SUBJECT	**Information Technology & Network Terms of Use Procedure**
	Information Technology (IT) & Network Terms of Use Policy # IT-3

PROCEDURES

ACCESS

Access to the College internal network, Information Technology (IT) resources and the College wired, and wireless internet is enabled by the College's IT department at the request of College departmental managers or designated departmental employees for employees, students, contractors, guests, or visitors at the College. Unauthorized use of the College's network is strictly prohibited and subject to criminal prosecution.

AUTHORIZED USERS

All authorized Users will have an expectation of privacy; however, all use of College networked resources is logged, and network administrators have access to all email, including data in transit. If an infraction is suspected, the traffic and files will be investigated in accordance with the applicable College process to ensure compliance with Northern College policy, and with federal, provincial, and municipal law. By accessing and using this network, Users are consenting to such monitoring and information retrieval by Northern College.

Employees

- Are provided with a Northern College User ID and email account.
- Are required to use their College provisioned email account for all communications of a work or academic nature.
- Are responsible for protecting the College's confidential information, when using email.
- Work with e-mails they receive from others at the College with confidentiality as required.
- Must take all reasonable steps to ensure that the intended recipients of emails, require the College's information and are authorized to receive the College's information.
- Must ensure when forwarding email, the "thread" only includes information the recipient **should be** receiving.
- Should "archive" relevant emails and permanently purge irrelevant ones, when their mailbox is full. Purging or deletion of emails only removes the email from an individual's account. The College's backup and archival processes will preserve a copy.
- Will use the College owned and provisioned devices and network resources for all work-related computing and electronic communication as the College controls and secures information that resides on its own System. Personal devices can be used for college related work provided that the conditions below are met and adhered to:
  - Written authorization must be obtained from their direct supervisor/manager.
  - Their personal device must be examined and/or approved by the College's IT department.
  - Their personal device must remain password protected to login and/or unlock the device.
  - Employees who intend to use a personal device to access their College email account will be migrated to the College's cloud system with multi-factor authentication (MFA) enabled.
  - The College's IT department reserves the right to deny a personal device from accessing the College's network and/or systems should it not meet proper security requirements.
- Will be required to create a password that meets the security requirements outlined by the College's IT department and will be required to change their password every six (6) months.

SUBJECT	**Information Technology & Network Terms of Use Procedure**
	Information Technology (IT) & Network Terms of Use Policy # IT-3

Students
- Are provided with a Northern College User ID and email account.
- Are expected to use their College provisioned email account for all communications of an academic nature.
- All official communications directed to students at Northern College will be sent to the College provided email address. Students are expected to check their email daily while attending the College. Email account access will remain in place for a maximum of two (2) years once a student is no longer attending College. Students who are expelled will have their access revoked immediately.
- Are responsible to take precautions to protect sensitive data by maintaining appropriate hardcopy or other backups of personal sensitive data in the event of a College Network or equipment failure.
- Must comply with directions given by a faculty or staff member during computer lab or classroom sessions, including online and/or web-based classroom sessions, some of which may be recorded. Students must also comply with instructions given for tests and exams, including but not limited to, during the use of Learning Management System (LMS) based software used for Academic Integrity.
- Must refrain from unrelated computer use, when in a faculty or staff lab or classroom led session unless expressly permitted by faculty or staff member (*i.e.*, recreational use is unrelated to course work).
- Must be considerate when a lab is at or near capacity or when other students are waiting to access the workstation.
- Must not change the configuration of computers.
- Must not eat or drink at the same table where the workstation is located.
- Must not use devices to amplify sound.
- Must not disturb others.
- Must comply with directions given by computer lab monitors and staff.

Guests/Visitors/Contractors
- May be provided a temporary User ID and password upon request by a designated manager.
- Are aware there are security, privacy and confidentiality risks inherent in the use of publicly available wireless communications and technology.
- Send and receive data at their own risk.
- Recognize that data is not encrypted and may be viewed or intercepted by others. Privacy and security safeguards are the User's responsibility; this network does not provide any.
- Recognize this service may interrupted, is not error-free or secure.

COMPUTER DESIGNATED AREAS
No food or drink is allowed near any desktop/laptop/electronic device stations within classrooms, computer labs, video rooms, offices, and Learning Resource Centers (LRC).

