

STUDENT RECORDSGeneral:

In accordance with the Public Schools Act (PSA) and the regulations therein, the Turtle Mountain School Division shall collect and maintain information on each student registered in the Division.

The Division is responsible for protecting this information from unauthorized release or access.

The collection, use, protection, retention and/or disclosure of information contained in Student Records shall be in accordance with the provisions of the Freedom of Information and Protection of Privacy Act (FIPPA), the Personal Health Information Act (PHIA), the Youth Criminal Justice Act (YCJA), the PSA – Appropriate Education Programming Regulation 155/2005 and Education Administration Act (EAA) Regulation 156/2005 as appropriate.

Turtle Mountain School Division accepts as policy the practices and procedures outline in Manitoba Education and Training's Guidelines on the Retention and Disposition of School Division/District Records and Manitoba Pupil File Guidelines, and shall ensure compliance with the Freedom of Information and Protection of Privacy Act (FIPPA), the Personal Health Information Act (PHIA) and the Youth Criminal Justice Act (YCJA).

Managing Pupil Files:Definitions:

The Pupil File is a record or collection of records respecting a pupil's attendance, academic achievement and other related matters in the possession or control of the school board. These records may include:

- Personal Information
- Personal Health Information
- Youth Criminal Justice Information
- Third Party Information

The *Adoptions Act* requires that the records of adopted persons must be managed in a way that ensures that cross-referencing between birth and adoptive identities cannot occur. For this reason, when a student enrolled in a school is placed for adoption, the MET No. assigned to the student will be retired and a new MET No. will be assigned to the student's adoptive identity. A new pupil file for the student's adoptive identity must be created before the pupil file is transferred to the student's new school.

The purpose of collecting information on students shall relate to the provision of educational programs and services supporting the student's educational progress. Information may be collected either directly from the pupil or parent/legal guardian or indirectly from another source. Both collections are allowed under PHIA and FIPPA, although indirect collection requires consent, except under certain limited conditions.

The Pupil File may be organized and separated into sub-files by three components: the cumulative file, pupil support file and Youth Criminal Justice file. All are considered part of the pupil file for definition, collection, access, retention, destruction or transfer considerations.

#### Cumulative File (all students):

- Standard or routine information that schools have on all pupils.
- Behavioural misconduct information including suspensions/expulsions.
- Child custody, guardianship agreements or orders.
- Home/school communications.
- Cross-reference listing identifying the location of all information about a pupil that is held by the school division/district.
- Results of tests administered to most students.
- Up-to-date notations or referrals to/contacts with external agencies.
- Admission advisement concerning whether the student has used or is continuing to use social services, psychological/psychiatric or counselling resources.

#### Pupil Support File (some students):

- Exists for some students.
- Information about a student may be held in more than one location if a system of cross-reference is in place.
- Detailed documentation about the provision of resource services from within or outside of the school division/district.
- Ongoing health/psycho-social/counselling information.
- School clinician reports/correspondence/logs/notes.
- Results of specialized diagnostic tests.
- Services provider reports.
- Individualized Education Plan and/or Health Care Plan.

#### Youth Criminal Justice File (some students):

- Exists only for a few students.
- Access, disclosure, retention and destruction set out in the Youth Criminal Justice Act (Canada)
- Strict security requirements (must be kept separate from cumulative and pupil support files).

#### Access:

All staff who may require access to student records must sign a pledge of confidentiality that includes an acknowledgement that they are bound by the policy and procedures of the Division and provincial legislation.

All student records, including student services records, shall be stored in a secure location under lock and key.

Principals, teachers, and other school personnel authorized by the principal shall have access to the student records.

#### Parent(s)/Legal Guardian(s):

1. Under Section 42.3(1) of the Public Schools Act, parent(s) or legal guardian(s) of students under the age of 18 years, shall be permitted to examine their child's designated basic student records (see above) by arrangement with the principal and in the presence of the principal or the principal's designate. When the student is 18 years or older the consent of the student is required.

Copies of these basic student records can be provided by the principal to the parent/legal guardian or adult student upon request.

In accordance with the Criminal Youth Justice Act Parent(s)/Legal Guardian(s) cannot access information that is in the young offender file.

2. The non-custodial parent/legal guardian shall have access to student records as defined under the Family Maintenance Act.
3. Adoptive parent(s)/legal guardian(s) shall have all rights of access to the student records of their child/children. The biological parent(s)/legal guardian(s) shall not have access to this information without the permission of the adoptive parent(s)/legal guardian(s).
4. Parent(s)/Legal Guardians may only have access to personal health information on their child/children when it has been determined that the child does not have the capacity to make his/her own basic health care decisions.

Pupil Support Files:

No school personnel shall have access to a clinical record other than its originator, the principal, and the professional staff members designated by the principal who have a legitimate interest in such information.

The Division may refuse to provide access to all or part of the student records where disclosure could reasonably be expected to:

- a) constitute unreasonable invasion of the privacy of a third party;
- b) be detrimental to the education of the student;
- c) endanger the mental or physical health or safety of a student or another person; or
- d) be injurious to the enforcement of an investigation under an enactment.

Release of Information:

No information shall be released to unauthorized persons nor shall any unauthorized person have access to the student records, with the exception being the provision of such information in response to a court subpoena.

If the student is 18 years of age or older, and not under the committee of the Public Trustee, the student's consent is necessary prior to the release of information.

The principal may authorize the release of pertinent student records to police officers, probation officers and representatives of child welfare agencies in order to assist these individuals or agencies to carry out their duties provided disclosure of personal information is limited to the amount necessary to accomplish the authorized purpose. Young Offenders Information in a pupil file can only be disclosed to ensure compliance by the pupil with an authorization respecting temporary release or with an order of any court concerning bail, probation or conditional supervision; or to ensure the safety of staff, students, or other persons connected with the school. Requests for access to clinical information shall be directed to the Assistant Superintendent of Student Services or Superintendent.

Student Services Records:

Parent(s)/Legal Guardians shall have access to the clinical records on their child/children who are under 18 years of age.

- a. A student (18 years or older) or parent(s)/legal guardian(s) who requests access to a clinical record or information from it, shall be referred to the originating person or agency for the information and an appropriate interpretation of it, and written copies of student services reports shall be provided by student services if requested.

- b. Parent(s)/Legal Guardian(s) who request access to a clinical record, or information from it about their child who is 18 years or over, shall require the consent of the child;
- c. Any requests from other individuals for access to clinical information in school records shall be directed to the Assistant Superintendent of Student Services or Superintendent. Superintendent and the release of this information shall require the consent of parent(s)/legal guardian(s), or student(s) over 18 years of age.
- c. Requests for any personal health information concerning specific students including the student's health or health care history, the provision of health care, the PHIN and any other identifying number other than by the parent/legal guardian or student shall be referred to the Secretary-Treasurer.

#### Third Party Requests for Information:

Third-party requests for personal and personal health information may only be granted where authorized under FIPPA, Section 44(1), or PHIA Section 22(2) or with consent of the pupil or parent/legal guardian. Pupil and Pupil Support Files may be transferred to another division without consent under PHIA and FIPPA, as required under Section 2((3) of the Education Administration Miscellaneous Provision Regulation. Requests for information in the Pupil Support file should be directed to the Student Services Department. Youth Criminal Justice File information may only be shared on a need-to-know basis under limited conditions.

- To ensure compliance by the pupil with a court order.
- To ensure safety of staff, students and others.
- To facilitate the rehabilitation of the young person.

For further information, please see the Manitoba Pupil File Guidelines.

#### Dispute Over Contents of Student Records:

If a question develops regarding the relevance or accuracy of information contained in the cumulative file, it shall be noted in writing (on the material in question) by the person reviewing the file, dated, and signed and shall become part of the file.

