# Acceptable Use of Technology Resources

## Purpose

The New Brunswick Community College (NBCC) is committed to providing a secure and conducive digital environment for teaching and learning, research, and supporting administrative functions. These guidelines are designed to ensure that Information and Communication Technologies (ICT) are used responsibly, ethically, legally, securely, and the Institution's Information Assets are protected.

These guidelines align with NBCC's Information Security Policy (2808).

## Scope

These guidelines apply to all members of the NBCC College Community including employees, students, contractors, visitors, volunteers, and Board of Governors members who have access to the institution's information systems. They cover all devices that are owned, leased, or managed by the college, as well as personal devices used to access the college's network, whether on campus or remotely.

All technology resources provided by NBCC, including hardware, software, and network systems, are the property of the institution. These resources are intended to support the educational and administrative activities of NBCC. Members are granted access to these resources to facilitate their work and studies, with the understanding that their usage must comply with institutional policies and guidelines. Unauthorized use, mismanagement, or any actions that jeopardize the integrity and security of these resources are strictly prohibited and may result in disciplinary action.

## Definitions

### Information and Communication Technologies (ICT)

ICT refers to the integration of computing and telecommunications technologies to enable access, storage, transmission, and manipulation of information. It encompasses

- Hardware: Computers, servers, mobile devices, and networking equipment.
- Software: Operating systems, productivity tools, enterprise applications.
- Communication Tools: Email, video conferencing, messaging platforms.
- Infrastructure: Networks, cloud services, and data centres.

### IT Identity

An IT Identity refers to the unique digital representation of a user within an organization's IT environment. It is the foundation for managing access, enforcing security policies, and enabling secure interactions across systems. It includes assigned usernames, email addresses, and authentication credentials, such as passwords, multi-factor authentication (MFA) tokens or biometric data used to verify a person's identity.

## Implementation

The following information is intended to provide models of acceptable use of ICT and is not intended to be a comprehensive list. The Information Technology department is committed to helping all users meet these obligations, whether through direct support or through training and awareness initiatives.

### Acceptable Use

The primary use of the college's ICT is to support its educational, research, and the supporting administrative activities.

As such, members must:

- Use ICT resources primarily for teaching, learning, research, and administrative purposes.
- Follow all college policies, and applicable laws.
- Respect the rights and privacy of others.
- Maintain the integrity and security of ICT resources.
- Protect their NBCC IT Identity (e.g., never share passwords or MFA tokens).
- Report suspected security breaches immediately to the IT Service Desk.
- Comply with all other parts of this guideline, and the Information Security Policy (2808).

Incidental personal use of ICT resources is permitted as long as it:

- Does not interfere with educational, research or administrative activities.
- Does not incur additional costs to the college. For example, personal international cellular roaming costs shall be reimbursed to the institution.
- Follows these guidelines and Policy 2808.

Members are responsible for all personal data on NBCC owned ICT devices. IT staff are not responsible for backing up or retrieving personal data.

### Prohibited Use

When using the NBCC's ICT resources, the following activities are prohibited:

- Gaining or attempting to gain unauthorized access to any ICT resource, network, system, or data. This includes using another member's NBCC IT Identity.
- Letting someone else use their NBCC IT Identity.  Users are fully accountable for all activity performed under their NBCC IT Identity, regardless of whether it was done by them or by someone else using their credentials with or without their knowledge.
- Infringing on intellectual property rights, including unauthorized copying or distribution of software, music, videos, and other copyrighted material.
- Engaging in any activity that violates local, provincial, national, or international laws.
- All software installed on institutional owned ICT resources must be approved by the IT department. Members must only use licensed and approved software.
- Creating, accessing, transmitting, or storing offensive, obscene, or inappropriate content, including pornography (except where demonstrably required for teaching or research purposes), hate speech, violence or advocating violence, or discriminatory material.
- Cyberbullying, harassment, or abusive behaviour using its IT resources. Users must not intimidate, threaten, demean, or harm others through NBCC systems.
- Introducing, creating, or spreading malware, viruses, or other malicious software.

- Performing actions that disrupt or degrade the performance of ICT resources, such as network probing, or conducting unauthorized scans.

