RECORDS MANAGEMENT

These regulations govern the records management procedures to collect, use and disclose, retain, and dispose of Pembina Trails School Division (the Division) records.

1. DEFINITIONS

1.01 Records

a) Records shall be defined as any type of recorded information or image created or received by any Division employee in schools or administrative departments or the Board, regardless of physical form or characteristics. Records include, but are not restricted to, administrative files, personnel records, and student records (which include Pupil Files) in both paper and electronic formats, whether in draft or final form;

b) Electronic records are information created, recorded, stored and/or manipulated in any digital storage device carrying data in any format but excluding the computer program(s) application(s) that were used to produce the electronic record(s);

c) Permanent records include any record which has been identified as having an enduring value. They may be of permanent significance to the Division for legal, fiscal, or administrative purposes. Permanent records may also be of historical and/or cultural importance to a wide range of people including former students, teachers, local historians, academics and the general public.

1.02 Archives

Archives is an agency responsible for the protection in environmentally sound storage conditions of permanent records no longer required for operational purposes. Records are serviced by knowledgeable staff and made available to the public under access conditions determined by provincial legislation or Division policy.

Archiving is the act of transferring (a) record(s) to an archival facility.

1.03 Digital Storage Device

A digital storage device is a piece of equipment that stores or records electronic data.

1.04 Designated External Party

A designated external party is any vendor or contractor who is engaged by the Division to provide services, including but not limited to, legal, financial, nursing, or clinician services, or software programs and support, and who, from time to time, needs access to specific information to carry out its obligations to the Division.

1.05 Destruction

Destruction of a record means the process of eliminating or deleting the record beyond any possible reconstruction.

1.06 Disposition

Disposition of a record means transfer of a record to another education authority, the destruction of a record, or transfer to the designated archives, following the expiration of the retention period.

1.07 Personal Information

Personal information means recorded information about an identifiable individual, including the following as defined in FIPPA:

a) the individual's name,

b) the individual's home address, or home telephone, facsimile or e-mail number,

c) information about the individual's age, sex, sexual orientation, marital or family status,

d) information about the individual's ancestry, race, colour, nationality, or national or ethnic origin,

e) information about the individual's religion or creed, or religious belief, association or activity,

f) personal health information about the individual,

g) the individual's blood type, fingerprints, or other hereditary characteristics

h) information about the individual's political belief, association, or activity,

i) information about the individual's education, employment or occupation, or educational, employment or occupational history,

j) information about the individual's source of income or financial circumstances, activities, or history,

k) information about the individual's criminal history, including regulatory offences,

l) the individual's own personal views or opinions, except if they are about another person,

m) the views or opinions expressed about the individual by another person, and

n) an identifying number, symbol or other particular assigned to the individual.

1.08 Personal Health Information

Personal health information as defined by The Personal Health Information Act (PHIA), Section l(1), is any recorded information about an identifiable individual, including electronic information, including:

a) the individual's health, or health care history, including genetic information about the individual,

b) the provision of health care to the individual, or

c) payment for health care provided to the individual,

d) the personal health information number (PHIN) as defined in PHIA, and any other identifying number, symbol or particular assigned to an individual, and

e) any identifying information about the individual that is collected in the course of, and is incidental to, the provision of health care or payment for health care.

1.09 Pupil File

The Pupil File is a record or collection of records as defined in Regulation JRA-R.

2. RESPONSIBILITIES

2.01 Secretary-Treasurer or Designate

The Secretary-Treasurer or designate shall be responsible for administration of this policy and management of Division records, including:

a) ongoing communication of records management procedures to appropriate Division staff, i.e. management and designated employees, and provision of instructions for the conduct of the records management operation, including any applicable training,

b) ongoing communication to all Division employees with respect to their personal duty of care with regard to Division records,

c) establishing procedures for the retention and disposition of all records in accordance with this policy and Retention Schedule (Exhibit EHB-E-1),

d) taking reasonable steps to ensure that policy provisions are being implemented and that any breach of security is recorded and corrective action taken.

2.02 Access and Privacy Officer & Access and Privacy Co-ordinator

a) In accordance with Policy GBJD, the Secretary-Treasurer shall be assigned as the Access and Privacy Officer under FIPPA and, as such, is responsible for the overall direction of access to information and protection and privacy functions within the Division, and for ensuring that the Division is collecting, using and disclosing personal information and personal health information in accordance with the provisions of FIPPA and PHIA.

b) In accordance with Policy GBJD, the Secretary-Treasurer shall designate the Access and Privacy Coordinator under FIPPA. The Secretary-Treasurer may assign responsibility for receiving applications for access to records, for the day-to-day administration of FIPPA, and for providing assistance respecting the collection, correction, use, protection, and disclosure of personal information.

