Administrative Procedure 2080

Records Management – Protection of Personal Health Information of Students

Board Governance Policy Cross Reference: 1, 9, 13, 14, 15

Administrative Procedures Cross Reference:

Records Management

Records Retention and Disposition

Records Management – Protection of Personal Information of Students

Records Management - Protection of Personal Health Information of Students

Records Management - Protection of Information Under the *Youth Criminal Justice Act (Canada)*

Records Management - Protection of Personal Information of Employees

Records Management - Protection of Personal Health Information of Employees

Form Cross Reference:

Pledge of Confidentiality

Legal/Regulatory Reference:

Manitoba Education - Guidelines on the Retention and Disposition of School Division/ District Records

Manitoba Education – Manitoba Pupil File Guidelines

The Freedom of Information and Protection of Privacy Act

The Personal Health Information Act

The Public Schools Act

Education Administration Miscellaneous Provisions Regulation

The Child and Family Services Act

Youth Criminal Justice Act (Canada)

Date Adopted: August 2006

Amended: May 2019

Introduction

The Brandon School Division (the "Division") is the custodian of Personal Information and Personal Health Information relating to students. The Division, as a public body, is responsible for protection this information from unauthorized release or access.

The Division recognizes the right of an individual to access information that the Division holds, including information about the individual, subject to certain specified exceptions and the right to privacy for Personal Health Information in the custody and control of public bodies. This Administrative Procedure has been put into place to recognize those rights and to comply with the requirements of *The Personal Health Information Act* respecting the collection, use, disclosure, security, retention and destruction of Personal Health Information.

Definitions

Confidential Information means Personal Information and Personal Health Information and any other information collected by or about an individual that is not generally known to the public, including but not limited to information relating to a "young person" as defined by *The Youth Criminal Justice Act (Canada)* or which is deemed confidential by the Division.

Divisional Level Pupil File means that portion of the Pupil File that is maintained at the Brandon School Division Office.

FIPPA means *The Freedom of Information and Protection of Privacy Act*, C.C.S.M., c.F175 as amended from time to time.

Health means the condition of being sound in mind, body and spirit.

Health Care means any care, service or procedure

- provided to diagnose, treat or maintain an individual's health;
- provided to prevent disease or injury or promote health;
- that affects the structure or a function of the body; and
- includes the sale or dispensing of a drug, device, equipment or other item pursuant to a prescription.

Human Resources means the Human Resource Department of the Division.

PHIA means *The Personal Health Information Act,* C.C.S.M., c.P33.5, as amended from time to time.

Personal Information means recorded information about an identifiable individual, including:

- the individual's name;
- the individual's home address, or home telephone, facsimile or e-mail address;
- information about the individual's age, gender, sexual orientation, marital or family status;
- information about the individual's ancestry, race, colour, nationality, or national or ethnic origin;

- information about the individual's religion or creed, or religious belief, association or activity;
- Personal Health Information about the individual;
- the individual's blood type, fingerprints or other hereditary characteristics;
- information about the individual's political belief, association or activity;
- information about the individual's education, employment or occupation, or educational, employment or occupational history;
- information about the individual's source of income or financial circumstances, activities or history;
- information about the individual's criminal history, including regulatory offences;
- the individual's own personal views or opinions, except if they are about another person;
- the views or opinions expressed about the individual by another person; and
- an identifying number, symbol or other particular assigned to the individual.

Personal Health Information means recorded information about an identifiable individual that relates to

- the individual's health, or health care history, including genetic information about the individual;
- the provision of health care to the individual; or
- payment for health care provided to the individual;

and includes:

- the personal health identification number (PHIN) assigned to an individual by the Minister of Health to uniquely identify the individual for health care purposes, and any other identifying number, symbol or particular assigned to an individual; and
- 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.

Pupil File means a record or a collection of records respecting a student's attendance, academic achievement and other related matters in the possession or control of the Division. The Pupil File may contain the following information:

- Personal Information;
- Personal Health Information;
- information relating to a "young person" as defined by *The Youth Criminal Justice Act (Canada);* and

- information relating to a third party.

