AVON MAITLAND DISTRICT SCHOOL BOARD
ADMINISTRATIVE PROCEDURE
NO. 103

SUBJECT: MANAGEMENT OF PERSONAL INFORMATION - STUDENT

Legal References: *Municipal Freedom of Information and Protection of Privacy Act, Personal Health Information Act, Education Act, Ontario Student Record (OSR) Guideline 2000*

Related References: *Administrative Procedure 140 Computers: Acceptable Use and Security; AP 194 Privacy Breach Protocol; FOI and Protection of Privacy AP 195; AP 370 Ontario Student Record*

1.0 Purpose

This Administrative Procedure was created to provide staff with guidelines for the use and management of students' personal information.

2.0 Definitions

2.1 "Personal information" refers to information about an identifiable or potentially identifiable individual and includes, but is not limited to, personal health information and opinions about the individual.

2.2 "Personal health information" is information about an individual that pertains to health care, including information about an individual's physical or mental health, receipt of health care services and health number.

2.3 "Privacy" is the right or interest of an individual to control collection, use and disclosure of their personal information. Privacy is a legislated right and school boards are required to comply with provincial privacy laws.

2.4 "Confidentiality" is a duty imposed on an organization or individual by laws or professional and ethical standards to restrict access to or disclosure of certain information, which may include personal and/or business information.

2.5 Security/Control" refers to measures designed to protect personal information regardless of media.

3.0 Legal Framework

Personal information is legislated by a legal framework of laws, regulations and standards.

3.1 Privacy Laws

3.1.1 The protection of privacy in Ontario school boards is legislated by the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) and the *Personal Health Information Protection Act, 2005* (PHIPPA). These laws require that the Board protect the privacy of individuals with respect to personal information about themselves held by institutions and to provide

individuals with a right of access to their own personal information. The protection of privacy includes the appropriate collection, use, retention and disclosure of personal information, including the use of appropriate security measures to protect information from unauthorized access.

3.1.2 If an individual feels his or her privacy has been compromised by a government organization governed by the Act, (i.e. a school board), he or she may complain to the Ontario Government's Provincial Information and Privacy Commissioner who will investigate the complaint.

3.1.3 Both MFIPPA and PHIPA also give individuals the right to correct their personal information or attach a statement of disagreement.

3.1.4 Information about a student is "personal information" and may require the student and/or the student's parent or guardian to consent to its use and/or disclosure.

3.1.5 Staff shall only access, use and disclose personal information within the custody and control of the Board in performance of their professional duties.

3.2 Education Act

3.2.1 The Education Act sets out the authority of a school board to collect and use personal information of students for the provision of educational services to students. Personal information is collected in accordance with section 265(1)(d) of the Education Act, which states that information may be collected in accordance with the Act, Regulations or Guidelines issued by the Minister. Additionally, section 266 of the Education Act provides for the establishment of the student's Ontario Student Record (OSR) in accordance with the OSR Guideline and Board AP 370

3.2.2 Section 266 of the Education Act requires that every person shall preserve secrecy in respect of the content of an OSR that comes to the person's knowledge in the course of his or her duties or employment, and no such person shall communicate any such knowledge to any other person except, (a) as may be required in the performance of his or her duties; or (b) with the written consent of the parent or guardian of the student where the student is a minor; or (c) with the written consent of the student where the student is an adult.

4.0 Responsibilities

4.1 Principals/Managers and Superintendents are responsible for:

a) implementing reasonable security measures and safeguards to protect student personal information;
b) ensuring that staff are aware of and adequately trained in their responsibilities as set out in this document and other Board procedures and guidelines;
c) ensuring that agreements with service providers contain privacy protection provisions with regard to the protection, collection, use, retention and disclosure of personal information.

4.2 Staff are responsible for:

a) complying with legislation, professional standards, Board directives, procedures and agreements when using personal information;
b) protecting personal information by following proper procedures and best practices as outlined in this document and as directed by the Manager/Supervisor/Principal;
c) reporting any suspected privacy or security breaches of which they are aware as outlined in Privacy Breach Protocol AP 194;

d) taking reasonable steps to ensure the personal information within their custody and control is secured and protected;
e) participating in training regarding their duties and obligations to protect personal information.

5.0 Collection and Use of Student Personal Information

5.1 Where student personal information is collected and used for the provision of educational services in accordance with the Education Act for a student who has registered in the Board, consent of the parent/guardian/student is not ordinarily required. However at time of collection individuals must be given notice of the legal authority for collection, the purpose(s) of its intended use and the title and contact information of an individual who may respond to specific questions regarding the collection. The Manager of Information Services can assist with the development of specific notice of collection statements. A sample collection notice is provided below.

