Student Records Management
Administrative Procedure 1.A.160

Board Governance Policy Cross Reference: 1, 2, 3, 16, 17

Legal Reference*: Freedom of Information and Protection of Privacy Act (FIPPA), Personal Health Information Act (PHIA), Youth Criminal Justice Act (YCJA), PSA- Appropriate Educational Programming Regulation 155/2005, EAA Regulation 156/2005*

Date Adopted: June 2002

Date Amended: October 2006, June 2012, June 2018, February 2019, September 2024

Evergreen School Division is the custodian of a large amount of confidential information (personal and health). The Division, as a public body, is responsible for protecting this information from unauthorized release or access.

The implementation of efficient records management, particularly in light of technological change, enables divisions to discharge their responsibilities to ensure both access to and protection of information.

Evergreen School Division accepts as policy the practices and procedures outlined in:

- Manitoba Education and Training's Guidelines on the Retention and Disposition of School Division/District Records
- Manitoba Pupil File Guidelines

Evergreen School Division 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)
- the policy requirements of The Personal Health Information Act respecting collection, use, disclosure, security, retention and destruction of personal health information.

NOTE: The Secretary Treasurer is responsible for records management. Duties may be delegated as needed.

Responsibility for Records Management

- each school, site or department is responsible for proper filing, retention and storage of the files and records relative to their site
- each school, site or department shall designate a staff person who is responsible for records management
- duties include:
    - general filing of hard copy materials
    - updating of file index for all items, providing all the data required for the index such as category, name, location, etc.
    - ensuring that copies of appropriate reports and documents are archived

- retaining electronic data
- disposing of files and records
- maintaining an audit trail of filing activity (transfers, disposal, loans)
- other filing and record-keeping tasks as assigned

Ownership of Records

- all files are the property of the Division
- staff leaving employment shall ensure that the files and records are transferred to the appropriate member of the site's administration.

Disclaimer

- the following disclaimer is to be included on all application forms, referral forms, reports, or any form where personal or personal health information is being collected in Evergreen School Division:

This personal information, or personal health information, is being collected under the authority of Evergreen School Division and will be used for educational purposes or to ensure the health and safety of the student. It is protected by the Protection of Privacy provisions of The Freedom of Information and Protection of Privacy Act and The Personal Health Information Act.

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 purpose of collecting this information must relate to the provision of educational programs and services supporting the pupil's educational progress

- information may be collected either directly from the pupil or parent/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 info 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, except that the Youth Criminal Justice component should never be transferred

Cumulative File:

- exists for all students
- standard or routine information that schools have on **all** pupils
- ***1.A.160A: Cumulative File Insert: Cross-Reference Listing*** which identifies the location of **all** information about a pupil that is held by the school division/district
- behavioral misconduct information including suspensions/expulsions
- child custody, guardianship agreements or orders
- home/school communications
- 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 counseling resources; this information is requested of parents/guardians on the ***Student Registration Form***

Pupil Support File Contents:

- exists for only some students
- information about a student may be held in more than one location if a system of cross-reference is in place
- documentation about the provision of resource services from within or outside of the school division/district; this information is requested of parents / guardians on the ***Student Registration Form***
- ongoing health/psycho-social/counseling information
- school clinician reports/correspondence/logs/notes
- results of specialized diagnostic tests
- service provider reports
- Individualized Education Plan and/or Health Care Plan
- if more information is required, use ***1.A.160C: Release of Information*** to request such

Youth Criminal Justice File:

- 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)

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, resource teacher, counselor 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 site's designated 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

File Control Procedure

Retention and Destruction of Records

- see ***5.140A: File Retention and Destruction Record***
- at the expiration of the retention period, records are to be forwarded to the Education Support Centre with a list or summary of contents. The records will be destroyed centrally under controlled confidential conditions unless deemed archival. The summaries or lists in will be filed in a disposition of records log.
- 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

- ESD Secretary Treasurer or designate 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
- ESD Secretary Treasurer or designate 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
- use ***1.A.160C Release of Information*** if parents want to authorize the school to share information with outside of Division agencies, etc.