Records Management Administrative Procedures means the Administrative Procedures of the Division relating to the collection, management, disclosure, protection, and destruction of records collected and maintained by the Division and shall include the following Administrative Procedures: *2090 – Records Management - Protection of Personal Information of Students; 2080 – Records Management - Protection of Personal Health Information of Students; 2070 – Records Management - Protection of Information under the Youth Criminal Justice Act (Canada); 2085 – Records Management - Protection of Personal Information of Employees; 2075 – Records Management - Protection of Personal Health Information of Employees;* and *2095 - Records Retention and Disposition.*

School Level Pupil File means that portion of the Pupil File that is maintained at the School within the Division that the Pupil is attending.

Senior Administration includes:

- the Superintendent/CEO of the Brandon School Division;
- the Assistant Superintendents of the Brandon School Division;
- the Secretary-Treasurer of the Brandon School Division; and
- the Assistant Secretary-Treasurer of the Brandon School Division.

Any terms not defined herein but defined in *The Public Schools Act* shall for the purpose of this Administrative Procedure have ascribed thereto the meanings set out in *The Public Schools Act*.

School Division Records Management

Responsibility for Records Management

The records manager and privacy officer for the Division will be the Secretary-Treasurer or designate who shall be responsible to administer this Administrative Procedure and who will delegate duties to each Superintendent, School Leader, site manager, department head or other person as they consider to be necessary.

Each School Leader, site manager or department head, as the case may be, is responsible for proper filing, retention and storage of the files and records relative to their site and shall designate a staff person to attend to the following tasks:

- general filing of hard copy materials;
- updating of the site's 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 forwarded for archival storage as indicated in the Division Administrative Procedure entitled, "*Records Retention and Disposition*";

- retaining electronic data as indicated in the Division Administrative Procedure entitled, "*Records Retention and Disposition*";
- disposing of files and records as indicated in the Division Administrative Procedure entitled, "*Records Retention and Disposition*";
- ensuring that an audit trail is maintained of filing activity such as transfers of files to other supervisory staff, disposal of files, loans of files, etc.; and
- other filing and record-keeping tasks as may be assigned from time to time.

Ownership of Records

All pupil files are the property of the Division. Staff leaving employment shall ensure that all pupil files and records are transferred to the appropriate member of the work site's administration who shall ensure that the site's file index is updated accordingly.

Notice

The following notice is to be included on all application forms, referral forms, reports, or any form where Personal Information or Personal Health Information is being collected.

This Personal Information or Personal Health Information is being collected under the authority given to the Division under *The Public Schools Act* and will be used for educational purposes or to ensure the health and safety of students. The information is protected by the Protection of Privacy provisions of the *Freedom of Information and Protection of Privacy Act* (including but not limited to section 37) and the *Personal Health Information Act* (including but not limited to Part 3, Division 1). If you have any questions about the collection, contact the Brandon School Division Access and Privacy Officer at (204) 729-3100 or by mail at the Brandon School Division, 1031 – 6th Street, Brandon, Manitoba, R7A 4K5.

Managing Pupil Files

General

The Pupil File will 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, use, disclosure, security, access, retention, destruction or transfer considerations. Information comprising the Pupil File of a student may be held in more than one location if a system of cross-reference is in place. Without limiting the generality of the foregoing, a Divisional Level Pupil File and a School Level Pupil File are permitted so long as the provisions of this procedure are followed.

Sub-components of the Cumulative File and Pupil Support File of a student may be held in more than one location if a system of cross-reference is in place. The Youth Criminal Justice File shall not be held in more than one location.

See the *Manitoba Pupil File Guidelines* for details regarding legislative requirements for pupil files.

Cumulative File

A Cumulative File exists for all students and may contain:

- cross-reference listing identifying the location of all information about a student that is held by the Division;
- standard or routine information that schools have on all students;
- behavioural misconduct information including suspensions/expulsions;
- child custody, guardianship agreements or orders;
- home/school communications;
- individual Education Plans and/or Health Care Plans;
- results of tests administered;
- up-to-date notations or referrals to/contacts with external agencies; and
- indication of whether there exists a Pupil Support File, or Youth Criminal Justice File for the student.

