EHB–R2

GUIDELINES FOR RECORDS MANAGEMENT – PROPERTY AND TRANSPORTATION

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. The school will designate a staff person to attend to the following tasks:

- General filing of hard copy materials
- Updating of the 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 of filing activity is maintained (transfers, disposals, loans, etc.)
- Other filing and record-keeping tasks as assigned

NOTE: For specific information regarding Student Records (Pupil Files) see Procedure JRA.

Ownership of Records

All files are the property of the Sunrise 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 must 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 Procedure JRA. For a definition of personal health information see GBJA.

> This personal information or personal health information is being collected under the authority of Sunrise 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 Sunrise School Division Access and Privacy Coordinator at 204-268-6500.

Retention and Destruction of Records

At the expiration of the retention period, records will be destroyed centrally under controlled confidential conditions, unless they are deemed archival. These records will be forwarded to the Division Office, and a list or summary of contents will be sent to the Records Manager. The Records Manager will file the summaries or lists in a Disposition of Records log. Disposition is either the destruction of records or the 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 part of 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 Records Management Schedule (EHB-E). 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 Security Officer must ensure that all confidential information, including personal health information, is stored and accessible in a locked, secure environment. This environment could be a whole wing of a building, a room or a filing cabinet.
- The Security Officer will maintain a duplicate key for each office or cabinet.
- 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 when away from the desk or work area. Confidential material will be cleared from the desktop at the end of the day.
- Portable computers will be locked away when not in use, and sensitive data on the hard drive will be secured (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. They must be locked in the trunk of the vehicle or placed in an inconspicuous location if the vehicle has no trunk.

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 an answering machine.
- Confidential information must be faxed only when required for urgent or emergent purposes and may only be sent under the following conditions:
    - If there is no chance the information being transmitted can be intercepted by unauthorized personnel
    - The individual sending the fax is authorized to release the information
    - The cover page of the 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.”
- Transmitting information via email 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:

- Shared user IDs and passwords must only be assigned where it is not possible to assign an individual user ID (e.g., because of degradation of service to the public). The Security Officer must approve sharing of user IDs and passwords and must maintain a list of these.
- The user ID or password must not be shared with anyone, unless authorized personnel need to perform maintenance on the PC. In this case the password must be changed as soon as the maintenance is performed.
- The Security Officer must delete the user ID as soon as they know the individual is leaving.
- The user ID or password must not be taped to the computer or left somewhere where it is easily accessible.
- The Security Officer is responsible for maintaining a listing of all user IDs and passwords for staff.
- Employees are responsible for logging out of the computer system each evening.
- Where possible, information must be encrypted when transporting electronic information on portable computers.

Reporting Security Breaches

Any security breaches involving personal or personal health information must 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 these breaches.

Reasonable Precautions

Division staff must take all reasonable precautions to protect personal and personal health information material from fire, theft, vandalism, deterioration, accidental destruction or loss and other hazards.

Sunrise School Division will review our security safeguards at least every two years and will take steps to correct any deficiencies as soon as practicable.

Cross Reference:		
Date Adopted: August 1, 2017	**Date Amended:**	**Board Motion(s):**
Procedure: EHB	**Guidelines:** EHB-R1	**Exhibit:** EHB-E