BUSINESS AND BOARD ADMINISTRATION | *3000*

PRIVACY AND INFORMATION MANAGEMENT PROCEDURES | *3092*

1. Policy

It is the policy of Lakehead District School Board (LDSB) to collect, use, retain and disclose personal information in the course of meeting its statutory duties and responsibilities. Lakehead District School Board is committed to the protection of privacy.

2. Definitions

2.1 General Information

General information refers to recorded information in the LDSB's custody and/or control that is not of a personal nature and is not exempt from public access under the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) unless an access exemption under this or other legislation applies. Examples of general information that can be routinely released include: LDSB and Ministry policies, guidelines and memorandum, or information on school events and programs.

2.2 Personal Information

Personal information is any recorded information that renders an individual identifiable. Examples of personal information that need protection include: Ontario Student Records, psychological and other health related assessments, student discipline related information, staff banking information, vendor and supplier resumes. Note that most employment related and employee related information is excluded from the access provisions of MFIPPA.

2.3 Record

Any record of information, however recorded, whether printed, on film, by electronic or other means. Examples include: written correspondence, pictures/photographs, sound and video recordings.

3. Accessing General Records

In general, staff, students and the general public shall be granted access to general information by making a formal application under MFIPPA:

- all requests should be forwarded to the Freedom of Information (FOI) Officer; and
- if a formal request requires extensive research and/or photocopying, fees may be charged consistent with the fee schedule set out in MFIPPA and its regulations.

4. Collecting and Accessing Personal Information

4.1 In accordance with MFIPPA, when personal information is collected on behalf of the Board, the Board shall inform the individual of:

- the legal authority for the collection;
- the principal purpose(s) for which the information is to be used; and
- the person to contact should additional information be required regarding the collection.

4.2 Physical records of personal information shall be secured in locked cabinets or otherwise controlled within a restricted area. Strong computer passwords or pass phrases containing letters, numbers and special characters should be used as appropriate. Where possible, multi-factor authentication should be used along with passwords to provide additional security.

4.3 Personal Information shall be stored by LDSB until such time as legislated under the appropriate Act, or in line with LDSB retention schedule. When required to dispose of personal information, LDSB shall do so in a manner that irreversibly destroys the media which stores personal information, so that it cannot be reconstructed or recovered in any way.

4.4 Access to personal information shall be restricted to:

- the individual about whom the information relates;
- Lakehead District School Board personnel who required access to specific information in the course of their work; and
- other individuals, only in accordance with MFIPPA.

4.5 Students, and parents/guardians of students under the age of 16, shall be granted access to their child's personal information without filing a formal request under MFIPPA. Appropriate personnel must be present to supervise the review of the Ontario Student Record. See Appendix A – Access to/Use of/Disclosure of Student Information.

4.5.1 Parents/guardians of students between the ages of 16 and 18 shall be granted access to information contained in the Ontario Student Record.

4.5.2 Parents/guardians of students over the age of 18 shall not be granted access to any of the student's personal information without the written consent of the student.

4.6 Employees shall be granted access to their personal information without filing a formal request under MFIPPA. Reviewing the documentation must be supervised by appropriate personnel and be conducted at a mutually agreeable time.

4.7 If an informal request for personal records requires extensive research and/or photocopying, fees may be charged consistent with the fee schedule set out in MFIPPA and its regulations.

4.8 A formal request for personal information made under MFIPPA must be directed to the FOI Officer. The Act dictates timelines and applicable fees for all requests.

5. Releasing Employee Information to Third Parties

5.1 Requests from financial institutions, credit agencies and other related businesses for information regarding an employee's position, salary and years of service are to be directed to the human resources department.

5.1.1 The human resources department will only confirm the accuracy of the requester's information and offer corrections, as required. The human resources department shall not provide additional information without prior written consent from the employee or as required by legislation.

5.2 The human resources department will process requests for information related to an employee's lost time from work, normal work schedule and related attendance history. This information may be provided to third parties on receipt of a written request that complies with legislation.

5.3 Requests for an employment reference will be forwarded to the appropriate supervisory officer/supervisor or specific named individual. A reference shall not be provided unless prior written consent has been provided by the employee.