#### Appeal Process:

If a parent/legal guardian or a student over the age of 18 wishes to appeal the relevance or accuracy of any information contained in the student records, the following appeal process shall be followed:

- a. A written request, outlining the specifics of the appeal, shall be submitted to the Access and Privacy Officer.
- b. The Access and Privacy Officer shall review the information and render a decision, in writing, within two weeks of receipt of the requested appeal;
- c. The Access and Privacy Officer's decision may be appealed to the Board of Trustees by written request.

#### Retention and Destruction of Records:

Records should be destroyed as soon as possible after the approved retention periods have lapsed.

A disposition of record logs should be maintained that includes a description of the records, the date range and amount of records, and the date, method, and person responsible for the destruction.

For health records, a log of records destroyed that meets the requirements of subsection 17(4) of PHIA must be kept for the destruction of records that contain personal health information.

Disposition is either:

- Destruction of records, or
- Transfer of records to archives.

Files and records should be disposed of as soon as possible after the retention periods have lapsed. In most cases, this should be undertaken as an annual procedure.

The log of records destroyed should provide the name of the individual whose personal health information is destroyed, date range, destruction procedure and name of person supervising the destruction.

#### Cumulative and Pupil Support File – Retention:

- Except for Grades 9-12 marks, information in the pupil file should be retained for a minimum of ten years after the student ceases to attend school or until the file is transferred to another school.
- Grade 9-12 marks should be retained for thirty years.

#### Cumulative and Pupil Support File – Destruction:

- Destruction must be carried out in a manner that protects the privacy of the pupil.
- Where personal health information is destroyed the individual whose personal health information is destroyed, the time period to which the information relates, the method of destruction and the person responsible for supervising the destruction must be recorded.

#### Youth Criminal Justice File – Retention and Destruction:

The Youth Criminal Justice File must be destroyed when it is no longer required for the purpose for which it was established, i.e.:

- To ensure the young person follows the conditions of reintegration leave, or an order of the youth justice court, such as bail or probation conditions;
- To ensure the safety of school staff, students or other persons; or
- To facilitate the rehabilitation of the young person.

Note: IF THE STUDENT TRANSFERS TO ANOTHER SCHOOL DIVISION OR DISTRICT, THE FILE MUST BE DESTROYED.

#### Archival Option:

Permanent records should be moved into the archives designated in the Retention and Disposition Schedule. Archival options include:

- Provincial Archives of Manitoba – The Archives legislation enables the Division to transfer its permanent records to the Provincial Archives.
- Divisional Archives – Divisional archives are established to ensure proper storage conditions and servicing of archival information. Each school will keep an up-to-date database of records stored in divisional archives.

### Physical Security:

- The Division's administration security officer must ensure that a locked environment is established where all confidential information, including personal health information, is stored or accessible. This could mean a whole wing, a room or a filing cabinet.
- The administrative security office must maintain a duplicate key for each office.
- Electronic doors, if applicable, must not be left open while the area is unattended; combinations must not be disclosed to unauthorized personnel.
- Materials dealing with confidential information must be closed and not left open for viewing when away from desk or work area. Confidential material must be cleared from the desktop at the end of the day.
- Portable computers must be locked away when not in use and sensitive data on the hard drive must be password protected or encrypted.
- When files are removed from the work site a staff member is responsible for ensuring an appropriate level of security and confidentiality at all times.
- Physical information (i.e. paper files), electronic media and/or portable computers must not be left unattended in open view in a vehicle but rather locked in the trunk of the vehicle. For vehicles that do not have trunks, items must be placed in an inconspicuous location.

### Transmission of Confidential Information:

- Confidential information that is provided over the telephone must only be given if the identification of the requester is verified. This information must not be left on the answering machine.
- Confidential information must be faxed only when required for urgent or emergent purposes and only sent under the following conditions: there is no chance the information being transmitted can be intercepted during transmission by unauthorized personnel; the individual sending the fax is authorized to release the information; cover page of fax indicates, where applicable, "Confidential information. Disclosure, distribution or copying of the content is strictly prohibited. If you have received this fax in error please notify the sender immediately"; to the extent possible, a designated recipient must be available to receive the fax containing personal health information.
- Transmitting information via e-mail must only be done if the venue of transmission is secure or the data is encrypted.

