FORT LA BOSSE SCHOOL DIVISION

TITLE – **SCHOOL DIVISION RECORDS MANAGEMENT*** POLICY - **EHBA-R**

Approval Date - 21/08/07 Cross Reference -

Resolution # - 282/07 Implementation - 21/08/07

Legal Reference - Last Reviewed - 27/10/08

RECORDS MANAGEMENT POLICY

Responsibility for Records Management

The records manager/security officer for the school division/district will be the Secretary Treasurer who may delegate duties as necessary.

Each school, site or department 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 file index of 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.
* Retaining electronic data.
* Disposing of files and records.
* Ensuring that an audit trail is maintained 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.)

…2

FILE CONTROL PROCEDURE

Retention and Destruction of Records

At the expiration of the retention period, records will be destroyed centrally under controlled confidential conditions unless deemed archival. These records are to be forwarded to the Division Board Office with a list or summary of contents to 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.

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.

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 administrative security officer must ensure that a locked environment is established where personal health information is stored or accessible. This could mean a whole wing, a room or a filing cabinet.

* The administrative security officer 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.

…3

* 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 secured; this is, 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.

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 purpose 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 indicate, where applicable, "confidential information and 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 the fax containing personal health information.

* Transmitting information via email must only be done if the venue of transmission is secure or the data is encrypted.

…4

Electronic Security

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. 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 PC in which case the password must be changed as soon as the maintenance is performed.

* The Electronic Security Officer must delete USERID as soon as it is known that an individual is leaving.

* USERID or password must be not taped to computer or left where it is easily accessible.

* The Electronic Security Officer must be responsible for maintaining a listing of all USERID's/passwords for its staff.

* Employees must be responsible for logging out of the computer system each evening.

* Information must be encrypted, where feasible, when transporting electronic information on portable computers.

* Physical information, 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.

…5

Reporting Security Breaches

* Any security breaches involving personal health information are to be immediately reported:

  A. to the school if the breach occurs at school. The Principal is then to inform the Divisional Privacy Officer using the divisional "Incident Report" form.

  B. to immediate supervisors if the breach is identified by a divisional employee. The immediate supervisor is then to inform the divisional Privacy Officer using The divisional "Incident Report" form.

  C. the Privacy Officer 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.

* Fort La Bosse 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 practical.

…6

ACCESS AND PRIVACY

Administrative Security

* Human Resources must ensure that each new employee sign a pledge of confidentiality. Before this pledge is executed the employee must be provided with a copy of the Division's Records Management Policies to protect Personal Health Information and procedures by way 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.

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 provided under Subsection 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. Young Offender 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 the safety of staff, students and others.

For further information on Access and Privacy please see pages 13-20 of the Manitoba Pupil File Guidelines.

…7

STATUTORY DEFINITION OF PERSONAL HEALTH INFORMATION

"personal health information" means recorded information about an identifiable individual that relates to:

(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,

and includes

(d) the PHIN 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.

"health care" means any care, service or procedure

(a) provided to diagnose, treat or maintain an individual's physical or mental condition,

(b) provided to prevent disease or injury or promote health, or

(c) 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.

"PHIN" means the personal health identification number assigned to an individual by the minister to uniquely identify the individual for health care purposes.

…8

PLEDGE OF CONFIDENTIALITY

As an employee of Fort La Bosse School Division, I acknowledge and understand that I may/will have access to personal health information (statutory definition attached) about others, including students, the confidentiality and protection of which is governed by The Personal Health Information Act (the Act).

I further acknowledge and understand that the School Division has established written policies and procedures containing provisions for the security of personal health information in the Division's possession during its collection, use, disclosure, storage and destruction; provisions for the recording of security breaches; and corrective procedures to address security breaches.

I further acknowledge that I have been provided orientation and that I have received or will receive ongoing training about these policies and procedures.

I acknowledge that I am bound by the policies and procedures established by the School Division in accordance with the Act and I am aware that a consequence of breaching them is prosecution under the Act, and/or disciplinary action.

_____ _____

(Date signed) (Signature)

_____

(Print name and position – Teacher, E.A., etc.)

…8