5.4 Requests for other types of personal or confidential employee information will be released only on the written consent of the employee unless required by legislation. Requests will be forwarded to the appropriate supervisory officer/supervisor or specific named individual.

6. Freedom of Information Breach

6.1 Privacy breaches occur when personal information is collected, used, disclosed, retained, or destroyed in a manner inconsistent with legislation and LDSB policy. Potential privacy breaches can occur when personal information is lost, stolen or inadvertently disclosed due to human error. Some examples of privacy breaches include: lost/stolen flash drive containing student or staff information, unlocked shredding bins, or correspondence being mailed or emailed to the wrong person.

6.2 Responsibilities

6.2.1 Employees

All employees are responsible to be aware of the LDSB policy, and for protecting personal information of others that they may be privy to in the course of their employment. Employees must inform their supervisor/manager or principal when they become aware of a privacy breach or potential privacy breach, and fully participate in any resulting investigation. Employees must take immediate steps to contain the breach if possible/appropriate (i.e. change security passwords, obtain copies of documents that have been shared in error, etc.).

6.2.2 Principals/Managers

In addition to the responsibilities of all employees, principals and managers are responsible for advising the appropriate superintendent and the FOI officer of the breach, conducting breach investigations, and implementing the breach response protocol.

6.2.3 Senior Administration

Implements the breach response protocol with the FOI officer and principal or manager.

6.2.4 Freedom of Information Officer

Ensures the breach response protocol is followed and implemented appropriately.

6.2.5 Third Party Service Providers

All third-party service providers (i.e., school photographers) are responsible to maintain the confidentiality of information provided to them by LDSB in the exercise of their responsibilities, inform LDSB if personal information in their possession has been compromised, contain the breach, document, and participate in investigation processes, and fully abide by all LDSB policies and procedures related to privacy.

6.3 Breach Protocol

Privacy breaches must be considered priorities. The following steps will be taken by the FOI officer and often needs to occur simultaneously, or in quick succession.

6.3.1 Respond

Assess the situation to determine if a breach has occurred. Contact the appropriate staff members to ensure they are aware of the breach.

6.3.2 Contain

Determine cause of and identify the severity of the breach and take steps to contain/mitigate damages. For example: obtain hard copies of information that has been disclosed, ensure additional copies are not made, determine if the breach would allow access to any other information (i.e. electronic security breach), and take necessary steps as appropriate. Document the breach and containment steps taken.

6.3.3 Investigate

Document all details of the breach and breach investigation. Interview complainants, staff, etc. Evaluate steps taken to contain the breach for effectiveness and make recommendations for change to prevent further breaches of a similar nature. Use the privacy breach checklist. See Appendix B.

6.3.4 Notify

Determine if it is appropriate to notify the impacted individuals (consider the following when determining notification requirements: risk of identity theft, risk of physical harm, risk of hurt, humiliation or damage to reputation, risk of loss of business or employment opportunities). Individuals should be informed of:

- the nature of the breach;
- steps being taken by LDSB to contain and prevent future occurrences;
- contact information for the principal/manager;
- contact information for the information privacy commissioner's office;
- steps individuals can take to protect themselves against future harm (i.e. if financial information is involved, advise individuals to contact their bank/credit card company, and to closely monitor their accounts for suspicious activity); and
- depending on the nature and severity of the breach, individuals may be informed verbally or in writing.

6.3.5 Implement Change

Review the situation and amend existing practices or create new practices, as appropriate, to ensure the prevention of future breaches. Ensure staff members are appropriately educated on privacy requirements and responsibilities. Test and evaluate new practices to ensure they will be successful.

7. Privacy Awareness

All employees are required to sign a confidentiality agreement. All employees are expected to participate in any privacy related training that may be offered by LDSB.

8. Review

These procedures shall be reviewed in accordance with 2010 Policy Development and Review Policy.

Cross Reference	***Date Received***	***Legal Reference***
Privacy Information Task Force PIM Toolkit	May 26, 2015 ***Date Revised*** June 5, 2023	*Education Act* *Municipal Freedom of Information and Protection of Privacy Act* *Personal Health Information Protection Act* Occupational Health and Safety Act Child, Youth and Family