ACCEPTABLE USE POLICY

NORTHWESTERN
POLYTECHNIC

ACCEPTABLE USE POLICY			
Effective Date	June 1, 2023	**Policy Type**	Administrative
Responsibility	Director, IT	**Related Policies**	IT Governance IT Passwords IT Security Information Management Records Management
Approval Authority	Executive Council	**Review Schedule**	June 1, 2026

1. Policy Statement:

The purpose of this policy is to outline the acceptable use of computer equipment and network connected devices at Northwester Polytechnic (NWP) for promoting academic use, operational purposes, and the public good. The Acceptable Use Policy (AUP) describes both the responsibilities and restrictions of the users and information technology (IT) personnel in support of the mission, vision, and values of the organization. The need for reliable, safe, and secure network and system access is balanced by reasonable IT controls, as well as the ethical, legal, and responsible use by the NWP community.

2. Scope:

This policy applies to:

- All Institution offices, campuses and learning centres.
- All students, faculty, staff, consultants, contractors, visitors, volunteers, and authorized users accessing Institution IT systems and applications.
- All IT systems or applications managed by the Institution that are storing, processing, or transmitting information, including network and computer hardware, software and applications, mobile devices, and telecommunication systems.

3. Reason for Policy:

NWP recognizes the academic and business requirements of information technology for all, in keeping with the goals, values, and mission of the organization. Members of the information technology department have a duty to maintain the effective use of computer networks, systems, and services. However, a technical response issues with digital services is not always desirable, warranted, or possible. In some instances, associated policy, procedure, regulation, or legislation provides better guidance to resolve those issues.

4. Guiding Principles

Everyone has a role in ensuring these resources are used safely, ethically, and responsibly. This includes the duty to protect personal and private information. In the event either the data or the system is compromised, everyone has a duty to appropriately report the issue.

IT has a duty to use the technical tools available to monitor, maintain, and protect the system resources. In doing so, members of the IT department must adhere to best practice with an open dialogue, while maintaining confidentiality, as part of the job responsibilities. This affirms that IT personnel also has a responsibility to report activities as required.

Authorized Users have a reasonable expectation of privacy in their use of NWP IT Resources. Authorized Users shall take reasonable and prudent steps to protect the Security and ensure the Confidentiality, Integrity and Availability of NWP IT Resources.

5. The Policy:

5.1. General Use and Ownership

5.1.1. NWP proprietary information stored on electronic and computing devices whether owned or leased by NWP, the employee or a third party, remains the sole property of NWP. You must ensure through legal or technical means that proprietary information is protected in accordance with the Data Governance*.*

5.1.2. You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of NWP proprietary information.

5.1.3. You may access, use, or share NWP proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

5.1.4. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of the Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

5.1.5. For security and network maintenance purposes, authorized individuals within NWP may monitor equipment, systems, and network traffic at any time, per NWP IT Security Policy.

5.1.6. NWP reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

5.2. Security and Proprietary Information

5.2.1. All mobile and computing devices that connect to the internal network must comply with the Security Policy.

5.2.2. System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

5.2.3. Employees must use extreme caution when opening email attachments received from unknown senders, which may contain malware.

5.3. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of NWP authorized to engage in any activity that is illegal under local, state, federal or international law while using NWP-owned resources.

5.4. Enforcement

A violation of the provisions of this Policy may constitute a disciplinary offence and, where appropriate, shall be dealt with under the regulations, policies, code or collective agreement to which the Authorized User is subject.

Any individual who has reasonable cause to believe that there has been a breach of this Policy shall report the matter to the Vice President, Corporate Services.

6. Roles and Responsibilities

Stakeholder	Responsibilities
Board of Governors	• Approve and formally support the Policy.
Vice-President, Corporate Service	• Review and formally support the Policy. • Ensure alignment of this policy to the Organizational Strategic Plan
IT Steering Committee	• Provides guidance for the IT Director regarding the academic and business needs related to information technology systems.
IT Director	• Develop and maintain the Policy. • Align the Policy to the IT Strategic Plan and IT procedures
IT Management	• Maintain IT procedures
IT Team Members	• Implement the IT procedures
Users	• Contact the IT Service Desk for any problem, issue or needs related to the technology. When a problem, issue or needs cannot be addressed by the IT Service Desk, they contact their supervisor or representative. • Contact their supervisor or manager for any request related to access rights and privileges or needs for IT equipment. • Contact their supervisor or manager with any request to change the existing technology. • Backup their personal files stored locally on computers and mobile devices.

7. Definitions

"Authorized User" means a member of the NWP community and includes faculty, staff, students, retirees, alumni, appointees, consultants, guests or other individuals who have been granted permission to access certain data or systems that are part of NWP IT Resources by virtue of their role and responsibilities.

"Availability" means the assurance of timely and reliable access to McGill IT Resources for their intended use.

"Confidentiality" means the assurance that IT Credentials or Data can only be accessed by Authorized Users or authorized systems.

"Confidential Data" means information whose protection and use is mandated and governed by law, regulation, industry requirement, contract or any NWP policy or directive because of its sensitive nature, including, but not limited to, Personal Information.

"Data" means digital information stored in or transmitted through NWP IT Resources and includes documents, files, databases, emails, and multimedia.

"Integrity" means the assurance of the accuracy and consistency of Data and that Data is not altered by unauthorized users.

"Non-NWP Use", also known as personal use, means usage that is not for the purpose of advancing the mission of the Polytechnic and supporting related administrative, financial and operational activities or that has not been otherwise authorized.

"NWP Network" includes any network that directly accesses NWP systems without traversing through the NWP firewall. Networks that only have access to the internet, such as the NWP public wireless network, are not considered to be part of the NWP Network in this policy.

"Personal Information" means information which relates to a natural person and allows that person to be identified, as provided for in applicable privacy legislation.

8. Revision history:

March 30, 2023
August 25, 2023 (minor edits)

References:

NIST Policy on Information Technology Resource Access and Use

SANS Acceptable Use Policy