and shared only with the student unless written consent has otherwise been received from the student. Care must be taken not to leave telephone messages on the home phone unless there is an emergency, and the number has been given as an emergency contact by the student.

ii) Confirmation of Registration/Attendance
Requests for a letter from a parent/guardian to confirm registration and/or attendance at the school may be provided by the current school or the last school attended. The letter is to be given to the parent/guardian directly and not to a third party.

c) Access to Students or Student Records by Third Parties

Schools receiving requests for student records by third parties (i.e., CAS, legal firms, insurance companies, summons to witness/subpoena, police, etc.) are to contact the school Superintendent, who will determine the legal right of the individual making the request and determine requirements for consent.

Use and disclosure of student personal information for a purpose other than planning and delivering educational programs and services, or in accordance with the specific exceptions outlined in *Section 2.d*, will require consent.

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

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

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

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

d) Disclosure Not Requiring Consent

MFIPPA sets out when a Board may use or disclose personal information in its custody or control without the consent of the parent/guardian/student.

i) Performance of Job Duties
Staff may use and share a student(s)' personal information for the purpose of planning and delivering educational programs and services. This includes

ancillary services such as student transportation. For example, student addresses may be provided to the Transportation Consortium and bus operators for the provision of home-to-school transportation.
Personal information may be made available to an officer, employee, volunteer, consultant, or agent of KPDSB 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 the risk of wrongful disclosure. Information may be limited to that which is necessary for the required purpose.

ii) Consistent Purpose

Personal information may be disclosed for the purpose for which it was obtained or compiled or for a 'consistent purpose'. A consistent purpose is how the individual, to whom the information relates, might reasonably expect their information to be used or disclosed.

iii) Legal Authority

Personal information may be disclosed for the purpose of complying with legislation.
When to 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.

iv) Law Enforcement

Personal information may be shared with the law enforcement agency to aid in 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, the police shall provide a written statement that personal information is required for investigative purposes.

v) Health and Safety

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

e) Displaying/Sharing Student Work/Achievement

i) Student Work and Achievement

Student work may be displayed in the classroom, 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.
Do not post, publish, or read aloud soon achievement grades without consent.

ii) School Memorabilia/School Reunions

Student records that were prepared for the public such as brochures, newsletters, plaques, and yearbooks may be provided for display at school reunions. Personal information otherwise is protected, under M FIPPA, until thirty (30) years after one's death.

If school administrators are instrumentally involved with the alumni association in planning the event, the use of class lists to facilitate contacting alumni of the school is permitted by the school. Class lists should not be copied and distributed.

3. Disclosure of Student Health Information

a) Personal Health information Disclosed During a Guidance Appointment

A guidance counsellor, or educator, receiving information from a student that is of a health-related nature is not required to share information with the parent(s)/guardian(s); confidentiality of the student is to be maintained. The only exceptions compelling a guidance counsellor, or educator, to share information with the parent(s)/guardians(s), or other authority, are if the student is a danger to themselves or others, or if there is a suspected case of child abuse or neglect.

This does not preclude the guidance counsellor/educator from sharing information as needed to ensure the health and safety of the student as per *Section 2.d)v* of this procedure.

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

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

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

4. Security of Personal Information

All KPDSB 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.).

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/or 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 ten (10) minutes of inactivity;
- Log off or apply 'lock' 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 a photocopier or fax machine in an open area; and
- Lock confidential information away at the end of the day.

a) 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:

i) Sensitive personal information should not be stored on mobile devices (i.e., laptop computers, USB Keys, cell phones, etc.) if they are unencrypted or non-password protected.

ii) 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.

iii) 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.

iv) 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.

v) While viewing personal information at locations outside of the office, ensure that it cannot be seen by anyone else.

vi) Records containing personal or confidential information must never be discarded in a public or employee's home trash/recycling bin.

vii) Records should not be left unattended and, where possible, should be physically locked away or secured.

viii) When traveling by bus, train, or airplane, records in any format must be transported as carry-on luggage and not left unattended.

ix) 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.