No personal Health Information shall be contained in the Cumulative File other than that which is necessary for the day-to-day programming for the student. In all other cases, if there arises a situation where Personal Health Information is contained in a record that is to be filed in the Cumulative File, the Personal Health Information shall be severed from the record with a fully intact record being stored in the Pupil Support File. Any Personal Health Information contained in the Cumulative File is to be governed by the provisions of *Personal Health Information Act* and the Division Administrative Procedure entitled "*Records Management – Protection of Personal Health Information of Students*".

Pupil Support File

A Pupil Support File exists for some students and may contain:

- cross-reference listing identifying the location of the Cumulative File;
- detailed documentation about the provision of resource services from within or outside of the Division;
- ongoing health/psycho-social/counseling information;
- school clinician reports/correspondence/logs/notes;
- results of specialized diagnostic tests;
- service provider reports;

- admission advisement concerning whether the student has used or is continuing to use social service psychological/psychiatric or counseling resources; and
- all other Personal Health Information.

Any Personal Health Information contained in the Cumulative File is to be governed by the provisions of *Personal Health Information Act* and the Division Administrative Procedure entitled "*Records Management – Protection of Personal Health Information of Students*".

Youth Criminal Justice File

A Youth Criminal Justice File exists for some students and the procedures relating thereto are set out in a separate Administrative Procedure entitled *Records Management - Protection of Information Under the Youth Criminal Justice Act (Canada)*. The Youth Criminal Justice File shall contain a cross-reference listing identifying the location of the Cumulative File.

School Level Pupil File Annual Review Procedures

The following guidelines and procedures apply to an annual review and culling of Pupil Files at the school level only. They are in addition to and do not replace the Division's existing Administrative Procedure entitled "*Records Retention and Disposition*" and the existing guidelines established by Manitoba Education entitled "*Guidelines on the Retention and Disposition of School Division/District Records*".

Each School Leader shall ensure that the Cumulative File and Pupil Support File are reviewed annually before the end of the school year for the purpose of culling the record to remove:

- undated and unsigned notes or documents;
- irrelevant and outdated student work; and
- meeting notes that are not necessary to ongoing educational services for the student.

The School Leader may delegate the review and culling of the file to their delegate, which may include classroom teachers, resource teachers, or school counselors. When in doubt about whether the record is to be removed, the delegate should consult the School Leader. If the School Leader is unsure as to whether the record should be removed, they should contact the records manager, who will make the ultimate decision in the matter.

Records that are removed in the culling process are to be shredded on site as soon as possible by the School Leader or delegate. File material that is culled from the Cumulative File and Pupil Support File must be listed for content. The summary will be kept on file as part of the disposition system with a copy of the listing being forwarded to the records manager. Following the review of the file the Index for each file shall be updated if necessary.

Any procedure for reviewing and culling the Youth Criminal Justice File shall be that set out in a separate Administrative Procedure entitled Records Management - Protection of Information Under The *Youth Criminal Justice Act* (Canada).

Divisional Level Pupil File Annual Review Procedures

The following guidelines and procedures apply to an annual review and culling of Pupil Files at the Divisional level only. They are in addition to and do not replace the Division's existing Administrative Procedure entitled "*Records Retention and Disposition*" and the existing guidelines established by Manitoba Education entitled "*Guidelines on the Retention and Disposition of School Division/District Records*".

The Administrator of Student Achievement Support Services or delegate shall ensure that the Pupil Support File are reviewed annually before the end of the school year for the purpose of culling the record to remove:

- undated and unsigned notes or documents;
- irrelevant and outdated student work; and
- meeting notes that are not necessary to ongoing educational services for the student.

The Administrator of Student Achievement Support Services may delegate the review and culling of the file to their delegate. When in doubt about whether the record is to be removed, the delegate should consult the Administrator of Student Achievement Support Services. If the Administrator of Student Achievement Support Services is unsure as to whether the record should be removed, they should contact the records manager, who will make the ultimate decision in the matter.

