

| | |
|-----------------|--|
| Section: | Human Resources |
| Title: | Network, Internet, and Wi-Fi Access for Employees |

Purpose

To set appropriate standards for users to access the MPSD Network, Internet, and Wi-Fi Access in order to perform work duties. The use must not jeopardize the operation of the School District Network or the reputation and/or integrity of the School District.

General Guidelines

Network Usage

Recognizing that our local network (MPSD.CA) and the Internet are limited and shared resources, all staff granted the privilege to use the network will be asked to pledge, in written form, to conduct themselves in a responsible, ethical, and polite manner while using the network.

Using MPSD.CA for illegal, political, commercial or obscene purposes or in support of such inappropriate activities is strictly prohibited and subject to the following:

- In the case of misuse or suspicion of misuse of the network or services, the MPSD.CA management reserves the right to access any files on the system.
- The system administrators will not intentionally inspect the contents of mail, or disclose such contents, unless required to do so by law or by this procedure, or as part of an investigation. Investigation of complaints regarding mail which are alleged to contain defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal material may occur by system administrators.
- Mission Public Schools and MPSD.CA will cooperate fully with any participating school district, local, provincial, or federal officials in any investigation concerning or relating to any mail transmitted through MPSD.CA.
- In the event of an alleged breach of this procedure by a network member, the systems administrators shall immediately notify the member's supervisor, who in turn shall ensure due process is afforded to the member before any action is taken.
- Vandalism will result in cancellation of MPSD.CA privileges. Vandalism is defined as any malicious attempt to harm or destroy data of another member, MPSD.CA, or any of the agencies or other networks that are connected to the Internet.

MPSD.CA accounts shall be used only by the authorized owner of the account. Account owners are responsible for activity within their account.

MPSD.CA is a publicly funded and finite resource, and as such must be used in moderation. Copyright material must not be placed on any computer system and/or file connected to MPSD.CA without the author's permission.

Members are expected to remove old electronic mail messages in a timely fashion, and the system administrators may remove such messages if not attended to regularly by the members. The system administrators will delete electronic mail messages that are in excess of 60 days old.

Staff are required to complete a [MPSD.CA - Network Registration form](#).

MPSD.CA members will be notified in a timely fashion of changes made to the policies and guidelines before implementation of these changes.

Internet Usage

- Users must comply with all applicable laws and regulations and must respect the legal protection provided by copyright and licenses with respect to both programs and data.
- Internet usage must be able to withstand public scrutiny and/or disclosure.
- Sensitive information must not be transmitted via or exposed to Internet access.
- Internet usage must be consistent with professional conduct and not for personal financial gain.
- Users must not attempt to obscure the origin or any message or download material under an assumed Internet address.
- Administrators must ensure that all employee users sign a [Network, Internet and Wi-Fi Access User Agreement Form](#) and the [MPSD.ca Network Registration Form](#) before access is allowed.
- The Systems Administrator monitors the use of the School District network and will monitor selected network traffic at the request of School District administration or the Ministry of Education.

Responsibilities

Users

- Users are responsible for ensuring that their use of the MPSD Network, Internet and Wi-Fi is appropriate and consistent with this procedure.
- Users with an Access Agreement completed are personally responsible for the security of their user account, if one is granted, as follows:
 - Passwords must not be disclosed to any other individual.
 - Responsible for all activity that occurs within their account.
 - Notifying the immediate supervisor, teacher or systems administrator immediately if a security problem is suspected.
- Users are responsible for informing a supervisor, manager or the system administrator if they mistakenly access inappropriate information or receive any message that they feel is inappropriate.
- Users are responsible for following virus protection procedures to avoid the spread of computer viruses.
- Users are responsible for checking their email on a regular basis and for deleting unwanted messages.

Administrators

- Supervisors or Managers are responsible for ensuring that all employees review this procedure.
- Supervisors or Managers are responsible for taking appropriate action when this procedure is contravened.

Systems Administrator

- The District Systems Administrator is responsible for monitoring network usage in terms of traffic/load.
- On an annual basis, the systems administrator will delete all non-renewed network access agreements (i.e. employees who have retired or left the School District, etc.).

- Employees who leave the School District will have their accounts disabled.
- A search will be conducted if there is a reasonable suspicion that an employee has breached the rules and regulations governing use of the MPSD.CA network, the [Safe, Caring and Respectful Schools Policy](#), and [Safe, Caring, and Respectful Workplaces Policy](#) or the law.
- The School District will cooperate fully with law enforcement officials conducting an investigation into illegal activities related to employee use of the MPSD.CA network.

Safe Practices

- The MPSD.CA network must not be used for any of the following. Engaging in any of these activities may be considered an illegal act and subject to an investigation by school and/or law enforcement officials.
 - transmitting any materials in violation of Canadian laws;
 - violating, or attempting to violate, the security of the district's computers, data or network equipment or services;
 - offering, providing or purchasing products or services;
 - political lobbying;
 - posting or linking personal and/or private information about themselves or other people. (See the Information and Privacy Act for a definition of *personal information*);
 - knowingly or recklessly posting false or defamatory information about a person or organization;
 - engaging in personal attacks, including prejudicial or discriminatory attacks;
 - using obscene, profane, lewd, vulgar, rude, inflammatory, threatening or disrespectful language at any time;
 - harassing another person;
 - posting chain letters or sending unnecessary messages (spamming) to a large number of people;
 - posting information that could cause damage or danger;
 - plagiarizing works found on the Internet;
 - accessing material that is profane or obscene (pornography), that advocates illegal acts, or that advocates violence or discrimination (hate literature);
 - pursuing unauthorized access or attempt to access another person's accounts, files or computer;
 - attempting to spread or create computer viruses, destroy data or disrupt the computer system in any way.

Date Adopted: October 2001

Date Amended: August 2022

April 2018 (Formerly Administrative Procedure 5.4.1, #210a and Administrative Procedure #601)

Definition:

- *"User" means employees authorized to access the network, internet and Wi-Fi via a School District service provider and.*
- *"Internet" means the global interconnection of data networks that commonly use (but are not limited to) the Internet Protocol.*
- *"Sensitive Information" means personal, confidential or protected information whose release is unauthorized – i.e. information which is reasonably likely to be accepted or excluded from access under the Freedom of Information and Protection of Privacy Act.*
- *"Offensive material" includes, but is not limited to, pornography, hate literature or any material which contravenes the BC Human Rights Act.*

Cross Reference: [Safe, Caring, and Respectful Schools Policy](#), and [Safe, Caring and Respectful Workplaces MPSD.ca Network Registration Form \(STAFF\)](#)
[Network, Internet and Wi-Fi Access User Agreement Form](#)