2.03 Administrative Responsibilities

Senior Administrators, Directors, and School Administrators shall be responsible for records under their jurisdiction with respect to:

a) implementing and maintaining a records management process that meets the requirements of this policy and is consistent with the records management procedures and directives established by the Secretary-Treasurer or designate.

b) assigning responsibility for maintenance of records, including file indices for efficient retrieval, retention, disposition, and destruction in accordance with Division policies,

c) taking reasonable precautions to protect Division records from fire, theft, vandalism, deterioration, accidental destruction or loss, or other hazards,

d) ensuring that staff under their supervision are kept informed of their responsibilities under this policy and regulation.

2.04 Employee Responsibilities

a) All employees are responsible for the accuracy and safekeeping of Division records under their care and/or in their possession and for the confidentiality of personal information and personal health information in accordance with Division policy and applicable legislation;

b) Employees with access to personal health information must sign the Pledge of Confidentiality as set out in Exhibit EHB-E-2 that includes an acknowledgement that the employee is bound by the Division's policy and procedures regarding personal health information and is aware of the consequences of breaching them.

2. RETENTION AND DISPOSITION

3.01 Division records shall be maintained and disposed of in accordance with conditions of this policy and Exhibit EHB-E-1. Although the disposition of some records could be delayed occasionally because of negligible accumulation, the provisions of Regulation EHB-R should be adhered to in normal circumstances.

3.02 The Archives of Manitoba shall be the designated archive facility for the Division;

3.03 Recording the Destruction of Records

a) A control log shall be kept of all pupil files that are destroyed. This record shall be in accordance with Provincial legislation, this policy, and the Guidelines on the Retention and Disposition of School Division/District Records;

b) A control log shall be kept of the destruction of records containing personal health information. This record shall be in accordance with subsection 17(4) of PHIA;
c) Records of destruction for any records other than Pupil Files or Personal Health Information shall be in accordance with Manitoba Education regulations and guidelines.

3.04 All paper records are to be destroyed by shredding under controlled and confidential conditions. The standard for shredding is 3/8 inch.

3. ACCESS

Use

4.01 Employees who retrieve records from a filing or storage location must safeguard them from inappropriate access and return the files to their proper locations as soon as they have served current use.

4.02 Personal information and/or personal health information included in Division records are to be used only by those employees and designated external parties who need the information in order to carry out their assigned duties as established.

4.03 Access to the Pupil File shall be in accordance with Regulation JRA-R.

Disclosure

4.04 Personal information and/or personal health information are not to be disclosed to any third party without the consent of the individual the information is about, or as provided for in legislation.

4.05 The Division shall allow individuals the right to examine and receive a copy of their own personal health information. The process for requesting and processing a correction shall be in accordance with PHIA, Section 12.

4.06 a) Where terms of a collective agreement cover access by an employee to the employee's personal records, access to the records shall be in accordance with the collective agreement;

b) Where there is no provision in a collective agreement, all employees shall have access to their personal records in accordance with Division procedures.

4.07 Information that the Division is obligated by legislation to disclose will be available to the public without a FIPPA application. Information that the Division does not routinely disclose may be made available without a FIPPA application at the discretion of the Division. All other requests for information will require a FIPPA application.

5. USE OF ELECTRONIC MEDIA

Electronic Mail (email)

5.01 Email messages shall be automatically deleted from the system once they are two years old. If an email recipient determines that an email is of enduring value, the employee shall retain the information in an appropriate manner and in accordance with this policy.

5.02 Routine administrative email messages may be deleted at such time as it has been determined that the information is no longer required.

Electronic Files

5.03 All electronic records must be backed up on a regular basis at appropriate time periods and in an appropriate manner to ensure that they are protected from accidental or deliberate loss. It is the responsibility of the IT Department to ensure that an effective, automatic back-up process for records is implemented and working properly.

5.04 All electronic records must be retained in a manner that will ensure security, long-term availability, minimal deterioration, and availability during the prescribed retention period.

5.05 When electronic records have exceeded the prescribed retention period, the data must be rendered unreadable.

5.06 Prior to the disposal or reuse of any digital storage device, all electronic records must be rendered unreadable.

Voice Mail

5.07 Employees shall delete administrative voice mail messages when the information is no longer required. Voice mail messages determined to be a retainable record should be transcribed before deleting or saved in an alternate electronic location and then retained in accordance with this policy.

5.08 No electronic or back-up copies of voice mail messages shall be retained on the Division's voice mail system.