Electronic Security

ESD Secretary Treasurer or designate (IT Manager) is responsible for the following:

- assigning USER ID's and passwords for all Divisional staff
    - 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
- maintaining a list of USER ID's and passwords for all Divisional staff
- approving any sharing of such list
- deleting USERID as soon as it is known that an individual is leaving

Employees are responsible for:

- ensuring USERID and password are not 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
- ensuring USERID or password is not taped to computer or left where it is easily accessible
- logging out of the computer system each evening
- ensuring information is password protected or encrypted, where feasible, when transporting electronic information on portable computers

Reporting Security Breaches

- any security breaches involving personal health information are to be immediately reported by Principal if the breach occurred at school or by immediate supervisor if the breach is identified by a divisional employee
- use ***8.00A Serious Incident Report*** and forward to ESD Privacy Officer (Assistant Superintendent)
- ESD Privacy Officer (Assistant Superintendent) will investigate all security breaches and recommend corrective procedures to address security breaches.

General

- reasonable precautions are to be taken to protect personal health information from fire, theft, vandalism, deterioration, accidental destruction or loss and other hazards
- Evergreen School Division shall conduct an audit of its security safeguards at least every two years and shall take steps to correct any deficiencies as soon as practicable

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 files guidelines, will be passed on to the requesting educational authority, with the exception of the following:
- personal notes of the resource teacher, counselor, 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 that 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 ESD Learning Coordinator
- personal notes and records of teachers, counselors 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 Education Support Centre for destruction
- the Principal must keep a record of the file management system and forward a copy of the record management to the ESD Secretary Treasurer or designate 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)
- the pupil and parent(s) or legal guardian(s) should be advised of the transfer of the file and the nature of the information transferred
- the cumulative file component and pupil support file component transfer must still take place when objections are raised
- 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
- duplicate information and information that is not necessary for the schooling and provision of education services may be culled and destroyed
- protect file from unauthorized access, disclosure, loss or destruction during transfer
- pupil support file component should be transferred from professional to professional (usually via Student Services Department)
    - if it is not possible to transfer from professional to professional, the files should be still transferred to the new school
    - the files should be clearly identified as containing sensitive personal health information so that the receiving school or school division can ensure that only appropriate personnel have access to these files
- 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

Access and Privacy

Administrative Security

- school divisions must ensure that each new employee signs a pledge of confidentiality. See ***2.A.87 H: Employee PHIA Pledge of Confidentiality***
- procedures regarding records management and protecting confidential information (personal and health) must be part of an orientation session
- staff access to files is permitted to the extent that the information is necessary to assist in the educational program of the pupil; various staff members may need to have access to different pieces of information in order to carry out their duties
- access to information in the Youth Criminal Justice File may only be made available under restricted conditions:
- to ensure compliance by the pupil with a court order
- to ensure safety of staff, students or other persons, or
- to facilitate the rehabilitation of the young person
- a list of those entitled to access should be attached to the Youth Criminal Justice File
- students who have reached the age of majority (18) may have access to their files except under certain conditions; this includes both personal and personal health information
- while a student under age 18 does not have a right to access his/her "pupil file" under the Public Schools Act, he/she may apply under FIPPA and PHIA to access this information
- school divisions are not authorized to disclose information in the Youth Criminal Justice file to the pupil or to the parent/guardian
- under Section 42.3(1)(a) of the *Public Schools Act*, parents/guardians can access the pupil file until the child reaches the age of majority; there are limited grounds for refusing access; pupils age18 years or older must indicate whether they allow their parent/guardian access to their pupil file
- see:***1.A.160B: Consent to Disclose Personal Information to Parents/Guardians of Students 18+***
- divorced/separated parents have the right to receive information as to the health and education of their child unless the court orders otherwise.

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/guardian
- Pupil and Pupil Support Files may be transferred to another division without consent under PHIA and FIPPA, as required under Section 29(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