> *Information is collected under the authority of the Education Act for Educational Service Purposes and will be used for the purpose identified above. If you have any questions about the collection of personal information please contact the Principal of the School.*

5.2 In general, teacher(s), principal(s) and supervisory officer(s) may collect, use and disclose a student's personal information for the purpose of planning and delivering educational programs and services that best meet student needs. However individuals should be notified annually of that consistent use of their personal information. Schools shall distribute annually a Notice of the Collection and Use of Student Personal Information which outlines student personal information that is routinely collected and used for the provision of educational services to students. New students registering throughout the school year should also be provided with the notification letter. **(Form 103A 103B Notification of Disclosure of Personal Information Elementary and Secondary).** The Director's Office will distribute specific directions through Memorandum each September. Consent to the collection and use of information as outlined in the aforementioned notice is not required; however parents/guardians/students are invited to communicate any concerns they may have to the school principal.

5.3 Where consent to collect, use or disclose personal information is required, consent shall ordinarily be sought from a parent or guardian for students under the age of 18. Consent will be sought from students 18 and older unless there are reasons to believe that the student is incapable of consenting on his or her own behalf.
Website, social media use and emerging technologies are found on the "Form 103C Confirmation of Emergency Contact and Personal Information Form" The schools should ensure the Confirmation of Emergency and Personal Information Form is collected every September for all students and the responses entered into Maplewood as per Administrative Procedure 197 - Student Information Standardization. Instructions for printing this form from Maplewood will be posted to the Secretaries conference in First Class every September.

5.4 Activities in a classroom related to teaching and learning strategies may be recorded from time to time in an effort to share effective teaching and learning practices. These recordings may include identification of individual students, teachers and/or the school. The recordings may be shared with other schools in our district, other boards, the Ministry of Education and/or posted on the internet (i.e., AMDSB website). Written consent for this activity should be captured on Form 103D.

5.5 Use and disclosure of other student personal information for a purpose other than planning and delivering educational programs and services that best meet student needs or in accordance with the specific exceptions outlined in MFIPPA and PHIPA will generally require written consent. The Manager of Information Services can assist schools with the creation of specific consents of use and disclosure of student's personal information.

5.6 A student's personal information may be used by officers or employees of the Board who need the information, including access to a record, in the performance of his or her duties – i.e. student personal information may be shared internally on a limited need-to-know basis. Use of personal information for this purpose is in accordance with MFIPPA and the Education Act.

6.0 Collection, Use and Disclosure of Personal Health Information

6.1 The Board utilizes the services of and employs health professionals (e.g. speech language pathologists, psychologists, social workers) who are required to treat personal health information in accordance with the Personal Health Information Protection Act, 2004 and applicable professional standards. Personal health information should only be disclosed with appropriate consent.

6.2 The Board collects personal health information from health professionals with the consent of the parent/guardian/student and only as is reasonably necessary for the purpose of planning and delivering educational programs and services that best meet student needs. A signed consent form describing the purposed use of the personal health information is presented to the health professional authorizing the release of the record(s).

6.3 Personal health information received by Board staff may be used for the purposes identified in the consent form and may be shared only with staff members if it is necessary for them to perform their duties – i.e. ordinarily to staff members who are working directly with or have responsibility for the student.

6.4 Sharing the personal health information of the student with staff will only be necessary in limited and specific circumstances requiring the creation of a Medical Management Plan as outlined in AP 314 Medically-At-Risk Students.

6.5 The Board may ask for a student's health card number to facilitate emergency care during field trips and co-curricular activities, but will not require parents or students to provide a health card number as a condition of attending school or participating in a field trip or school-related event. Health card numbers shall not be recorded in the student information system and shall be protected from unauthorized access.

6.6 Law Enforcement
Personal information may be disclosed to an institution or a law enforcement agency in Canada to aid an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result. Examples include police, the Ministry of Community and Social Services Eligibility Review Officers. In non-urgent situations, police shall provide a written statement that personal information is required for investigative purposes.

The contents of the OSR may be made available to the police in the following circumstances:

a) with the written permission of the parent or guardian of the student or, where the student is an adult, with the written permission of the student;
b) through a warrant requiring the surrender of an OSR to the police.

Schools should refer to AP 357 Code of Conduct and AP 357 Violence Free Schools for the specific processes for the disclosure of personal information through the Threat Risk Assessment and Police/School Protocol.

6.7 Third Party Requests

6.7.1 Information shall not be disclosed to third parties, including the student's lawyer, without the written consent of the parent/guardian/adult student and signatures shall be original. A duly executed release form which clearly identifies the information requested may be used as authority to release the information.

6.7.2 Staff shall take reasonable care to authenticate the request, which may include contacting the parent/guardian/adult student or requesting identification or credentials.

6.7.3 Consent forms for access to OSR records shall be retained in the OSR in accordance with AP 370.

7.0 Ontario Education Number

7.1 The Ontario Education Number (OEN) is a unique number assigned to each person who is enrolled in or who seeks admission to be enrolled in a school.

7.2 The Education Act allows for the OEN to be collected, used, or disclosed for purposes such as the provision of educational services and for purposes related to education administration, funding, planning, research and for providing financial assistance to students.

7.3 No person shall, collect, use, or disclose another person's OEN except as provided by the Education Act.

8.0 Security of Personal Information

8.1 Workplace Security

8.1.1 Paper and electronic files containing personal/sensitive information shall be kept secure at all times. For example, when transporting records, laptops, CDs, etc. care shall be taken to keep them secure.

8.1.2 All working copies of paper files containing personal information shall be returned to the office or a secure environment for destruction. Records containing personal or confidential information shall never be discarded in an individual's or a public trash or recycling bin.

8.1.3 Areas of the building where personal information is stored shall be secured after normal business hours.

8.1.4 Keys and access to locked file cabinets and locked areas shall be controlled and monitored.

8.1.5 When discussing a student, staff shall ensure that the conversations are professional, appropriate and respectful of the audience.

8.2 Computers and Electronic Information

8.2.1 Email messages whenever possible should not contain sensitive personal information about an identifiable individual unless absolutely necessary. Where it is necessary to include such information in an email, consider using the individual's initials, symbols or a code rather than a full name to help maintain anonymity of the individual.

8.2.2 Where possible computer monitors shall be positioned to minimize unauthorized viewing of the information displayed on the monitors.

8.2.3 Where possible computer monitors displaying personal information shall not be left unattended and password protected screen saver options shall be used during periods of inactivity.

8.2.4 Computer hard drives and file storage media must be rendered unusable upon disposal. Contact the Information Technology Helpdesk for guidance.

8.3 Mobile Devices

8.3.1 Mobile devices include, but are not limited to, integrated hand held/Personal Digital Assistants (PDAs), cellular phones removable media (flash drives, memory sticks, removable drives) that are connected to board computing devices and used to store and/or transport information to another device. Do not share or leave file storage media containing personal information unattended. Ensure that it is secured when not in use. <u>All mobile devices must be secured against improper access by a strong password and should be kept under the control of the employee at all times.</u>

8.3.2 All Avon Maitland District School Board laptops shall be BIOS password-controlled by a strong password. Other reasonable safeguards, such as anti-virus, anti-spy ware software and personal firewalls, should be installed. It is the responsibility of the employee to ensure this software is kept up-to-date. Employees should only use software that has been approved by the AMDSB Information Technology Department. Laptops should be set to lock screen after 5 minutes of non-use.

8.3.3 Board owned laptops with Personal Health Information and highly sensitive data must be secured with a BIOS password controlled and encryption software. Employees should contact the Information Technology Tech Help Desk for assistance with encryption installations and updates.

8.3.4 Portable devices and storage media that contain personal information should have that personal information destroyed or erased so that there is no possibility of subsequent data recovery upon completeness of its use. If employees require assistance they should contact the Information Technology Help Desk.

8.4 Working from Home

To preserve integrity and availability of records:

8.4.1 Take records off-site only when absolutely necessary; whenever practical, the original shall remain on-site and only copies removed. OSRs shall not be removed from the school.

8.4.2 Copies of documents containing personal information (for example IPRC packages) shall be clearly identified as such and destroyed when no longer needed.

8.4.3 A sign-in/sign-out procedure including sign out date to monitor removed files shall be established.

8.4.4 Records shall be returned to a secure environment as quickly as possible.

8.4.5 Employees working from home must ensure that they take reasonable steps to protect any personal information they use in their home “work” location by:

a) store all work records and sensitive information in the most secure manner possible;
b) avoiding saving personal work information on home computers. Use Board owned password protected storage media, or web enabled programs whenever possible;
c) ensuring that any documents containing personal information that require disposal are returned to an appropriate work location for shredding and not disposed of in the household garbage;
d) employees working from home should be accessing work records through a secure network connection whenever possible

8.5 General

8.5.1 When communicating personal, confidential or sensitive information, consider the physical setting and try to ensure that no one overhears the conversation, i.e. hallways, main office, etc. public telephones, etc.

8.5.2 Care must be used when transmitting personal information via a fax machine. If it is necessary to fax highly sensitive personal information, ensure that someone is ready to receive the transmission prior to sending it.

8.5.3 To ensure board access and protection of privacy, board records should not be stored and/or retained on personally owned devices.

8.5.4 To ensure the security and protection of privacy of electronic student data; access to student records within the Student Information System is distributed by the role of the employee upon login. The Principal must approve any changes to that standardized access.

8.5.5 Exporting student data from the Student Information System should only happen when absolutely necessary and the data must be kept secure at all times.

9.0 Training Related to the Management of Student's Personal Information

Employees must be trained on the proper usage of the mobile device. Training should include privacy and security requirements as well as responsibilities for appropriate care of information according to this Administrative Procedure.

9.1 Principals should remind staff to review this Administrative Procedure every September.

9.2 All new employees must receive a copy of this Administrative Procedure in their orientation package.

10.0 Retention and Destruction of Personal Information

10.1 In accordance with MFIPPA, personal information that has been used shall be retained for a minimum of one year.

10.2 Personal information may be destroyed prior to the one year minimum retention period with the agreement of both parties.

10.3 The Board's Records Classification Schedule and Retention Schedule set the retention and destruction requirements of all Board records.

10.4 Staff must ensure that records containing personal information be destroyed in a method appropriate to the medium, i.e. paper-shred, computers - rendered unusable.