



**MOOSE FACTORY ISLAND
DISTRICT SCHOOL AREA
BOARD**

BOARD POLICY NO. GOV-28	
Effective	Dec 2, 2025
Revision Date	
Motion #	25-12-06

USE OF TECHNOLOGY AGREEMENT

PURPOSE

This acceptable use policy is a collection of guidelines that set out what actions are permissible when using a specific service or system. This policy is put in place to protect the service or system from being misused in ways that could harm the service or its users, thus preventing legal or ethical issues.

It is often used to outline the acceptable uses of the internet and computer systems, but it can also be used for other types of services, such as phone systems or email services.

SCOPE

Moose Factory Island District School Area Board technology includes, but is not limited to, computers, the Board’s computer network including servers and wireless computer networking technology (wi-fi), the Internet, email, USB drives, wireless access points (routers), tablet computers, smartphones and smart devices, telephones, cellular telephones, personal digital assistants, pagers, MP3 players, wearable technology, any wireless communication device including emergency radios, and/or future technological innovations, whether accessed on or off site or through Board-owned or personally-owned equipment or devices.

PROCEDURES

1. Clean Desk

- 1.1. The clean desk policy encourages or requires employees to keep their desks clean and organized, typically in the interests of security, efficiency, and/or professionalism. The goal of this policy is to create a more orderly and professional work environment, as well as to protect sensitive information from being compromised.
- 1.2. Employees will log off from applications or network services when they are no longer needed.
- 1.3. Employees will lock their workstations and laptops when their workspace is unattended.
- 1.4. Confidential or internal information will be removed or placed in a locked drawer or file cabinet when the workstation is left unattended or at the end of the workday. This

is imperative, especially if physical access to the workspace cannot be secured by other means.

2. E-mail and Communication

- 2.1. The email and communication policy outlines the appropriate use of email and other forms of electronic communication within the organization.
- 2.2. The purpose of this policy is to ensure that all employees understand how to use these tools effectively and responsibly. Activities that are prohibited include, but are not limited to:
 - a) sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (spam);
 - b) any form of harassment via email, telephone, text, or paging, whether through language, frequency, or size of messages;
 - c) unauthorized use, or forging, of email header information;
 - d) solicitation of email for any email address other than that of the poster's account, with the intent to harass or to collect replies;
 - e) creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type; and
 - f) use of unsolicited email originating from within Board networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the corporation connected via the network.

3. Installing Software

- 3.1. Employees and contractors will not download or install any software application without the authorization of an authorized organization representative.
- 3.2. The Information Technology team installs only approved software.
- 3.3. Employees will be disciplined if caught downloading or installing unauthorized software.

4. Internet Use

- 4.1. This policy ensures that employees use the organization's information technology resources in an appropriate, responsible, and ethical manner. The policy has been put in place in order to protect the organization's interests, intellectual property, and reputation.
- 4.2. In addition, this policy outlines the organization's expectations:
 - a) Internet access is to be used for Board purposes only.
 - b) Internet access will be provided for users to support business activities and only as needed to perform their jobs.

- c) Personal devices are not to be used on the Board network unless authorized by a manager and the IT team.

4.3. Other activities that are strictly prohibited include, but are not limited to:

- a) Accessing company information that is not within the scope of one's work.
- b) Misusing, disclosing without proper authorization, or altering customer or personnel information.
- c) Any conduct that would constitute or encourage a criminal offense, lead to civil liability, or otherwise violate any regulations.
- d) Any form of gambling.
- e) Acquisition, viewing, storage, and dissemination of data that is illegal, pornographic, or negatively depicts race, sex, or creed are specifically prohibited.

4.4. The Board also prohibits the conduct of a business enterprise or political activity, engaging in any form of intelligence collection from Board facilities, engaging in fraudulent activities, or knowingly disseminating false or otherwise libelous materials.

4.5. Removal of Privileges

Internet access will be discontinued upon the termination of an employee, completion of a contract, end of service of a non-employee, or disciplinary action arising from the violation of this policy.

5. Passwords

5.1. The password policy is designed to ensure the security of passwords within an organization. This policy specifies the requirements for the creation and management of passwords, such as the minimum length, complexity, and expiration of passwords. It also outlines procedures for handling password changes and password resets, as well as restrictions on the sharing of passwords. The purpose of a password policy is to protect against unauthorized access to systems and data by establishing strong and unique passwords that are difficult for attackers to crack.

5.2. Access to all devices, applications, and folders that create or process non-public information must be protected by an authentication mechanism that consists of, at a minimum, a username, and a password.

5.3. Passwords must be changed if there is suspicion or evidence of compromise.

5.4. An additional authentication factor, such as a device-based or biometric-based factor, may be required.

5.5. All user accounts must be assigned an initial password, and that must be changed by the user upon first access.

5.6. All passwords must meet the following requirements:

- a) For regular accounts, passwords must be 10 characters or more and include:
 - A mixture of upper and lower-case letters.
 - At least one numeric or special character.
- b) For privileged accounts (system administrators, financial controllers), passwords need to be at least be 15 characters or more and must include:
 - a mixture of upper and lower-case letters; and
 - at least one numeric and special character.
- c) Passwords must not consist of a single guessable item (username, name, address, phone number, or any single word that can be found in any dictionary in any language).
- d) Common variations on names or words (e.g., M1ch@el, p@22word) are not acceptable.
- e) Common phrases (e.g., letmein, or opensesame) are not acceptable passwords.
- f) Passwords must not be reused for more than one system or application.
- g) Authorized Password Manager solutions are recommended.
- h) Employees must not share passwords with coworkers.
- i) Passwords must always be secured. They must not be stored where people can see them.

