Procedure Title	**Privacy and Information Management**		
Date of Issue	April 6, 2005	**Related Policy**	BP 1408-D
Revision Dates	April 28, 2021; May 26, 2021; January 19, 2022	**Related Forms**	AF 6801; AF 6810
Review Date		**Originator**	Administrative Council
References			
Education Act; Municipal Freedom of Information and Protection of Privacy Act; Personal Health Information Protection Act; Children's Law Reform Act; Divorce Act; Combined - MOE OSR Guidelines, 2000 and BWDSB AP 6701-D Ontario Student Record Nov. 7, 2018; Bluewater District School Board Classification and Retention Schedule; AP 1409-D "Privacy Breach Protocol"; AP 1410-D "Employee Personal and Medical Information – Collection and Use"			

1.0 RATIONALE

1.1 Bluewater District School Board recognizes the importance of establishing and maintaining a culture of privacy that is consistent with relevant federal and provincial legislation.

1.2 All board staff, trustees, and volunteers are responsible for the protection of personal, confidential, and/or sensitive information entrusted to them, or that they are exposed to within their duties. 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 the procedures and best practices as outlined in this procedure, and other board policies and procedures as necessary.

2.0 PRIVACY BREACH

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

2.2 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 widescale, such as when a computer program change causes the personal information of many individuals to be compromised through inadvertent distribution.

2.3 Administrative procedure AP 1409-D "Privacy Breach Protocol" is designed to help schools/departments contain and respond to incidents involving unauthorized disclosure of personal information.

3.0 PRIVACY IMPACT ASSESSMENTS

3.1 Staff responsible for developing, implementing, and/or managing projects that will involve personal/confidential information 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 will 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.

*If the project will involve software/apps, the staff responsible must contact the Information Communications Technology department to complete the Vetting Applications for Security and Privacy (VASP) process.

3.2 Completing the Privacy Impact Assessment
Forms are available through Corporate Services. The staff lead for the initiative is responsible for completing the forms and may need to consult with the freedom of information and protection of privacy coordinator and the ICT Department when doing so.

Copies of the completed forms shall be submitted to the freedom of information and protection of privacy coordinator and maintained as per the board's retention schedule.

4.0 EMPLOYEE PERSONAL INFORMATION (INCLUDING HEALTH INFORMATION)

4.1 Please refer to administrative procedure AP 1410-D "Employee Personal and Medical Information – Collection and Use" for expectations regarding the proper management of employee personal information, including employee files and health/medical records.

5.0 STUDENT PERSONAL INFORMATION (INCLUDING HEALTH INFORMATION)

5.1 Collection

5.1.1 **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 school boards fall into two broad categories:

i) OSR Records
The Ontario Student Record (OSR) is the confidential record of a student's educational progress through the schools in Ontario. The board's 'Combined - MOE OSR Guidelines, 2000 and BWDSB AP 6701-D Ontario Student Record' document 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 board's 'Combined - MOE OSR Guidelines, 2000 and BWDSB AP 6701-D Ontario Student Record Nov 7, 2018' document also sets out the criteria for managing OSR access, use, maintenance, transfers, retirement, retention, storage, correction, destruction, and removal of information.

ii) Non-OSR Records (retained outside of the OSR)
Non-OSR records 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 tests, photographs of students including names, and honour rolls.

5.1.2 **Notice of Collection**
Anytime that personal information is collected directly from students, parent(s)/guardian(s), or employees, notice of collection must be given and must include:

a. The legal authority for the collection;
b. the primary purpose(s) for which the personal information is intended to be used; and
c. the title, business address, and telephone number of a person employed by the institution who can answer questions about the collection.

Corporate Services will add a notice of collection to formally approved administrative forms where personal information is collected.

5.2 Use with Consent

Bluewater District School Board can use a student's personal information if one or more of these circumstances apply:

5.2.1 The Parent/Guardian or Adult Student (18 years of age or older) has Signed a Consent Form

The board uses a variety of administrative forms to obtain informed consent with regards to the use of student personal information. For example, each school year, administrative form AF 6810 "Annual Notification and Consent for the Use of Student Personal Information" is distributed to families (or with any new registration package throughout the school year), and obtains consent to use a student's name, image, and/or video or voice recording in school/classroom activities.