5. Retention and Destruction of Personal Information

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.

Personal, confidential, and sensitive information in paper format must be destroyed by shredding or replacing them in the locked shredding bins provided on-site.

Personal, confidential, and sensitive information stored in the memory of electronic devices that are being discarded for permanent destruction (i.e., hard drives, printers, photocopiers, fax machines. CDs, USB keys, etc.) must be deleted permanently prior to their removal from the office/workplace.

6. 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 KPDSB must comply with the rules set out by the MFIPPA.

a) School Video Surveillance

For information on videotaping for the purposes of safety and security, see the Board's policy and procedure on Video Security Surveillance in Schools.

b) In the Classroom

Taking photos, videos, voice recordings, and participating in video conferencing (i.e., Google Hangouts, Skype, Adobe Connect, etc.) 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 several responsibilities under privacy legislation for how photos, videos, and voice recordings are collected, used, shared, and stored/retained.

i) 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, KPDSB 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.

Consent is not required for taking photos/videos/voice recordings when:

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

Taking photographs and video/voice recordings outside of these purposes requires informed consent.

Examples of where you require informed consent 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; or
- Sending home photos or video/voice recordings of classroom activities.

ii) Security, Storage, and Retention

Photos, videos, and voice recordings are KPDSB records; they must remain at the school (securely stored) or in KPDSB approved cloud-based storage location that is password protection.

Care for the security of technology is required (*see Section 4*). KPDSB staff may not store student photos, videos, or voice recordings on personal devices.

iii) 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 always be appropriately supervised.

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

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.

c) School or Public Events

The Principal, or Designate, 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, etc.), it is generally not possible for the school or KPDSB 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.

d) Media

The media, such as print, television, or radio, may be invited by KPDSB 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 'Consent to Release Personal Information' may provide that consent.

e) Third Parties

If a third party wishes to take photos or video recordings of students for their own use, consent is required. This may include, for example, a group or organization that is invited into the school/classroom, or it may be an organization/business/location that a group of students may be visiting as part of a field trip. The 'Consent to Release Personal Information' does not provide for that consent.

7. Use of Cloud-Based Applications in the Classroom

KPDSB 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.

Educators must ensure privacy and security are 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 Terms and Conditions of the tool/application carefully;
- Determine how student information will be depersonalized; and
- Determine if parental consent is required. May applications require parental consent for users under the age of thirteen (13).

8. 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 several 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.

a) Appropriate Use of Personal Information in Electronic Communications

KPDSB 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 KPDSB who needs the information in the performance of their duties (i.e., requesting an OSR transcript, or providing copies of applications to an interview committee, etc.).

The following protections are to be followed:

- Password-protect documents containing personal/sensitive information;
- 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 KPDSB; and
- Ensure mobile devices are password protected.

b) Appropriate Use of Cloud-Based Technologies

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

- Only KPDSB approved applications may be used; and
- Records about students may be accessible under a Freedom of Information request; as such they must be producible.

c) Record Retention

The responsibility for the 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 or forward it on.

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 (i.e., until they are made obsolete by an updated version of the record, or by a subsequent transaction or decision).

9. Third Party Service Providers

a) 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 the MFIPPA, and as a record of KPDSB, information other than the vendor's name and the bid price submitted and agreed to under contract with KPDSB also will be made available through a Freedom of Information request. Vendors will be notified regarding requests for any other information submitted in a big submission; information may be disclosed to a requestor in whole or part unless otherwise considered exempt from disclosure under the MFIPPA.

b) Contracts and Agreements with Third Party Service Providers

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

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

i) A written confidentiality statement;
ii) Acknowledgement of and adherence to the MFIPPA (or applicable privacy legislation);
iii) Limitations for the collection, use, and disclosure of personal information;
iv) A description of the safeguards in place for the protection of personal information;
v) 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
vi) A description of the retention period and disposal of personal information.

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.