### Electronic Security:

The following process will be adhered to ensure security of electronic information.

- Shared USER ID's and passwords must only be assigned where it is not feasible to assign an individual USERID because of degradation of service to the public. USER ID's and passwords will be maintained.
- USERID and password must not be shared with anyone except as may be necessary for authorized personnel to perform maintenance on the PC in which case the password must be changed as soon as the maintenance is performed.
- The USERID is deleted as soon as it is known that an individual is leaving.
- USERID or password must not be taped to computer or left where it is easily accessible.
- A listing of all USER ID's/passwords for divisional staff will be maintained.
- Employees must be responsible for logging out of the computer system each evening.
- Information must be password protected or encrypted, where feasible, when transporting electronic information on portable computers.
- Reasonable precautions are to be taken to protect personal health information from fire, theft, vandalism, deterioration, accidental destruction or loss and other hazards.

### Pupil File Transfer Procedures:

- When pupil files are transferred from division to division, they should be reviewed to ensure that only the personal information and personal health information necessary for the provision of educational services to that pupil is forwarded. All pupil file records, as defined in the pupil file guidelines, will be passed on to the requesting educational authority, with the exception of the following:
- Personal notes of the resource teacher, counsellor, clinician or administrator will be reviewed and summarized for the file before it is transferred.
- Meeting notes that are not necessary for the continued educational services for the student.
- Irrelevant or outdated student work samples with the exception of those samples needed for future programming.
- Information about a third party.
- Unsigned/undated notes.
- Other agency information that does not pertain to schooling and provision of educational services.
- When in doubt, consult with the Principal or Access and Privacy Coordinator.
- Personal notes and records of teachers, counsellors and administrators must be kept for a period not to exceed the end of the school year following the year of departure.
- Personal notes must be forwarded upon culling and summarizing to the school principal for filing and records management.
- The principal should set up procedures for the filing and retention of the above files for the period defined and establish procedures for forwarding the records to the divisional records manager for destruction.
- The principal must keep a record of the file management system and forward a copy of the record management to the records manager with the materials to be destroyed.

### Please also note the following:

- A principal must forward the pupil file when the pupil transfers out of the school and enrolls in another school (M.R. 468/88).
- A principal must provide the pupil file of a pupil who has transferred to another school to that school within one week of the school requesting it (M.R. 156/05).
- When a pupil transfers into a school, he/she cannot be denied educational programming for more than 14 days regardless of whether that school has received the pupil's pupil file. An exception is risk of safety (M.R. 155/05).
- FIPPA and PHIA allow for the transfer of the personal and personal health information in the cumulative file component and the pupil support file component of the pupil file (with or without consent) because it is required by an enactment.
- Only information necessary for the schooling and provision of educational services should be forwarded.
- Protect file from unauthorized access, disclosure, loss or destruction during transfer.
- Pupil support file component should be transferred from professional to professional (Student Services Department).
- The YCJA does not allow for the Youth Criminal Justice File to be transferred to another division/district. However, the principal must inform the youth worker responsible for the student of the move and the name/location of the new school. The youth worker is responsible for advising the new school of any pertinent information.

### Pupil File Annual Review Procedures:

The following guidelines and procedures apply to an annual review and culling of pupil files:

- Pupil files and working files are to be reviewed annually before the end of the school year by each classroom teacher, student services teacher, student services counsellor or clinician.
- The files should be culled to remove:
  - Undated and unsigned notes or documents
  - Irrelevant and outdated student work
  - Meeting notes that are not necessary to ongoing educational services for the student
  - When in doubt, the teacher should consult the principal.
- Files that are culled from the pupil file must be listed for content and sent to the records manager for destruction. A copy of the records content should be sent with the records to be destroyed. The summary will be kept on file as part of the disposition system.