School District Records Management

Administrative Procedure 5.140

Board Governance Policy Cross Reference: Policy 1, 2, 3, 16, 17
Legal Reference: Freedom of Information and Protection of Privacy Act (FIPPA), Personal Health Information Act (PHIA), Youth Criminal Justice Act (YCJA), PSA- Appropriate Educational Programming Regulation 155/2005, EAA Regulation 156/2005

Date Adopted: June, 2012
Date Amended: September, 2012; January, 2018; April, 2020; April, 2023
Date Reviewed: October, 2022

*** This procedure does not apply to the electronic version of student records. ***

The School District of Mystery Lake is the custodian of a large amount of personal and personal health information. The District, as a public body, is responsible for protecting this information from unauthorized release or access.

The implementation of efficient records management, particularly in light of technological change, enables districts to discharge their responsibilities to ensure both access to and protection of information. The School District of Mystery Lake accepts as policy the practices and procedures outlined in Manitoba Education and Training's Guidelines on the Retention and Disposition of School Division/District Records and Manitoba Pupil File Guidelines, and shall ensure compliance with the Freedom of Information and Protection of Privacy Act (FIPPA), the Personal Health Information Act (PHIA) and the Youth Criminal Justice Act (YCJA).

The following policies and procedures are designed to comply with the policy requirements of The Personal Health Information Act respecting collection, use, disclosure, security, retention and destruction of personal health information.

I. 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 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 archived.
- Retaining electronic data.
- Disposing of files and records.
- 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 District. 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 or personal health information is being collected in the School District of Mystery Lake.

> This personal information, or personal health information, is being collected under the authority of the School District of Mystery Lake 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.

II. Managing Pupil Files

Definitions

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
- Youth Criminal Justice Information
- Third Party Information

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 Youth Criminal Justice file. All are

considered part of the pupil file for definition, collection, access, retention, destruction or transfer considerations.

Cumulative File (all students)

A) Contents

Standard or routine information that schools have on **all** pupils.

- The student's name as registered under The Vital Statistics Act or, if the student was born in a jurisdiction outside Manitoba, the student's name as registered in the jurisdiction, and any other names/surnames by which the student is known
- Current registration form
- An annual summary or a summary at the end of each semester or term of the student's achievement or progress in the courses and programs in which the student is enrolled (i.e. report cards/transcripts)
- The names of all schools attended by the student and the dates of enrollment, if known
- Attendance records
- Photographs
- Communication regarding the student between the home and school e.g. discipline, behavior, achievements, etc.
- Behavioral misconduct information including suspensions/expulsions.
- Child custody, guardianship agreements or orders.
- Home/school communications.
- The results obtained by the student on any diagnostic test, achievement test or examination conducted by or on behalf of the Province, and standardized tests under any testing program administered by the board to all or a large portion of the students or to a specific grade level of students
- Indications of awards/prizes
- Any other assessment or evaluation that the parent or the student wishes to be placed in the cumulative file
- There could also be personal health information in a pupil file
- 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 services, psychological/psychiatric or counseling resources.

B) Security

The cumulative file requires the lowest level of security and may be located in a secured area of the school.

Pupil Support File (where applicable)

A) Contents

The Pupil Support File exists for some students and will typically include:

- Behaviour Intervention Plans
- Detailed documentation from school clinicians and special education / resource staff about all inter-agency contacts and the provisions of any other resource services from within or outside the school division that are occurring.
- Ongoing health/psycho-social/counseling information, whether medical, psychological and behavioural. (Schools should endeavor to ascertain at point of first admission whether students have used or are continuing to use social service, psychological. psychiatric, counselling resources of any professional, or any agency, or of any school previously attended).
- School clinician reports/correspondence/logs/notes from meetings/discussions concerning intervention strategies, contact logs and consultation notes
- Results of specialized diagnostic tests.
- Service provider reports such as agencies, hospitals and clinics
- The most recent Individualized Education Plan and/or Health Care Plan specifically devised for a student and any amendments to these plans.
- Provincial funding applications
- Summative report of school counselor or resource involvement

B) Security

The information comprising the Pupil Support File should be kept in a secured area. Pupil support information may be held in more than one location within a school district. For example, there may be pupil support information on an individual in the school counselor's office as well as the resource teacher's office. Arrangements such as this are acceptable as long as documentation identifying that information on the pupil is being held in separate locations is recorded in the pupil's Cumulative File.