UNAUTHORIZED USES
The System may only be used for purposes that are consistent with the business and academic objectives and the policies of the College. The following uses are unauthorized and expressly prohibited:

SUBJECT	**Information Technology & Network Terms of Use Procedure**
	Information Technology (IT) & Network Terms of Use Policy # IT-3

- Unauthorized access: This may include using unauthorized usernames, passwords, computer addresses or identities, or modifying assigned network settings to gain access to computer/ telecommunication resources and/or data and telephone records.

- Vandalism of data: Under no circumstance may a User access, inspect, alter, delete, publish, or otherwise tamper with files or file structures that do not belong to the User without prior consent or authorization for such activity with respect to such files or file structures. In addition, Users shall not send communications that appear to be sent by someone other than themselves.

- Interference with other Users' work: This includes use of any process that causes a User to be deprived of services or resources that they would normally expect to have available. It covers but is not limited to the creation of "Spam," the playing of computer games, the downloading or streaming of audio and video files and the introduction of Viruses.

- Inappropriate use of the Internet: Access to the Internet is provided to Users as a necessary resource in the completion of their work assignments or course learning related activities and all Users are expected to exercise good judgment and remain productive in the completion of assignments or activities.

- Squandering resources: Resources are shared, and no User may degrade the systems by: unwarranted use of data space, time and bandwidth consumption through resource-intensive programs, unattended network connections and/or lengthy print jobs. Users who exceed established limits must secure the approval from their immediate supervisor/manager and the Director of Information Technology.

- Sharing of account: The College Network is available to groups and individuals for specific academic and administrative purposes. It is not acceptable to give, sell or otherwise provide computing resources to individuals or groups that do not have explicit permission to use them from the College authority.

- Commercial uses: The College Network and IT resources may not be used to sell or promote products or services for personal gain. This includes uses such as distribution of advertising materials, the offering of network information or services for sale, and private enterprises.

- Breach of copyright: This includes installing, reproducing and/or distributing copyrighted materials such as proprietary software, publications, or files without permission. College software is provided under license agreements with various vendors and may not be copied or otherwise removed.

- Offensive material: Materials not subject to legal sanction may be objectionable or repugnant to persons other than the User. Importation or distribution of such material (including, but not limited to material that is obscene, pornographic, defamatory, racist, offensive, or otherwise inappropriate) is prohibited unless an underlying academic or educational purpose exists and is approved by the Academic Dean and the Director of Information Technology. If in doubt the User should obtain explicit permission from the relevant College authority.

- Hostile atmosphere: The display of sexually explicit or violent images in public spaces and/or the initiation of unsolicited communication with sexual content will not be tolerated and will be subject to immediate disciplinary action.

SUBJECT	Information Technology & Network Terms of Use Procedure
	Information Technology (IT) & Network Terms of Use Policy # IT-3

- Harassment: Harassing or defamatory material may not be sent by electronic means, including email and voice mail, or posted to news groups or social media sites. Suspected violations will be investigated and if warranted will be subject to immediate disciplinary action.

- Excessive personal use: Use of the System for personal reasons shall not interfere with an employee's productivity to any degree, may not pre-empt any business or academic activity and may not disrupt normal operation of the System.

Users who have complaints about computer lab operations or about other Users should address them to lab monitors or to the IT Department.

Lab monitors or College staff may draw Users' attention to the provisions of this policy and request compliance. If a User fails to comply, the incident will be escalated to appropriate authority and future access to the College System may be revoked.

If the College has reason to believe that the System has been used to commit a crime it may report the matter (with supporting evidence) to the police or otherwise enlist police assistance. The College will also comply with any lawful demand for access to information by a law enforcement body.

FAILURE TO COMPLY
Inappropriate use of the System will result in immediate suspension of access.   Users who breach this policy will be subject to discipline in accordance with the College's Discipline Policy.

ADMINISTRATION
Questions regarding this procedure and the *"Information Technology and Network Acceptable Use Policy"* may be directed to itdepart@northern.on.ca.

DISCLAIMER
Northern College assumes no liability for any direct or indirect damages arising from the User's connection to the guest wireless internet.

Supersedes the following policies
Acceptable Computer Use Policy dated 2004-05-03
Internet Security Policy dated 2004-05-17
E-mail Policy dated 2004-04-13