Records that are removed in the culling process are to be shredded on site as soon as possible. File material that is culled from the Pupil File must be listed for content and a copy of the list sent to the records manager. The summary will be kept on file as part of the disposition system.

Any procedure for reviewing and culling the Youth Criminal Justice File shall be that set out in a separate Administrative Procedure entitled Records Management Protection of Information Under *The Youth Criminal Justice Act* (Canada).

Access and Privacy

Access to Information under *The Public Schools Act*

Parents or guardians of students under the age of majority (18) and students who have reached the age of majority may have access to the student's Pupil File except where its disclosure would:

- constitute an unreasonable invasion of the privacy of a third party;
- be detrimental to the education of the student;

- cause serious physical or emotional harm to the student or another person; or
- be injurious to the enforcement of an enactment of legislature or the conduct of an investigation under an enactment of legislature.

Once a student has reached the age of majority, their Pupil File will not be disclosed to their parents or guardians in the absence of the student's written consent, an order under *The Vulnerable Persons Living with a Mental Disability Act* or a court order.

Access to Personal Information under *The Freedom of Information and Protection of Privacy Act (FIPPA)*

The provisions of FIPPA are in addition to and do not replace existing procedures for access to records or information normally available to the public and thus do not replace the access provisions under *The Public Schools Act*.

An applicant has a right of access to any record in the custody or under the control of the Division, including a record containing Personal Information about the applicant subject to the exceptions set out in FIPPA or any similar legislation, as amended from time to time. The Privacy Officer for the purpose of FIPPA shall be the Secretary-Treasurer or designate.

Access to Personal Health Information under *The Personal Health Information Act (PHIA)*

An individual has a right, on request, to examine and receive a copy of their Personal Health Information maintained by the Brandon School Division, subject to the exceptions set out in PHIA or any similar legislation as amended from time to time. In the case of a minor, their parent(s) or legal guardian(s) may exercise this right unless the Privacy Officer can reasonably determine that the minor has the capacity to make health care decisions on their own behalf, at which point the minor will be referred to as a mature minor and will be treated under this Administrative Procedure as if they were over the age of 18 years.

Without limiting the discretion of the Privacy Officer, in so making this determination they may rely on any relevant information which may include the following:

- a letter or certificate from the minor's family physician;
- a letter or certificate from the school counselor;
- a letter or certificate from the school clinician; and
- any relevant information contained in the Pupil File.

The Privacy Officer for the purpose of PHIA shall be the Secretary-Treasurer or designate.

Other Access Considerations

Divorced/separated parents have the right to receive information as to the health and education of their child in accordance with all legislative provisions unless a court

orders otherwise. It is the responsibility of the parents of the students, and not the Division, to ensure that these orders are kept up to date.

Administrative Security

Human Resources shall ensure that each new employee is provided access to a copy of the Division's Record Management Administrative Procedures, and must be made familiar with the procedure therein by way of an orientation session. Every employee of the Division must receive ongoing training about these procedures. As required by relevant legislation, the Division must ensure that each new employee signs a pledge of confidentiality (see *Pledge of Confidentiality*). Before this pledge is executed, the employee must be provided access to a copy of the Division's Administrative Procedures entitled "*Records Management –Protection of Personal Information of Students", "Records Management – Protection of Personal Health Information of Students", "Records Management – Protection of Information Under the Youth Criminal Justice Act (Canada)", "Records Management – Protection of Personal Information of Employees",* and/or *"Records Management – Protection of Personal Health Information of Employees*", as may be appropriate, and must be made familiar with the procedures therein by way of an orientation session. Every employee of the Division shall receive ongoing training about these procedures as required by the relevant legislation.

Staff access to files is permitted to the extent that the information is necessary to assist in the educational program of the pupil. Where it is unclear as to whether such access is necessary, the School Leader shall make the determination at a school level, with or without input from the records manager, and the records manager will make the determination at the Divisional level.

Third Party Requests for Information

Third party requests for Personal Health Information may only be granted where authorized under Part 2 of PHIA, as may be amended from time to time, or with written consent of the student or in the case of a student under the age of 18 years, the student's parent or legal guardian, where that student is not a mature minor. Third party requests for information must be directed to the Privacy Officer who may delegate duties as they see fit.