Youth Criminal Justice File (where applicable)

A Youth Criminal Justice File will only exist where a court may provide information on a youth for the purpose of assisting the school:

- in its attempts to deal with a violent or dangerous offender, or to maintain a safe and orderly environment for other students and staff;
- in monitoring an offender's compliance with conditions of bail, probation or release; and/or
- in providing 'pre-sentencing' information to the court

A) Contents

File contents will typically include:

- The type of youth court order with which the young person is expected to comply (i.e. bail, probation, conditional supervision, temporary release)
- The expected expiry date of the court order
- The offence for which the order has been made
- The particular terms of the order which relate to school attendance or any other education matter
- Prior record of offences if safety of staff and students may be at risk
- Any identifiable individual or group of persons who could be at risk from the young offender
- Patterns of behavior which may signal the onset of activity which might affect safety
- Any recommendations for reducing the risk of violence and increasing the level of safety

B) Security

The Youth Criminal Justice File has the highest level of security. Records should be kept in a locked cabinet, under the control of designated staff (i.e. the principal in the case of records kept at the school).

C) Access and Privacy

The consequences for inappropriate disclosure of information are severe and could result in fine or imprisonment.

Access is on a strict ‘need-to-know’ basis only. To ensure that privacy interests of students are appropriately protected, The Young Offenders Act provides that disclosed information about a young offender shall be kept separate from the Cumulative and Pupil Support File and from any other record accessible to other staff.

The Act does not authorize a school division or district to disclose young offender information in a pupil file to the young offender, or to the parent/guardian. It is recommended that principals of schools, in keeping with their responsibilities for pupil files, be designated as the custodian for the young offender information and bear responsibility for the receipt and release, maintenance, protection and security of young offender information.

D) Transfer, Retention and Destruction

The Youth Criminal Justice File must be destroyed as soon as it is no longer required for the purpose for which it was established. If the student transfers to another school division, the file must be destroyed immediately. Justice officials must be advised that the student is no longer attending the school. It is the responsibility of justice officials to advise the new school of any pertinent information. School officials may recommend to justice that the information be transferred and if possible, should provide the name(s) of an appropriate officer in the new school authority for justice officials to contact.

Pupil File Annual Review Procedures

The following guidelines and procedures apply to an annual review and culling of all components 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 to the school board office. The summary will be kept on file as part of the disposition system.

III. 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 School Board Office.

Disposition is either:

- Destruction of records, which will be by shredding, 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 Grades 9-12 marks, information in the pupil file should be retained for a minimum of ten years after the student ceases to attend school or until the file is transferred to another school.
- Grade 9-12 marks should be retained for thirty years.
- Following the retention period, records are destroyed via shredding.

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.