## Protection of Data

NBCC information is an asset critical to the delivery of programs and services. To ensure its continued availability and appropriate use, members must protect it from unauthorized disclosure, modification, use, or destruction. This responsibility includes complying with all applicable policies, procedures, and legal obligations related to information security.

- Be cautious when sharing information both inside and outside of NBCC.
- Do not share confidential information without explicit authorization.
- Store institutional data only in approved NBCC provided services (e.g., M365 OneDrive, SharePoint, Microsoft Teams). Do not use unapproved third-party cloud storage services such as Box, Dropbox, Google Drive, iCloud Drive, or personal OneDrive accounts for storing or sharing NBCC data. If an NBCC partner or external collaborator requires the use of one of these services, please consult with NBCC IT prior to use.
- Only use NBCC supplied email services for institution-related business.
- Do not store or transmit sensitive information such as payment card numbers.
- Immediately report any breaches or suspected data breaches to the IT Service Desk.

## Ownership

NBCC retains full ownership of all data that members use, create, or modify during their active relationship with NBCC (employment, contract, etc.). Upon the end of the relationship, members shall ensure all data in their possession is returned to the institution. This does not apply to student created data as part of their educational program.

**All ICT resources provided by NBCC are the property of the institution. As such, members shall return any assigned equipment upon request by NBCC IT, their supervisor, or a designated representative.**

## Secure Use of ICT Devices

As part of keeping NBCC's data safe and its Information Systems secure, members shall ensure that the use of ICT devices (NBCC owned or personal), are used in a secure manner. This includes:

- Locking the device when not in use to prevent unauthorized access. A secure authentication method, such as biometric recognition (e.g., fingerprint or facial recognition), a PIN, password or a smart card, is required to resume using the device.
- Ensuring that devices are not left unattended in a non-secure area.
- Reporting the loss or theft of ICT devices immediately to the IT Service Desk. This includes any personal devices (e.g., an enrolled mobile phone or tablet) that is being used to access NBCC data.
- Not tampering with any security settings or security software on NBCC devices.
- Hardware changes or repairs to NBCC ICT devices shall be done only by NBCC IT, or their approved providers.
- Use of personal mobile devices for NBCC work is permitted; however, the device must be enrolled in NBCC's Mobile Device Management (MDM) platform. Enrollment allows NBCC IT to manage security settings and protect institutional data, but NBCC does not monitor personal content, applications, or usage unrelated to NBCC business.

- If an NBCC owned or personal ICT device does not meet NBCC IT's minimum standards to be operated securely, it will be restricted from accessing institutional systems, services, and data.

## Monitoring, Access and Threat Prevention

To uphold the integrity, confidentiality, and availability of NBCC's digital infrastructure, the IT department monitors activity across the NBCC network and NBCC-owned systems. Monitoring is necessary to detect and prevent cyber threats, unauthorized access, ensuring a secure and reliable environment for all users.

This monitoring includes such things as:

- Scanning inbound and outbound internet traffic for malicious software, phishing attempts, and other cyber threats.
- Reviewing audit logs, user sessions, and system alerts for security or operational issues.
- Using technologies such as intrusion detection and prevention systems (IDPS), and web filtering tools to block harmful content.
- Monitoring is never used for personal surveillance.

Data collected during monitoring is limited to information required for institutional purposes, such as:

- Network traffic metadata (e.g., source/destination addresses, timestamps).
- Email headers and content flagged by security systems.
- System and application logs related to NBCC resources.

All monitoring activities comply with applicable Canadian privacy legislation, including the Personal Information Protection and Electronic Documents Act (PIPEDA) and relevant provincial laws.

To maintain a secure and resilient digital environment, access to NBCC-owned equipment, systems, and data may occur without prior notice when necessary for investigations, policy enforcement, or technical troubleshooting, but only within the scope permitted by law and NBCC policy.

## Other Related Documents

Information Security Policy (2808).

| | | |
|---|---|---|
| **Document Author and Owner** | Blair T. Sawler | Manager, Infrastructure & IT Security, DISO |
| **Document Approver** | Simon Collier | Director, Information Technology |

*Any document appearing in paper form is uncontrolled and must be compared to the electronic version.*