The Pine Creek School Division accepts as policy the practices and procedures outlined in Manitoba Education, Training and Youth's Guidelines on the Retention and Disposition of School Division/District Records and Manitoba Pupil File Guidelines. It shall ensure compliance with the *Freedom of Information and Protection of Privacy Act* (FIPPA), the *Personal Health Information Act* (PHIA), and the *Young Offenders Act* (YOA) respecting the collection, use, disclosure, security, retention, and destruction of personal and personal health information.

Responsibility for Records Management

The Records Manager/ Security Officer for the Division will be the Secretary-Treasurer, who may delegate duties as necessary.

Each school, site, or department is responsible for the 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:

a) General filing of hard copy materials.
b) Updating of the file index for all items, providing all the data required for the index such as category, name, location, etc.
c) Ensuring that copies of appropriate reports and documents are forwarded for archival storage.
d) Retaining electronic data.
e) Disposing of files and records.
f) Ensuring that an audit trail of filing activity is maintained (transfers, disposals, loans, etc.)
g) Other filing and record-keeping tasks as assigned.

For specific information regarding Student Records see Pupil Files.

Ownership of Records

All files are the property of the Pine Creek School 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 divisional application forms, referral forms, reports, or any form where personal or personal health information is being collected. For a definition of personal information, see Section D. For a definition of personal health information, see Pledge of Confidentiality.

This personal information, or personal health information, is being collected under the authority of Pine Creek 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 Pine Creek School Division Access and Privacy Coordinator at 385-2216.

Retention and Destruction of Records

At the expiration of the retention period, records will be destroyed under controlled confidential conditions, unless they are deemed archival. These records are to be forwarded to the Division 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 the person supervising the destruction.

Archival Option

Permanent records should be moved into the archives designated in the Retention and Disposition Schedule of the Guidelines.

Archival options include:

a) Provincial Archives of Manitoba - The Archives legislation enables the Division to transfer its permanent records to the Provincial Archives.
b) 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

a) The Division's Security Officer must ensure that a locked environment is established where all confidential information, including personal health information, is stored or accessible. This could mean a whole wing, a room, or a filing cabinet.
b) The Security Officer must maintain a duplicate key for each office.
c) Electronic doors, if applicable, must not be left open while the area is unattended; combinations must not be disclosed to unauthorized personnel.
d) Materials dealing with confidential information must be closed and not left open for viewing when away from the desk or work area. Confidential material must be cleared from the desktop at the end of the day.
e) Portable computers must be locked away when not in use, and sensitive data on the hard drive must be secured; that is, encrypted.
f) 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.
g) 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

a) 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.

b) 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".

c) 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 Security Officer is responsible for ensuring that the following is adhered to:

a) 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 Security
b) Officer must approve sharing of USERID's and passwords, a listing of which must be maintained.
c) 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.
d) The Security Officer must delete USERID as soon as it is known that the individual is leaving.
e) USERID or password must not be taped to computer or left where it is easily accessible.
f) The Security Officer must be responsible for maintaining a listing of all USERID's passwords for its staff.
g) Employees must be responsible for logging out of the computer system each evening.
h) Information must be encrypted, where feasible, when transporting electronic information on portable computers.

Reporting Security Breaches

Any security breaches involving personal or personal health information are to be immediately reported to the Principal or immediate supervisor, who will inform the Privacy Officer. The Privacy Officer will investigate all security breaches and recommend corrective procedures to address security breaches.

Reasonable Precautions

Reasonable precautions are to be taken to protect personal and personal health information material from fire, theft, vandalism, deterioration, accidental destruction or loss, and other hazards.

The Pine Creek School Division shall review its security safeguards at least every two years, and shall take steps to correct any deficiencies as soon as practicable.

References

References requested regarding an employee's or prior employee's work record in the Division shall be completed by the Superintendent or designate. Provisions of the *Personal Investigations Act* shall apply. References shall only be provided in confidence.

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
f. provided to diagnose, treat or maintain an individual's physical or mental condition,
g. provided to prevent disease or injury or promote health, or
h. the affects that 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.