Youth Criminal Justice File – Retention and Destruction

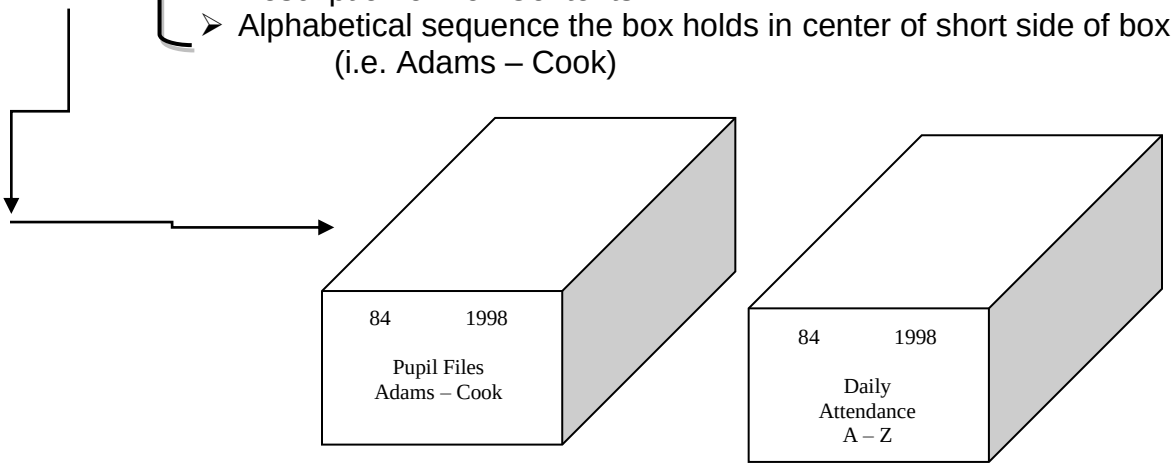
The Youth Criminal Justice File must be destroyed when it is no longer required for the purpose for which it was established, i.e.:

- To ensure the young person follows the conditions of reintegration leave, or an order of the youth justice court, such as bail or probation conditions;
- To ensure the safety of school staff, students or other persons; or
- To facilitate the rehabilitation of the young person.

Note: IF THE STUDENT TRANSFERS TO ANOTHER SCHOOL DIVISION OR DISTRICT, THE YCJA FILE MUST BE DESTROYED BY SHREDDING.

Boxing/Transfer

- Culled pupil files are to be boxed alphabetically in standard sized storage boxes.
- For each box, compile a list detailing the contents (include student's last name, first name, date of birth and first and last years attended).
- Indicate the following on the storage box:
  - School number in upper left hand corner of short side of box
  - Last year attended in the upper right hand corner of short side of box
  - Description of Box Contents
  - Alphabetical sequence the box holds in center of short side of box (i.e. Adams – Cook)



- Complete a Records Transfer Box List. (Appendix 4)

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.
- District Archives – District 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 district archives.

Physical Security

- The District's administration 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.
- The administrative security office 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 password protected or 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 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 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 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”;
  - 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 District’s electronic security officer is responsible for ensuring that the following is adhered to:

- Shared USER ID’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. I.T. must approve sharing of USER ID’s and passwords, a listing of which be maintained.
- USERID and 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 I.T. Department 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 I.T. Department must be responsible for maintaining a listing of all USER ID’s/passwords for district staff.
- Employees must be responsible for logging out of the computer system each evening.
- Information must be password protected or encrypted, where feasible, when transporting electronic information on portable computers.

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 District Privacy Officer.
  b) To immediate supervisors if the breach is identified by a district employee. The immediate supervisor is then to inform the District Privacy Officer.

- 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.

IV. Pupil File Transfer Procedures

- 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, counselor, 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.
  - 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, counselors 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 materials to be destroyed.

Please also note the following:

- A principal must forward the pupil file when the pupil transfers out of the school and enrolls in another school (M.R. 468/88).
- A principal must provide the pupil file of a pupil who has transferred to another school to that school within one week of the school requesting it (M.R. 156/05).
- When a pupil transfers into a school, he/she cannot be denied educational programming for more than 14 days regardless of whether that school has receive the pupil's pupil file. An exception is risk of safety (M.R. 155/05).
- FIPPA and PHIA allow for the transfer of the personal and personal health information in the cumulative file component and the pupil support 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 Services Department).
- The YCJA does not allow for the Youth Criminal Justice File to 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.

V. Access and Privacy

Administrative Security

School Divisions must ensure that each new employee signs a pledge of confidentiality. (Appendix 1) Before this pledge is executed the employee must be provided with a copy of the Division's Records Management Procedures to Protect Personal Health Information 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.

Access to information in the Youth Criminal Justice 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, or
- To facilitate the rehabilitation of the young person.
- A list of those entitled to access should be attached to the Youth Criminal Justice 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 districts are not authorized to disclose information in the Youth Criminal Justice file to the pupil or to the parent/guardian.

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. Pupils age18 years or older must indicate whether they allow their parent/guardian access to their pupil file (See Appendix 2).