5.2.2 Use by Third Party Individuals

A properly authorized written request, signed by the parent(s)/guardian(s)/adult student, is required before information regarding a student, or former student, of the board can be released third party individuals.

The written request/form must be specific to the information that is being requested.

5.3 Use without Consent

5.3.1 Performance of Job Duties

Staff may use and share student's personal information for the purpose of planning and delivering educational programs and services, which includes services provided by the Student Transportation Service Consortium of Grey-Bruce.

Student personal information may be made available to a board staff member who requires 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 information being provided will assess what information should be made available and to whom. Information shared should be limited to what is necessary for the required purpose.

5.3.2 Consistent Purpose

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

Bluewater District School Board will use student personal information for a variety of purposes consistent with the board's requirements for the planning and delivery of educational programs and/or to comply with legislation. These uses do not require additional written consent from parent(s)/guardian(s) and/or the adult student. Administrative form AF 6810 provides notification to families each year regarding what may be considered routine use of personal information by the school/board.

5.4 Access/Disclosure

5.4.1 Ontario Student Records (OSRs) must be kept confidential. The following will be considered prior to disclosing student personal information from an OSR (please refer to Bluewater District School Board's OSR Guidelines for additional information):

i. Information may only be examined by educational personnel such as teachers of the student, the principal of the school, and/or supervisory officers for the purpose of improving instruction of the student.
ii. A student, of any age, may examine their OSR.

iii. Parent(s)/guardian(s) (those with lawful custody) or an adult student may examine the OSR, and obtain a copy of its contents, unless otherwise indicated in a court order/separation agreement that is filed with the school (in the OSR documentation folder).

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

i. When consent has been obtained from the individual;
ii. To comply with legislation;
iii. To assist in an official law enforcement investigation (limited applicability – please consult with area superintendent of education);
iv. In compelling circumstances affecting the health and safety of an individual (limited applicability – please consult with area superintendent of education);

5.4.3 Records/personal information of students over 18 years old may only be discussed/shared with the student, unless written consent has otherwise been received from the student.

5.4.4 If a student, aged 16-17, has officially withdrawn from parental control using AF 6208, the parent/guardian loses all rights to educational information, as well as any other information that the school board may have (e.g., student's phone number).

5.4.5 Under the Children's Law Reform Act and the Divorce Act, unless otherwise stipulated by a parenting order, the non-decision-making parent has the legal right to make inquiries and to be given information concerning their child's health, education, and welfare.

5.4.6 Schools must not create letters/emails of opinion about a student if requested to do so by a parent/guardian, adult student, or lawyer for use in legal proceedings. Administrators may contact the superintendent of education responsible for human resources services for further information.

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

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

i. Only a health information custodian (HIC), or their designated agent, may disclose student personal health information. Written approval for disclosure between a HIC and non-HIC must be given by the parent/guardian, or student over the age of 16. If disclosure is between HICs for health care purposes, consent may be implied.
ii. Care must be taken to ensure health information is not accessible when an OSR is viewed.
iii. Care must be taken to ensure that student health information is not openly accessible (e.g., pinned to a bulletin board that 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.

6.0 RETENTION AND DESTRUCTION OF STUDENT PERSONAL INFORMATION

6.1 Student records are to be retained in accordance with the board's Classification and Retention Schedule, in coordination with the board's internal 'Combined - MOE OSR Guidelines, 2000 and BWDSB AP 6701-D Ontario Student Record' document.

6.2 Record retention requirements apply to paper and electronic records. Bluewater District School Board does not employ an electronic records management system, therefore record retention beyond short-term should be paper based. Email is not considered an electronic records management/filing system.

6.3 Records containing student personal information must always be disposed of securely to ensure that they are permanently destroyed or erased in an irreversible manner and by a method that ensures that the record(s) cannot be reconstructed in any way.

7.0 VIDEOTAPING, VIDEO CONFERENCING, VOICE RECORDINGS, AND PHOTOGRAPHY

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

7.1.1 School Video Surveillance

Information regarding school video surveillance can be found in administrative procedure AP 6815-D "Video Surveillance".

7.1.2 In the Classroom – Collecting, Using, and Sharing Student Photos, Videos, and Voice Recordings

i. Taking photos, videos, voice recordings, and participating in unrecorded video conferencing via Microsoft Teams within the classroom for the purposes of delivering an education program and/or documenting student learning is permissible. While permissible though, there are numerous responsibilities required by privacy legislation for how photos, videos, and voice recordings can be collected, used, shared, and stored/retained. Photographs and video/voice recordings of students are considered personal information; therefore, consideration should always be given to whether informed consent is required to take a photo/voice/video recording and how that recording may be used.

ii. Administrative form AF 6810 "Annual Notification and Consent for the Use of Student Personal Information" is distributed to families (or with any new registration package throughout the school year), and obtains consent to use a student's name, image, and/or video or voice recording in school/classroom activities. Use beyond that described on this form, or as described as routine use, will require additional consent using AF 6801 "Event Specific: Consent for Photographs, Video Recordings, Interviews, Sound Recordings and Work Samples for Training, Classroom Resources and Public Relations Purposes".

7.1.3 Security, Storage, and Retention

i. Photographs, videos, and voice recordings are board records; they must remain at the school (securely stored) or on a BWDSB password protected network drive location (not on one's computer desktop).
ii. Bluewater staff must not store student photos, videos, or voice recordings on personal devices.
iii. Destruction of photos, videos, and voice recordings must follow the board's classification and retention schedule (as indicated in Section 6 of this procedure).
    a. Unless otherwise specified, retention is current school year.

7.1.4 School or Public Events

i. 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), it is generally not possible for school or the board to control the use of such recordings, which may result in photos or recordings being posted on social media sites (see AF 6810 "Annual Notification and Consent for the Use of Student Personal Information"). It is important, that when taking pictures/recordings, individuals are respectful of the privacy rights of anyone captured in their recording, and practice good digital citizenship by only posting photos involving other students with permission of the individual or their parent/guardian.

ii. Schools should 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 Bluewater District*

School Board. Families are requested not to upload images of student other than their own to the Internet (e.g., social media sites). Your cooperation is appreciated.

8.0 COMMUNICATION AND USE OF EMAIL, FAX, INSTANT MESSAGING, AND CLOUD-BASED

8.1 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 regarding how electronic communications, such as email, fax, and cloud-based applications, are used to collect, use, share, and store/retain student and/or staff personal information.

8.1.1 **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 (e.g., providing copies of applications to an interview committee).

8.1.2 The following protections are to be followed:

i. Do not include student or staff names in the subject line of an email.
ii. Within the body of the email, where the student or staff member is known to the recipient, avoid using identifying information (e.g., name, initials) where possible.
iii. 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 (in a private location) and may confirm via email referencing, for example, "the individual we spoke of this morning".
iv. 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.
v. Emails addresses/fax numbers should be confirmed prior to sending any personal information.
vi. Ensure mobile devices are password protected and those passwords are not auto saved.
vii. If sending information via fax, a standard fax cover sheet should be used (AF 2305) that identifies the sender and the receiver and indicate that the fax is only intended for the individual to which it is addressed. The sender should confirm transmission by printing a Fax Confirmation Report, if available.

8.1.3 **Electronic Correspondence (Email) Retention**

i. 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.

ii. 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 Classification and Retention Schedule based on the record subject matter. The board’s email system is not considered to be an electronic records management system, therefore care should be taken to ensure records are retained in an alternate format, when required.

iii. If the Classification and Retention Schedule does not set out a prescribed period, electronic records containing:
    a. general business information must be kept for one year after the matter has been completed;
    b. 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.

iv. 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.

9.0 SECURITY OF STUDENT AND/OR EMPLOYEE INFORMATION - BEST PRACTICES

9.1 All Bluewater District School Board employees are responsible for ensuring that student and employee information is secured in a reasonable manner to prevent its loss or unauthorized use of disclosure. This applies to records and information in all formats (paper, computer, photos, drawings, recordings, etc.).

9.1.1 Employees are encouraged to adopt the following best practices to ensure confidential and/or personal information is not openly accessible. This list should not be considered exhaustive.

i. Do not release student or employee personal information over the phone before confirming the identity of the caller and confirming that they would have access to the information.
ii. Use care when talking over the telephone or to others so that personal information cannot be overheard by co-workers.
iii. Adopt a 'clean desk' model such that no personal, confidential, and sensitive information is left unsecured on your desk.
iv. Position your monitor so that casual observers cannot view the screen and/or add a monitor privacy screen.
v. Use a password-protected screen saver; ensure it is set to turn on after 10 minutes of inactivity.
vi. Log off or apply a stand-by mode when leaving or desk.
vii. Log off or sign out of applications you are not using.
viii. Ensure documents containing confidential or personal information are not left at a photocopier or fax machine in open area.
ix. Lock confidential information away at the end of the day or when not in use.

9.1.2 Employees are responsible for taking additional care when working outside of the office or school. The following are provided as examples of best practices, that should be implemented when transporting or using personal/ confidential information outside of the worksite.

i. Sensitive personal information should not be stored on unencrypted mobile devices (laptop computers, USB keys, cell phones, etc.).
ii. Only connect to a password-protected wireless network that only allows access to trusted devices.
iii. 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.
iv. Records should not be left unattended and, where possible, should be physically locked away or secured.
v. Personal devices (e.g., home computer) should not be used to create and/or store documents that contain sensitive or confidential information. If a personal device is used to create documents that contain sensitive or confidential information, 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.
vi. 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.
vii. When travelling by bus, train, or airplane records in any format must be transported as carry-on luggage and not left unattended.

viii. When making telephone calls or participating in video conferences from outside the office, staff must safeguard personal and confidential information. Consider your physical environment to ensure that no one overhears a telephone conversation.
ix. While viewing personal information at locations outside the office, ensure that it cannot be
x. seen by anyone else.
xi. Avoid printing documents with personal or confidential information, where possible.
xii. 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. Documents that would normally be shredded should be retained until these can be returned to school board facilities for secure destruction.
xiii. Minimize risks of taking documents off-site by:
    a. only removing copies where practical;
    b. using a sign-in/sign-out procedure with a due-back date to monitor removed files;
    c. removing only relevant or required documents;
    d. returning records to a secure environment as quickly as possible.

10.0 FREEDOM OF INFORMATION (FOI) REQUESTS

10.1 The MFIPPA sets out requirements for municipal government institutions (which includes school boards) to follow, in order to provide a right of access and a right of correction to recorded information under their custody or control, and to protect personal information about individuals held by those institutions.

10.2 There are two types of freedom of information (FOI) requests made under the MFIPPA:
i. for general information held by the institution
ii. for personal information about an individual, held by the institution.

10.3 Prior to a request for general information being processed it should be determined if the information can be provided informally. Staff may release general information that does not identify individuals in accordance with the MFIPPA (e.g., the number of students in your school). Other requests for access to information received by staff shall be referred to the appropriate manager/supervisor and then to the board's freedom of information and privacy coordinator.

10.4 Requestors will be asked to complete a request form (available through the www.ipc.on.ca website) and submit the required $5 application processing fee to the attention of the freedom of information and privacy coordinator.

10.5 The freedom of information and privacy coordinator will receive, review, and process each request in accordance with the requirements of current privacy legislation. The freedom of information and privacy coordinator may need to work with the requestor to define the scope of the information that they are requesting. The freedom of information and privacy coordinator may also request the assistance of other board staff in order to obtain the required records. Staff receiving such a request shall comply fully and quickly to satisfy the request.

10.6 It is the responsibility of the freedom of information and privacy coordinator to review each document collected during the search for responsive records and determine if an exemption (mandatory or discretionary) to full or partial disclosure can be made under the appropriate legislation.

10.7 Requests for information from an Ontario Student Record may be processed in accordance with the 'Combined - MOE OSR Guidelines, 2000 and BWDSB AP 6701-D Ontario Student Record' and would not be considered as an FOI Request.

10.8 In response to a FOI request, or other request for information with legal implications, it may be necessary to place documents on 'legal hold/litigation hold' until the request is resolved. A 'legal hold' would require staff to not delete electronically stored information or discard paper documents that may be relevant to the new or imminent request/legal case.

Once a request for information has been made, the legal hold also extends to any future correspondence about the information/request. Upon resolution of the request for information/legal proceedings, staff will be informed that the legal hold may be removed. Following that, record retention in accordance with the board's Classification and Retention Schedule would apply.