Northlands College Policy
Information Technology Acceptable Use

POLICY STATEMENT

This policy guides users of the Northlands College Information Technology (IT) infrastructure. It balances the employee's ability to benefit fully from information technology with the College's need for secure and effectively allocated IT resources. Employees who violate this policy will be subject to progressive discipline as outlined in article 18.2 of the Collective Agreement.

GUIDELINES

There are three usage types for the College's infrastructure: core, incidental, and unacceptable. Appendix A provides examples of these three usage types and may be used as a guideline when assessing use of information technology.

1. Core uses are activities required to conduct the business of the College. They help fulfill the department's mandate. The College's IT infrastructure primarily exists to facilitate Core College purposes.
2. Incidental uses are those which are neither explicitly permitted nor explicitly denied. Incidental applications never require any action or intervention by anyone at the workplace other than their user. Incidental usage that becomes an imposition on others or burdens systems is no longer incidental, but unacceptable, and is not permitted.
3. Unacceptable use represents actions of a serious nature and may result in reporting such activities to law enforcement authorities, the provincial and/or federal government. Unacceptable use can also impede the work of others or needlessly squander IT resources. Such unacceptable use may unintentionally damage the IT infrastructure, and may generate extra costs. Unacceptable use includes, but is not limited to:
    - Use, copy, or otherwise access anyone else's files without permission.
    - Use the College's IT infrastructure for activities that contravene the law, existing policies or regulations.
    - Use the College's IT infrastructure for any activities that are offensive or perceived to be offensive.
    - Distribution, downloading, engagement in or use of pornography.
    - The unauthorized access of, distribution and/or modification of College data, databases such accounting, human resources, student records.
    - Download data or introduce data from an external sources without ensuring that it is virus-checked, software compliant, security and privacy compliant, and compliant with Northlands College IT policies. Please note that all software is to be installed by the College's IT department.
    - Use any part of the College's IT infrastructure for personal financial gain.
    - Infringe copyright, intellectual or proprietary rights.
    - Permit unauthorized access.

- Alter, bypass, circumvent, damage, impair, impede, modify, restrict or have unauthorized use of any of the security components or systems of the IT infrastructure.
- Create or knowingly propagate computer viruses, privacy risks, security risks.
- Damage files, equipment, software, or data belonging to others.
- Use or attempt to use unauthorized access methods or abilities.

While the College does not prohibit limited incidental use of information technology for personal reasons, users should recognize that the primary intention of providing this resource is to support the core work of the College.

Without specific authorization, employees must not cause, permit, or attempt any installation of hardware or software, destruction or modification of data or equipment.
Employees should be aware that computer usage can be traced by site logs and other tracked information. The College reserves the right to access the contents of all files stored on its systems and all communications and messages transmitted through its Information Technology infrastructure.
Employees must not intentionally access sites or engage in practices on the Internet that have the potential to bring the College into disrepute. Access entails personal responsibility and employees are responsible for any activity carried out under their account. Employees who access the internet should be familiar with:

- copyright laws as they apply to software and electronic forms of information;
- applicable libel and slander laws, and
- this policy

Email that is of personal or transitory nature need not be archived. However, email that is an official record of the College is to be retained. Email is accessible under the terms of The Freedom of Information and Protection of Privacy Act. The use of the College's Information Technology infrastructure and Email is subject to monitoring and employees should have no reasonable expectation of privacy. Email, and the Information Technology infrastructure is for College purposes and not personal use.

Employees must not attempt to read another person's Email unless otherwise authorized. The email system is the property of the College. Employees should have no reasonable expectation of privacy in Email transmitted, received and stored on and/or through the College's system. An Email is the property of the College and is not a private employee communication (whether created or received).

It is unacceptable to send large files such as singing Christmas Cards or animated Valentine's greetings as attachments to email – such attachments can seriously affect the performance of the College's network.

Using College infrastructure to play games is an unacceptable use of a valuable resource and is not permitted.

Northlands College Policy
Information Technology Acceptable Use

Staff authorized to use a mobile computing device (including but not limited to laptops, tablets [such as iPads], and mobile phones [such as iPhones]) to carryout College business are responsible for protecting the confidentiality, integrity, and availability of College information and information systems. Staff should ensure that the mobile computing device is protected from theft or removal at all times that the device is not in their immediate possession. Staff are required to keep their mobile devices in their College-provided protective cases.

Staff should store all College materials, such as data, documents, email messages, spreadsheets, databases, programs etc. that were received, created or edited on office computers in the course of carrying out College business on network storage devices. Files of a departmental nature should be stored on the network storage devices assigned to their department. The use of network storage devices will provide for recovery of such materials in the case of loss.

Cellular phones are part of the College's technology infrastructure. Cellular transmissions are not secure and employees should use discretion in relaying confidential information. This policy also applies when employees use cellular telephones for email and internet access.

Policy Originated: December 2005	Approved by: President & CEO
Last Approved: January 2018	Signature: 

Appendix A

These are examples only and not exhaustive or inclusive.

Technology	Core	Core/ Incidental	Incidental	Incidental/ Unacceptable	Unacceptable	Against Existing Policy	Illegal
Phone	Answering an inquiry from a member of the public.		Making a brief personal call.	Making many personal calls & work calls answered by busy co-workers	Accessing 1-900 numbers	Using a College phone during office hours to buy and sell stocks	Recording phone conversations without permission.
Networked Computer	Sending an email to all the members of the OH&S committee with minutes of the last meeting.		Email to co-workers with birthday wishes, holiday greetings.	Sending emails with "puppies 4 sale" type messages	Distributing chain emails with large executable file attachments that waste limited network resources and contain viruses	Distributing a racist or obscene joke via email	Making a libelous or slanderous statement about a co-worker in an email.
Networked Computer on the Internet	Researching the latest development in your profession on the internet.	An email to a colleague deals with work and the schedule for your upcoming hockey tournament.	Browsing a news site during the lunch hour to keep up with world events.	Subscribing to a newsgroup on a College internet account that is of a personal nature.	Downloading and installing software on your computer.	Buying and selling stocks at work on the internet	Download, storing, distributing and selling child pornography.
Stand Alone Computer	Word processing, working on a budget		Preparing a roster for your child's soccer team over the lunch hour.	Preparing a roster for your child's soccer team, tying up the computer when co-workers need to access it.	Crashing the computer by installing a game or other software.	Using the spreadsheet on the computer to analyze the performance of your stock portfolio.	Running a pirated (illegal) version of a popular program on the computer.