6. Personal Devices

- 6.1. If an employee/user uses a personally-owned device to access Board technology or conduct Board business, they shall abide by all applicable Board policies, administrative regulations, and this Use of Technology Agreement.
- 6.2. Any such use of a personally-owned device may subject the contents of the device, and any communications sent or received on the device to disclosure pursuant to a lawful subpoena or public records request.

7. Privacy

- 7.1. Since the use of technology is intended for use in conducting business, no employee/user should have any expectation of privacy in any use of Board technology.
- 7.2. The Board reserves the right to monitor and record all use of Board technology, including, but not limited to, access to the Internet or social media, communications sent or received from Board technology, or other uses within the jurisdiction of the Board.

7.3. Such monitoring/recording may occur at any time without prior notice for any legal purposes including, but not limited to, record retention and distribution and/or investigation of improper, illegal, or prohibited activity.

7.4. Employees/users need to be aware that, in most instances, their use of Board technology (such as web searches or emails) cannot be erased or deleted.

8. Remote Access

8.1. This policy outlines the types of remote access methods that are permitted, the security measures that must be taken to protect the network and data, and the responsibilities of the users who are granted remote access.

8.2. Employees are required to have the proper authorization to access the internal systems remotely. A Board laptop will be used unless otherwise permitted by management.

8.3. No employee or contractor may install any software or application that allows access to the organization's systems from a remote location without the appropriate authorization from the Board.

8.4. Employees shall not connect to unknown Wi-Fi networks. Public Wi-Fi networks can only be used if a VPN is enabled.

9. Reporting Security Incidents

9.1. This policy specifies to whom the incidents must be reported, such as the IT department or a designated incident response team. The report will include steps for documenting and investigating the incident. The goal of an incident reporting policy is to ensure that all incidents are promptly and properly addressed to minimize the impact on the organization.

9.2. Types of incidents that must be reported are:

- a) any observed unauthorized disclosure of Protected Information or Confidential Information, whether intentional or unintentional;
- b) any observed attempt to view or access Protected Information or Confidential Information by a person not authorized to do so;
- c) any unauthorized attempt to gain physical access to or install unauthorized software applications on any server or workstation;
- d) any telephone, email, or other communication that includes an unauthorized attempt to receive or access Protected Information or Confidential Information; and
- e) any unusual computer behavior (unusual error messages, unusual pop-up windows, website redirection, etc.).

- 9.3. When unusual computer activity is observed, the computer must not be turned off to preserve valuable evidence. The Security Officer or other authorized organization representative must be contacted immediately.
- 9.4. If any of these situations are observed, it is the employee's responsibility to promptly notify their manager.

10. Social Media

- 10.1. This policy outlines the acceptable use of social media platforms, such as Twitter, Facebook, and LinkedIn, for personal and professional purposes. It also specifies which types of content are acceptable to share and how employees should manage sensitive or confidential information. The goal of a social media policy is to protect the reputation of the Board and its employees. It ensures that all communications are consistent with the values and goals of the Board.
- 10.2. All employees need to be aware of the social media policy and understand their responsibilities when using social media at work.
- 10.3. Employees need to be careful not to share any confidential or proprietary information on social media, as this can put the Board at risk.
- 10.4. Employees must not use social media to discriminate against or harass coworkers or any other person.
- 10.5. Employees must respect the intellectual property rights of others and not share or use copyrighted material without permission.
- 10.6. Employees will not use their Board e-mail addresses to sign up for personal social media accounts.

11. Security Awareness Training

- 11.1. This policy states the requirements for educating employees about cybersecurity and related topics. The goal of this policy is to ensure that all employees are aware of their role in protecting the organization's information and systems and to provide them with the knowledge and skills they need to do so effectively.
- 11.2. All new employees must complete an approved security awareness training class prior to, or at least within 30 days of being granted access to any Board information resources.
- 11.3. All employees must be provided with the document included in this policy, and acknowledge they have received the information, and agree to adhere to the Board Information Security Policies before they are granted access to information resources.
- 11.4. All employees must complete the annual security awareness training.

REFERENCE DOCUMENTS

Legal References:

Education Act, Section 169.1 Duties and Powers of Boards: Stewardship of Resources
Education Act, Section 265 Duties of Principal: Care of Pupils and Property
Ontario Regulation 298 Operation of Schools, section 11: Duties of Principals
Ontario Regulation 298 Operation of Schools, section 20: Duties of Teachers
PPM 128 The Provincial Code of Conduct and School Board Codes of Conduct

Board References

Board Policy GOV-01 Vision, Mission, and Values
Board Policy GOV-03 Role of the Corporate Board
Board Policy GOV-04 Role of the Supervisory Officer
Administrative Procedure 147 Staff and Student Use of Technology
Administrative Procedure 215 Effective Use of Technology
Administrative Procedure 416 Electronic Monitoring of Employees

Acknowledgement

I have read, understand, and agree to abide by, this Use of Technology Agreement Board Policy:

Print: _____ Date: _____

Signature: _____