SCHOOL DIVISION RECORDS MANAGEMENT

Responsibility for Records Management

The records manager/security officer for the school division 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 person to the following tasks:

- 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 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.

Disclaimer

The following disclaimer is to be included on all application forms, referral forms, reports, or any form where personal health information is being collected.

> This personal information, or personal health information, is being collected under the authority of Seine River 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. If you have any questions about the collection, contact the Seine River School Division Access and Privacy Coordinator at 878-4713.

APPROVED:
REVISED: February 2004
SOURCE:
OTHER REFERENCE:

Managing Pupil Files

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
- Young Offender Information
- Third Party Information (e.g. psychological assessment done in another school division)

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 into sub-files by three components: the cumulative file, pupil support file and Young Offender 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.
- Behavioral 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.
- 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 service psychological/psychiatric or counseling resources.

Pupil Support file (some students – see Student Services Handbook)

- Exists for some students (e.g. clinical file).
- Information about a student may be held in more than one location if a system of cross-reference is in place (e.g. Student Services clinical master file).
- 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.

APPROVED:
REVISED: February 2004
SOURCE:
OTHER REFERENCE:

- Results of specialized diagnostic tests.
- Service provider reports.
- Individualized Education Plan and/or Health Care Plan.

Young Offender File (some students)

- Exists only for a few students.
- Access, disclosure, retention and destructions as set out in the Young Offenders 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 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.

APPROVED:
REVISED: February 2004
SOURCE:
OTHER REFERENCE:

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;

Cumulative and Pupil Support File – Retention

- Except for Senior 1-4 marks, information in the pupil file should be retained for a minimum of ten (10)years after the student ceases to attend school or until the file is transferred to another school.

- Senior 1-4 marks should be retained for thirty (30) 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.

Young Offender File – Retention and Destruction

The Young Offender File must be destroyed when it is no longer required for the purpose for which it was established (e.g., the need to comply with a court order, or when safety was no longer an issue.) **IF THE STUDENT TRANSFERS TO ANOTHER SCHOOL DIVISION OR DISTRICT THE FILE MUST BE DESTROYED.**

APPROVED:
REVISED: February 2004
SOURCE:
OTHER REFERENCE:

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 (Maintenance Supervisor) 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 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.
- 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; that is, encrypted where feasible. At a minimum, sensitive data must be password protected.
- 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 (ie. 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 requested is verified. This information must not be left on the answering machine.

APPROVED:
REVISED: February 2004
SOURCE:
OTHER REFERENCE:

- 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", and

  - 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 Division's electronic security officer (Information Systems Technology Coordinator) 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 is to 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 not be 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.

APPROVED:
REVISED: February 2004
SOURCE:
OTHER REFERENCE:

- Information must be encrypted, where feasible, when transporting electronic information on portable computers. At a minimum, sensitive data must be password protected.

Reporting Security Breaches

- Any security breaches involving personal health information are to be immediately reported.

  A. To the school principal 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.

- 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.

- Seine River 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 (Refer to Student Services Handbook)

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, 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 that student.

- Irrelevant or outdated student work samples with the exception of those samples needed for future programming.
-
- Information about a third party.
-

APPROVED:
REVISED: February 2004
SOURCE:
OTHER REFERENCE:

- 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 material to be destroyed.

Please also note the following:

- A principal must forward the pupil file when the pupil transfers out of the school and enrols in another school (M.R. 468/88).
- The YOA does not permit the transfer of the Young Offender File component outside of the school division/district.
- FIPPA and PHIA allow for the transfer of the personal and personal health information in the cumulative file component and the pupil support file (clinical 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 Service Department).
- The Young Offender File may not 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.

APPROVED:
REVISED: February 2004
SOURCE:
OTHER REFERENCE:

ACCESS AND PRIVACY

Administrative Security

Human Resources must ensure that each new employee signs 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 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 pupil files. 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 Young Offender 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,
- A list of those entitled to access should be attached to the Young Offender 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.

Note: 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 Young Offender file to the pupil.

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.

Divorced/separated parents have the right to receive information as to the health and education of their child unless the court orders otherwise.

School divisions are not authorized to disclose information in the Young Offender file to the parent/guardian.

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. 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 pleas see pages 13-20 of the Manitoba Pupil File Guidelines.

APPROVED:
REVISED: February 2004
SOURCE:
OTHER REFERENCE:

STATUTORY DEFINITION OF PERSONAL 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:

The PHIN 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.

"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.

APPROVED:
REVISED: February 2004
SOURCE:
OTHER REFERENCE: