INFORMATION TECHNOLOGY POLICY

SUBJECT	ACCEPTABLE COMPUTER USE POLICY

POLICY

Northern College is committed to the creation of a technology-supported learning and working environment for all students and staff. To this end, the College has established the following standards with respect to the use of College networks and computer accounts.

1. GENERAL

Computing and networking facilities at Northern College are provided for the use of Northern staff and students in support of the mission of the College. All staff and students are responsible for seeing that these computing facilities are used lawfully, ethically, and courteously.

The College is responsible for securing its facilities to a reasonable and economically feasible degree against unauthorized access and/or abuse. This responsibility includes informing users of expected standards of conduct and the resultant penalties for not adhering to them.

2. RESPONSIBILITIES

The users of the network are responsible for respecting and adhering to local, provincial, federal and international laws, the Internet Service Provider's (ISP) Acceptable Use Policy, as well as the policies of the College. Computers and networks can provide access to resources on and off campus, as well as the ability to communicate with other users worldwide. Such open access is a privilege, and requires that individual users act responsibly. Users must respect the rights of other users, respect the integrity of the systems and related physical resources.

3. USER ID

Authorized users of College network facilities shall be issued a unique User ID. Prior to being issued a unique User ID, users shall agree to uphold the User Agreement appended to this policy. The User Agreement may be amended from time to time as deemed appropriate by the College. Authorized users are solely responsible for all actions, including electronic messaging, taken while the User ID is in use. Authorized users are responsible for maintaining the confidentiality of their passwords and the security of their accounts.

4. PENALTIES

Any attempt to violate the provisions of this policy, regardless of the success or failure of the attempt, will result in disciplinary action. Disciplinary action may range from reprimand to loss of account privileges to maximum penalties afforded under College policies, which could include expulsion of a student from the College or the termination of employment for staff. Any attempt to circumvent local, provincial, federal, or international laws through the use of College owned facilities may result in litigation against the offender by the appropriate authorities. If such an event should occur, the College will fully comply with authorities to provide any information necessary for the litigation process.

Violation of Computer/Internet use could result in a criminal charge. Such violations would include: Unauthorized use of a Computer (Criminal Code section 342.1), Mischief (Criminal Code section 430.(1.1), Corrupting Morals (Criminal Code section 163), Making/Distributing/Selling/Possession of Child Pornography (Criminal Code section 163.1).

5. PRIVACY

The College respects users' privacy and under normal circumstances will not access users' accounts. However, the College reserves the right to examine the contents of users accounts should the need arise. Such circumstances might include suspected misuse of the facilities or protection of the integrity of the system.

6. PROVISION OF INFORMATION

Information provided on college facilities is subject to a number of Provincial and College policies including but not limited to: Freedom of Information, Copyright, and Confidentiality of Records.

Information providers must use official College data provided by the department that is normally responsible for maintaining that data. For example, the Registrar is responsible for program and course information. Information providers, therefore, must use the Registrar's data sources rather than create their own. Information provided must not consist of illegal or offensive material. Storage media remains the property of the College and the College retains the right to examine those contents at any time.

7. COMPUTER LABS

All students in good standing who are entitled to use the Computer labs are responsible for complying with the following regulations:

7.1 Faculty/Professor Lead Computer Labs

1. Students are to adhere to rules set by the professor or faculty that are leading the class.
2. The principle use for computer labs is for educational and academic purposes. Students are to refrain from using the Internet, e-mail, and chat lines, etc unless otherwise directed by the professor leading the class.
3. No pornographic, discriminatory, or offensive material is to be displayed, transmitted, or downloaded in the computer labs
4. All users must log-off before leaving the computer labs.
5. Only software provided by the college is to be used in the computer labs.
6. Computer labs are not to be used for commercial purposes.
7. Students are not to change the configuration of the machines. Problems regarding configurations should be referred to the IT department.
8. No food or drink is to be taken into the computer labs.
9. No amplification devices are to be plugged into computers.
10. No loud talking or any other disturbance is permitted in the computer labs.
11. No equipment is to be connected to the College network without prior approval by the IT department. The IT department may revoke this permission if it suspects that the equipment is compromising IT operations.

7.2 Open Computer Labs

1. Students are to adhere to the same regulations (as 7.1 above) when there is no professor/faculty leading the class.
2. Students are to respect and adhere to requests from the “Lab Monitors”. Students that do not comply with requests made by the Lab Monitors will be reported to the IT Department and may have their computer privileges revoked.
3. Computers are not to be used for recreational purposes (i.e. not related to course work) when computer lab workstations are at full capacity. The Lab Monitor may ask you to leave if you are engaged in recreational activities and there are students waiting for a computer to do course work.