Pupil and Pupil Support Files may be transferred to another division without consent under the provisions of PHIA and FIPPA, as required under Section 29(3) of the *Education Administration Miscellaneous Provisions Regulation*. Requests for information in the Divisional Pupil File should be directed to the Student Achievement Support Services Department of the Division for this purpose. Whenever possible the Divisional Level Pupil File will be transferred directly from professional to professional. The School Level Pupil File will be transferred from school to school.

Use and Disclosure of Records

General

Personal health information shall only be used for the purpose for which it was collected. Personal health information shall only be disclosed in accordance with the laws of Canada and Manitoba, which include, but are not limited to, the provisions for disclosure under *The Public Schools Act, The Child and Family Services Act,* and *The Personal Health Information Act*, which are available to employees and students of the Division online free of charge on the Government of Manitoba's website. In addition, copies of *The Personal Health Information Act* are available in paper form at every school, work site and the Divisional office.

Consequences of Breaching PHIA

Every employee of the Division is bound by the procedures established by the Division in accordance with the provisions of PHIA relating to the access, use and disclosure of Personal Health Information. Consequences of breaching the procedures may include disciplinary action up to and including dismissal.

Every employee, trustee or information manager who commits an offense under Part 6 of PHIA may be prosecuted under that Act.

Duty of Care to Students

Notwithstanding the foregoing, the Division acknowledges that along with its obligations under the relevant legislation to protect privacy there exists also an obligation under the common law to provide a safe environment for students and to maintain the same duty of care as a reasonably prudent parent. To that end, the Division recognizes that there exists a need to disclose the Personal Health Information of its students with serious health conditions or concerns.

Where a student has a serious health concern that needs to be disclosed to those school employees and volunteers in a supervisory position, a bulletin containing a picture of the student, their name, the condition and symptoms of their conditions, treatment instructions and contact numbers for parents or next of kin shall be posted in the staff room of the relevant school. A secondary bulletin may be placed in the school office if warranted by the student's health condition or because of the location of treatment items such as medications or EpiPens. Whenever possible bulletins in the school's office will be placed in a location out of the view of the general public, that is still readily accessible in order to ensure the health and safety of the child to the best of the Division's ability.

The form of the bulletin will be included in the Health Care Plan of the students and wherever possible the consent of the parent/guardian of the students, or if the student is over the age of 18 years or a mature minor, the student him/herself, will be obtained prior to the bulletin being posted.

Notwithstanding the bulletin, Personal Information and Personal Health Information remains confidential and shall be treated as such by the Brandon School Division.

Student specific Unified Referral and Intake System (URIS) medical plans will be kept in a central location in each school and will be accessible by staff. Each School Leader will be responsible for ensuring the confidentiality of the information and ensuring that staff is aware of the location of the medical plans.

Mandatory Disclosure

Subject to the provision of *The Child and Family Services Act*, where a person has information that leads the person reasonably to believe that a child is or might be in need of protection, such as where the life, health or emotional well-being of the child is endangered, the person shall forthwith report the information to the Child and Family Services Agency or to a parent or guardian of the child.

File Control Procedure

Retention and Destruction of Records

At the expiration of the retention period set out in the Division's existing Administrative procedure entitled "*Records Retention and Disposition*" and the existing guidelines established by Manitoba Education entitled "*Guidelines on the Retention and Disposition of School Division/District Records*", records will be destroyed under controlled confidential conditions unless deemed archival. These records will be destroyed by each School Leader or department head, or their delegate. The list or summary of contents of records destroyed are to be forwarded to the Division Office to the attention of the records manager. The records manager will file the summaries or lists in a disposition of records log.

Disposition is either:

- destruction of records; or
- transfer of records to archives.

Where Personal Information is destroyed the following information must be recorded in a disposition of records log:

- the identity of 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.

The Division shall not destroy any record with the intent to evade a request for access under *The Personal Health Information Act*.

