BUSINESS AND BOARD ADMINISTRATION | 3000

ELECTRONIC INFORMATION SECURITY PROCEDURES | 3093

1. The Policy

Lakehead District School Board (LDSB) will take measures to protect information residing on networked computers, mobile devices, and other storage media. Measures will be commensurate with the value, sensitivity, and confidentially of the information. Measures will strike a balance between the need to secure information and the need to run the organization efficiently. In general, the cost of protecting information against a threat will be less than the cost of recovering should we be affected by security threats.

2. Procedures

2.1 Security Structure

Computer services is responsible for developing implementing, maintaining, coordinating, and monitoring a security program consistent with 3093 Electronic Information Security policy. These responsibilities include, but are not limited to:

2.1.1 developing, approving and issuing technical standards and guidelines on computer network security;

2.1.2 providing advice and guidance on the planning, acquisition, installation, and use of security related systems;

2.1.3 conducting periodic risk assessments and providing advice on threat and risk assessments as required;

2.1.4 evaluating security aspects of products and systems;

2.1.5 providing, or arranging for, specialized training on security;

2.1.6 providing assistance with investigations related to security issues; and/or

2.1.7 performing regular backups using authorized tools.

2.2 Superintendents, principals, and managers/supervisors are accountable for safeguarding information and physical assets under their control. All employees are responsible for the protection of these assets from unauthorized use, modification, disclosure, or destruction (whether accidental or intentional), and for maintaining the integrity of these assets and their availability to others as required in the performance of their duties. These responsibilities include, but are not limited to:

2.2.1 protecting personal and group account passwords;

2.2.2 accessing Board resources only through authorized systems and processes;

2.2.3 ensuring staff log off computers and networks after use;

2.2.4 taking reasonable precautions (i.e., security cables, storing equipment in locked rooms, etc.) to secure physical assets;

2.2.5 adhering to acceptable use policies;

2.2.6 refraining from accessing the Internet or any other network through unauthorized connections;

2.2.7 reporting any unauthorized use of LDSB information or physical assets; and

2.2.8 using secure encryption methods to protect data from unauthorized access.

3. Classification and Risk Management of Information and Physical Assets

3.1 Information will be classified and safeguarded as to its value, sensitivity, integrity, availability, and accountability requirements. The chart below will assist in determining the level of sensitivity of certain types of information. The examples are not meant to be all-inclusive, but rather to provide a sample of data that would fall in that particular category.

Level of Sensitivity	Ways to Protect the Information	Examples of Information
Low Sensitivity	• No need to protect the information. The information is publicly available.	• Corporate or school websites. • Minutes of the Board. • General information about enrolment (e.g., numbers of students).
Medium Sensitivity	• Share information on a need-to-know basis. • Limit the number of copies of the information. • Password protect the data where possible. • Destroy the information in a secure manner when no longer required.	• Email messages that do not contain any personal or confidential business information. • Student collaborative work on projects. • Agendas and minutes of meeting.

Level of Sensitivity	Ways to Protect the Information	Examples of Information
High Sensitivity	• Password protection. • Data encryption. • Non-disclosure. • Securely erase data when no longer required.	• Student data (e.g., personal, medical, family, achievement, demographic information, etc.). • Staff data (e.g., personal, medical, absence, payroll, performance reviews, demographic information, etc.). • Confidential financial or other corporate data. • In-camera Board meeting minutes. • E-mail messages containing personal or confidential information.

3.2 Access to assets that contain sensitive information is restricted to those whose duties require such access. Assets include servers, workstations, storage media, etc.

4. Personnel Security

4.1 The human resources department will ensure that superintendents, principals and managers/supervisors conduct the appropriate background reference check on any individual who is appointed to a position in the LDSB in which there is access to sensitive information.

4.2 The human resources department is responsible for notifying the computer services department of any employee resignations/terminations. The computer services department is responsible for removing the employee's computer access privileges.

5. Access to the Internet and Lakehead District School Board Networks

5.1 The computer services department will establish and maintain a network firewall to protect the Board network from external unauthorized access, and control internal access to Internet information and facilities.

5.2 Unauthorized, private Internet connections from any LDSB networked workstation (including school/department, local and wide area networks) are prohibited.

5.3 Lakehead District School Board expressly prohibits staff or students from accessing or disseminating any material that is pornographic, racist, or promotes violence.

6. Security Awareness and Training

Superintendents, principals and managers/supervisors are responsible for ensuring that all staff and students are provided with a computer network security awareness program suitable for their needs.

7. Contingency Planning

Computer services is responsible for the maintenance of a plan of action to backup and recover information and critical applications in the central computing environment and the LDSB wide area network in the event of a security incident resulting in a loss of data.
Computer services is responsible for providing hardware, data services, and remote access to data and applications to enable staff to carry out the operations of the Board during any disruption of access to normal on-site working activities.

8. Security Breaches and Violations

8.1 All staff are responsible for monitoring and enforcing compliance with this procedure within the scope of their duties and responsibilities. Violations or suspected violations of these responsibilities must be reported immediately to the appropriate superintendent, principal or manager/supervisor who will investigate and, where warranted, take appropriate administrative or disciplinary action.

8.2 Persons found to be in violation of this procedure may be subject to immediate disciplinary action up to and including termination of employment.

9. Review

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

Cross Reference	**Date Received**	**Legal Reference**
3096 Information/Communication Technology Use Policy	January 27, 2009 **Date Revised** May 27, 2014 May 24, 2022	Education Act Copyright Act Trade-marks Act Municipal Freedom of Information and Protection of Privacy Act Personal Health Information Act