8. COMPUTER LABS - CONTROL PROCEDURES

1. Users, who have complaints about the computer lab operations or about other users, should address them to Lab Monitors or to the IT Department.
2. Lab Monitors may be required to draw users' attention to the provisions of this policy. If a user fails to comply with the Lab Monitor's request, the Monitor will report the situation to the IT Department.
3. Computer lab users must comply with directions of Lab Monitors and staff. Account holders should review the Penalties section of this policy for the possible consequences of non-compliance.
4. The Computer labs may be closed from time to time, in whole or in part, for maintenance. As much notice as possible will be given to users.

9. COMPUTER ACCOUNT USER RULES

In consideration of the issuance to me of an Northern College computer account User ID, I agree that:

General

- I am the sole person authorized to use this User ID.
- I am solely responsible for all actions taken under my User ID while my User ID is valid.
- I will not allow others to use my User ID.
- I will not sell/lease/rent my account to another.
- I will not apply for a User ID under false pretenses.
- I will not use the facilities and/or services for commercial purposes.
- I will not delete, examine, copy or modify files and/or data belonging to other users without their prior consent.
- I will not evade or change resource quotas.
- I will not deliberately impede other users through mass consumption of system resources.
- I will not take any unauthorized, deliberate action that damages or disrupts a computing system, alters its normal performance, or causes it to malfunction, regardless of system location or time duration.
- I will not send, display, download, load, or print offensive and/or pornographic pictures, or messages
- I will not use obscene language
- I will not damage computers, computer systems or computer networks
- I will not violate copyright laws

- I will not use another's password
- I will not trespass in another's folders, work or files
- I will not intentionally waste limited resources
- I will not employ the Internet to commit a crime, or for commercial purposes
- I will not use chat lines (including ICQ), subscribe to inappropriate newsgroups, play games, or engage in any other inappropriate use

Electronic Messaging Systems

- I am responsible for all electronic mail originating from my User ID.
- I will not forge, or attempt to forge, electronic mail messages.
- I will not attempt to read, delete, copy, or modify the electronic mail directed to other users without prior consent.
- I will not send, or attempt to send harassing, obscene and/or other threatening email to another user.
- I will not send unsolicited "for-profit" messages or chain letters.
- I will not send unauthorized network broadcast messages

Network Security

- I will not attempt to use College Systems or Networks in attempts to gain unauthorized access to remote systems.
- I will not use College networks to connect to other systems in evasion of the physical limitations of the remote system.
- I will not decrypt system or user passwords.
- I will not copy system files.
- I will not intentionally attempt to "crash" Network systems or programs.
- I will not attempt to secure a higher level of privilege on Network systems than authorized.
- I will not willfully introduce computer "viruses" or other disruptive/destructive programs into the College network or into external networks
- I will not connect any devices to the College network without prior approval by the IT department. The IT department may revoke this permission if it suspects that the equipment is compromising IT operations.

Unauthorized Access (Hacking)

This may include using unauthorized user names, passwords, computer addresses or identities or modifying assigned network settings to gain access to computer resources and/or data, or otherwise attempting to evade, disable or "crack" security provisions of college or external systems.

Vandalism Of Data

Deliberate alteration or destruction of computer files is a Criminal Code offence (Section 430 [387]) and will be prosecuted. Under no circumstance may a user inspect, alter, delete, publish or otherwise tamper with files or file structures that the individual is not authorized to access.

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," and the introduction of viruses or chain letters.

Squandering Resources

Resources are shared and no user may degrade the systems by: unwarranted data space, time and bandwidth consumption through resource-intensive programs, unattended network connections and/or lengthy print jobs.

Sharing Of Account

The college's computing resources are allocated 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 system(s) 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. Faculty and staff are referred to the institution's policy on these matters.

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 computer user. Importation or distribution of such material (including, but not limited to racist material, hate literature, sexist slurs or pornography) requires an underlying academic or educational purpose.

Hostile Atmosphere

A hostile environment is created with the display of sexually explicit or violent images in public spaces, and/or the initiation of unsolicited communication with sexual content that contravenes the college's sexual harassment policy.

Harassment

Harassing or defamatory material may not be sent by electronic means, including email, or posted to news groups.

I have read and understood this User Agreement and I agree to use my account(s) in accordance with this document.

I accept full legal responsibility for all of the actions that I commit using the College's network according to any and all applicable laws.

I understand that from time to time the College network and attached equipment may fail unexpectedly while I am using them, and I will not hold the College responsible for lost time or data.