Cumulative and Pupil Support File Destruction

Destruction must be carried out in a manner that protects the privacy of the student. Wherever possible, the Division will shred or will cause to be shredded records that are to be destroyed and a disposition of records is to be maintained.

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; and
- 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 administrative security officer will be the Secretary-Treasurer or designate, who may delegate to the School Leader or site manager as they see fit, who shall 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, or any combination thereof.

The administrative security officer must maintain a duplicate key for each office at the Brandon School Division head office and each School Leader or site manager must maintain a duplicate key for each office within their respective school or site.

Electronic doors, if applicable, must not be left open while the area is unattended and 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 information must be cleared from the desktop at the end of the day and placed in a secure location such as a locked filing cabinet.

Portable computers must be secured in a locked area when not in use and sensitive data on the hard drive must be secured by password protection.

Pupil Files are not to be removed from the work site by any staff member except for the purpose of transferring the record to the Division Office. The staff member transporting the files is responsible for ensuring an appropriate level of security and confidentiality at all times the file is in their possession. Records are not to be left unattended or unsecured while being transported.

Notwithstanding the foregoing, pupil course work and information, such as essays, projects, tests, and results of assessments may be removed from the work site for the purpose of marking, programming, and evaluating. The staff member transporting the course work is responsible for ensuring an appropriate level of security and confidentiality at all times the file is in their possession. Course work and information is not to be left unattended while being transported and will be treated to the same level of security as they normally would if located within the Division. No student's personal health information shall be maintained on the personal home computer of the employee.

Notwithstanding the foregoing, in the event of an emergency where there is risk of the Pupil File being damaged or destroyed a staff person may remove the Pupil File from any school or office of the Brandon School Division where that risk exists provided they, as soon as practicable, transport the file to another school or office of the Brandon School Division where it may be secured in accordance with this procedure.

Notwithstanding the foregoing, any member of Senior Administration of the Division may remove the whole or any part of the student Pupil File from any school or office of the Brandon School Division if it is being removed for the purpose of obtaining legal advice on the contents thereof. In that event, the member of Senior Administration transporting the files is responsible for ensuring an appropriate level of security and confidentiality at all times the file is in their possession and that a log is created and maintained which records the name of the student, date file removed, date returned, location of file and information taken. Records are not to be left unattended while being transported.

Notwithstanding the foregoing, the Administrator of Student Achievement Support Services or delegate may remove Pupil Support Files from the Division Office for the purpose of planning individual student plans with the relevant school. In this case only the minimum amount of information that may reasonably be required may be removed and a log stating the name of the student, information removed from file, date out and date in will be maintained in the Pupil File.

Transmission of Confidential Information

When confidential information is requested over the telephone it may only be released if the requesting party's contact information correlates to the contact information on the student's registration form and the requesting party is entitled to access to the information. Confidential information that is requested by outside agencies such as Child and Family Services over the telephone shall only be released if the person requesting the information is known to the employee. If the person is not known to the employee, then no confidential information shall be released over the telephone unless the identity of the caller is verified.

Notwithstanding the foregoing, due to students safety concerns and issues, any employee working in Transportation Services may confirm whether a child made or missed their bus over the phone if the employee is reasonably satisfied of the identity of the caller and that the caller is entitled to receive said information.

No confidential information shall be left on an answering machine or by voicemail unless the identity of the receiving party is known. Further, it is the responsibility of the staff member to ensure the confidentiality, the authenticity and the appropriateness of the venue of communication.

Nothing in this section shall limit an employee's ability to telephone a student's contact person in the case of an emergency arising from a medical, health or safety concern.

Confidential information must be faxed only when required for urgent or emergent purposes and only sent under the following conditions:

- there is no reasonable possibility that the information being transmitted can be intercepted during transmission by unauthorized personnel;
- the individual sending the fax is authorized to release the information;
- the 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.”; and
- to the extent possible, a designated recipient must be available to receive faxes containing Personal Health Information and that recipient shall be contacted prior to the fax being sent.

Transmitting confidential information via e-mail must only be done if the venue of transmission is secure or the data is encrypted.

Electronic Security

The Division’s electronic security officer will be the Secretary-Treasurer or designate who may delegate duties as they see fit. The Division’s electronic security officer is responsible for ensuring that the following is adhered to:

- shared USERID’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. The electronic security officer must approve sharing of USERID’s and passwords, a listing of which be maintained;
- USERID or password must not be shared with anyone except as may be necessary for authorized personnel to perform maintenance on the Personal Computer in which case the password must be changed as soon as the maintenance is performed;
- the electronic security officer must delete an employee’s USERID from the system as soon as possible after the termination of the individual’s employment with the Division;
- USERID or password must not be taped to a computer or left where it is easily accessible;
- the electronic security officer shall be responsible for maintaining a listing of such USERID’s and passwords for the staff as may be reasonably necessary to maintain the computer system and network of the Division; and
- information must be encrypted; where feasible, when transporting electronic information on portable computers.

Employees shall be responsible for logging out of the computer system at the end of each work day. Employees must also log out or utilize password access when the computer will not be in use for a period exceeding 10 minutes.

Additional Safeguards for Electronic Health Information System

The Division's electronic security officer or designate shall ensure every electronic information system that the trustee designs or acquires after December 11, 2000

- produces an electronic record of every successful or unsuccessful attempt to:
    - gain access to the Personal Health Information maintained on the system;
    - add to, delete or modify the Personal Health Information maintained on the system; and
- records every transmission of Personal Health Information maintained on the system.

The Division's electronic security officer or designate shall regularly review the electronic records as produced above to document and detect any security breaches.

The requirements of this paragraph only apply to an electronic information system used by a trustee to maintain Personal Health Information.

Reporting Security Breaches

Any security breaches involving Personal Health Information are to be immediately reported:

- to the School Leader if the breach occurs at school. The School Leader is then to inform the Divisional Privacy Officer using the Divisional "Incident Report" form, a copy of which is to be forwarded to the Assistant Superintendent; and
- to immediate supervisors if the breach is identified by a Divisional employee. The immediate supervisor is then to inform the Privacy Officer in writing of the breach.

The Privacy Officer will investigate all security breaches and recommend corrective procedures and/or discipline measures, where appropriate, 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.

The 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 Health Information necessary for the provision of educational services to that pupil is forwarded.

Under *The Public Schools Act,* a Principal must forward the Pupil File when the student transfers out of the school and enrolls in another school. All Pupil File records 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. Instead these notes 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;
- confidential information about a third party;
- unsigned/undated notes;
- other agency information that does not pertain to schooling and provision of educational services; and
- third-party reports not generated by the Brandon School Division.

Personal notes and records of teachers, counselors and administrators must be kept for a period not to exceed the end of the school year in which the student departed, after which time they will be destroyed in conjunction with the provision of this Administrative Procedure, the Division's existing Administrative Procedure entitled "*Records Retention and Disposition*" and the existing guidelines established by Manitoba Education entitled "*Guidelines on the Retention and Disposition of School Division/District Records*". Notwithstanding the foregoing, personal notes may be kept for a longer period of time if there are reasonable grounds to believe that such notes will be required in the future. This might include their use for legal, administrative or disciplinary purposes or review. Notes that are retained in accordance with this provision shall be forwarded to the Administrator of Student Achievement Support Services and shall be retained for such period of time as the Administrator of Student Achievement Support Services sees fit. Such notes will be maintained in a secure location.

Records that are removed in the culling process are to be shredded on site as soon as possible. The School Leader is responsible for ensuring that the files are shredded on site at the end of the retention period in such a way that protects the file from unauthorized access, disclosure, loss or destruction. File material that is culled from the Cumulative File and Pupil Support File must be listed for content. The summary will be kept on file as part of the disposition system with a copy of the listing being forwarded to the records manager. Following the review of the file the Index for each file shall be updated if necessary.

The Divisional Level Pupil File component should be transferred from professional to professional through the Student Achievement Support Services Department of each

school division whenever possible. The Cumulative and School Pupil Support File will be transferred from school to school within the Division whenever possible, and the School Leader will be responsible to supervise the transfer of the same.

The School Leader must keep a record of the file management system and forward a copy of the record management upon the destruction of the record.