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

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 (Appendix 3). 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. Youth Criminal Justice 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 safety of staff, students and others.
- To facilitate the rehabilitation of the young person.

For further information, please see the Manitoba Pupil File Guidelines.

APPENDICES

Appendix 1

School District of Mystery Lake
PHIA PLEDGE OF CONFIDENTIALITY

As an employee of the School District of Mystery Lake, 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 District has established written policies and procedures containing provisions for the security of personal health information in the District'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 read procedure 5.110, and 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 District 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)	(Position – Teacher, E.A., , Etc.)

This personal information, or personal health information, is being collected under the authority of the School District of Mystery Lake 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.

STATUTORY DEFINITION OF PERSONAL HEALTH INFORMATION

"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 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

- Provided to diagnose, treat or maintain an individual's physical or mental condition,
- Provided to prevent disease or injury or promote health, or
- 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.

(Attachment To Pledge)

Appendix 2

School District of Mystery Lake

ACCESS TO PUPIL INFORMATION
Pupils 18 Years of Age or Older

Consent to Disclose Personal Information to Parents/Guardians

_____ _____ _____
Student's Legal Last Name First Name Middle Initial

Date of Birth: _____ _____ _____
Year Month Day

☐ I give _____ permission to release
(name of school)
information, such as academic progress, attendance records and conduct reports to my parent(s)/guardian(s).

☐ I do not give _____ permission to release school-
(name of school)
related information, such as academic progress, attendance records and conduct reports to my parent(s)/guardian(s).

Parent/Guardian Name: _____

Parent/Guardian Address: _____

Town: _____ Postal Code: _____ Phone: _____

Dated this _____ day of _____, 20_____.

Student Signature: _____

Witness (18 years or older): _____

Note: This release form must be signed on or after the student's 18th birthday and returned to the School Administration Office.

This personal information, or personal health information, is being collected under the authority of the School District of Mystery Lake 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.

Appendix 3

School District of Mystery Lake

AUTHORIZATION FOR RELEASE OF INFORMATION

Student: _____

Birthdate: _____ Age: _____

School: _____ Grade: _____

Date: _____

I, _____, being parent/legal guardian of _____
(child's name)
do hereby authorize _____ to release
(School Division/Agency/Clinic)
information pertaining to _____
_____
_____
_____
_____
with the School District of Mystery Lake.

THIS INFORMATION IS TO BE RELEASED TO:

Student Services Coordinator/Principal/Resource Teacher
School District of Mystery Lake
408 Thompson Drive, Thompson, MB R8N 0C5
Fax: (204) 677-9528

This information is confidential and to be used for the purpose of providing a service to the above-named child.

_____ _____
(Date) (Signature of parent/legal guardian)

This personal information, or personal health information, is being collected under the authority of the School District of Mystery Lake 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.

School District of Mystery Lake

AUTHORIZATION FOR RELEASE OF INFORMATION

Student: _____

Birthdate: _____ Age: _____

School: _____ Grade: _____

Date: _____

I, _____, being parent/legal guardian of _____
(child's name)
do hereby authorize _____ to release
(School Division/Agency/Clinic)
information pertaining to _____
_____
_____
_____
_____ .

THIS INFORMATION IS TO BE RELEASED TO:

_____

_____

_____

_____

This information is confidential and to be used for the purpose of providing a service to the above-named child.

_____ _____
(Date) (Signature of parent/legal guardian)

This personal information, or personal health information, is being collected under the authority of the School District of Mystery Lake 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.

Appendix 4

Records Transfer Box List

School	Area (Finance, Personnel, Student)
Disposal Action (Circle) Destroy Storage	

Box Contents

Temp Box #	Dates (Year) From	Dates (Year) To	MET #'s	Cumulative File	Pupil Support File	Both

I confirm that the disposal action and the contents listed above are in accordance with the records retention guidelines of The School District of Mystery Lake Administrative Procedures.	Report Compiled By: _____ Date:
Authorizing Signature: _____	Date:
Destruction Complete: _____ Secretary-Treasurer	Date: