NORTHERN LIGHTS COLLEGE

Information Technology Acceptable Use

Policy Number:	A-3.09
Category:	Administration
Effective Date:	February 12, 2016
Approval Process:	Administrative Policies
Approval Date:	February 12, 2016
Date Last Reviewed:	February 12, 2016

POLICY

Northern Lights College (NLC) provides information technology resources to NLC users to support the teaching, learning, research and administrative goals of the College. These resources are valuable community assets to be used and managed responsibly to ensure their integrity, security, and availability for educational and business activities.

Any materials, which may violate a person's right to work and study in an environment free from discrimination and/or harassment, are not to be accessed, stored, displayed, transmitted or otherwise linked to NLC's information technology services and equipment.

PURPOSE

Northern Lights College's information, network, and other information technology (IT) services are shared resources that are critical to teaching, learning, research, College operations, and service delivery.

The purpose of this policy is to:

- Establish responsibilities regarding acceptable use of information technology for all NLC users.
- Ensure the safe and respectful use of NLC's information technology for all NLC users.
- Ensure the security of the NLC computing infrastructure and its resources.
- Ensure confidential information of NLC students, employees, and others is protected.

The principles contained within this policy are:

- Technology resources are provided primarily to support and further the College's vision, mission and values.
- Users are expected to comply with all federal and provincial legislation as well as NLC policies and procedures.
- Users are responsible and accountable for their actions and statements in the electronic working and learning environment.
- Users are expected to use reasonable restraint in the consumption of valuable shared resources and to use resources in ways which do not interfere with the work, study, or environment of other users.
- Users of the College's IT resources should have no expectation of privacy when using IT resources. As a public institution, employees of NLC should be aware that all documents, e-mail messages, text messages, or other correspondence directed to, or transmitted by or through College owned equipment may also be subject to freedom of

information requests in accordance with the Freedom of Information and Protection of Privacy Act (FOIPPA) and the Canada Anti-Spam Law (CASL).
- Information technology resources provided by the College remain the sole property of NLC, who may exercise its rights of ownership without limitation.
- College network administrators may, without notification, remove any user from the College network if they suspect that the user's activity may violate legislation, regulations, College policy or compromise College assets.
- It is acknowledged that when technology users access external networks from within the College network that users are also bound by the policies of those external networks. Should there be a conflict between the policies of the external networks and the College network; the more restrictive policy will apply.

SCOPE

This policy applies to all NLC information and computing, communications, and networking resources whether individually controlled or shared, stand-alone or networked. It applies to all computer and communication owned, leased, operated or contracted by NLC including all personal computers, communication handheld devices, cell phones, digital storage devices , networks and associated peripherals, software, intranet and internet resources, or any other device connected to the NLC network and the users of these resources.

PROCEDURE

Monitoring and Privacy

The College regularly monitors its assets, and all non-College information transferred or stored on College assets may be reviewed as a result of this routine monitoring activity, and therefore users should have no expectation of privacy regarding any College or non- College information stored on or transmitted using College assets. Students using computer lab facilities during scheduled class time may be subject to monitoring at the instructor's discretion. Use of computer lab facilities at any time is subject to the routine monitoring activities.

Users can expect that their communications and the contents of their accounts will be treated as confidential. However, individuals have no right to absolute privacy when using information technology at the College. The College owns the information technology infrastructure and is responsible for its use.
Privacy does not extend to the following situations:
- Aggregate statistics about user accounts are not confidential (for example, data that indicates the amount of storage being used by particular accounts for .jpg files).
- As a normal part of system administration, information technology employees monitor levels of network traffic, use software that logs network activity, make copies of files, and maintain archives of these copies.
- Information technology employees may access any file, data, program, or e-mail in order to gather sufficient information to diagnose and correct network, hardware, and software problems.
- Information technology employees will compile and release otherwise confidential information when this is requested in accordance with this Policy.

The College information technology staff will gather and release information that is normally confidential only when specifically requested to do so and only when the request meets the following three conditions:

- The request is made by the appropriate office in the institutions. These offices are:
    - The Executive Director of Organizational Development and Human Resources with respect to compliance with Workers' Compensation legislation.
    - The Registrar (or another person authorized by the President to execute the legal obligations of the College with respect to legislation concerning freedom of information and protection of privacy) with respect to Freedom of Information requests or requests from law enforcement agencies for assistance with investigations.
    - The Vice President Academic and Research (in the case of students) or the Executive Director of Organizational Development and Human Resources (in the case of employees and associates) with respect to an internal College investigation.
- The request is made in writing, is reasonably specific in terms of the information required, and specifies to whom the information is to be released. The request to the Director of IT to gather and release information need not contain reasons why the information is required. The person and office issuing the request according to the policy has the obligation to establish and document these reasons and to ensure that the request and subsequent actions comply with the appropriate laws and policies under which they are acting.
- The request is addressed to the Director of IT who shall be responsible for fulfilling the request, even though the actual work of gathering the requested information may involve other information technology employees.

Prescribed Activities

All users of NLC Information Technology must:

- Comply with all applicable laws including the *Criminal Code of Canada*, *Copyright Act*, *BC Freedom of Information and Protection of Privacy Act*, *BC Civil Rights Protection Act* and *BC Human Rights Code*, and NLC policies in the course of using NLC Information Resources, and by licenses governing the use of computer programs, software and documents;
- Take appropriate steps to ensure the security of NLC's Information Resources by adhering to all applicable security measures including using and safeguarding all necessary passwords, and using encryption on portable storage devices;
- Secure their workstations when they are absent from them;
- Use only computer IDs or accounts and communication facilities which they are duly authorized to use, and use them for the purposes for which they were intended; and
- Respect copyrights, software licenses, intellectual property rights and contractual agreements.

Prohibited Activities

The following activities are strictly prohibited:

- Using Information Resources to access, create, view, listen to, store or transmit material that is harassing, obscene, abusive, illegal, pornographic, discriminatory or that otherwise violates applicable laws, NLC's agreements, policies or community standards, except if such use is part of assigned Northern Lights College duties or course work;
- Tampering with files, digital storage media, passwords, or accounts of others, misrepresenting one's identity as a sender of messages or the content of such messages or attempting to circumvent or subvert security measures;
- Intentionally developing programs or making use of existing programs that harass other users, or infiltrate a computer or computing system, or damage or alter the software components of a computer or computing system, or gain unauthorized access to other facilities accessible via the network;
- Using Information Resources, services or facilities for non-Northern Lights College purposes, projects, commercial or other external purposes
- Unauthorized release of private/personal and/or confidential information related to NLC's business, employees or students;
- Downloading and/or installing unauthorized programs, files or software; and
- Creating, transmitting, distributing, forwarding, downloading or storing any software, files or programs that infringe any copyright, trademark or intellectual property rights or which exposes NLC to unauthorized legal obligations or liability.
- Users may not send any electronic communication that contravene Canada's Anti-Spam Law (CASL)

    Any electronic communications that can be considered promotional, commercial, or could cause a person to believe that a monetary or commercial gain may be expected must not be transmitted without the express or implied consent of the recipient. Refer to CASL documentation for clarification.

Consequences of Policy Violation:

The College reserves the right to terminate or restrict the access privileges of a user whose activities negatively affect or pose a threat to a facility, another account holder, normal operations, or the reputation of the College.

Following due process, the College may take one or more of the following actions against any user whose activities are in violation of this policy or the law:

- Restrictions or removal of access to any or all College computing facilities and services
- Legal action that could result in criminal or civil proceedings
- In the case of students, disciplinary action under, Standards of Non-academic conduct.
- In the case of employees, disciplinary action up to and including termination
- Any equipment that violates NLC policy or negatively affects or poses a threat to a facility, normal operations, or the reputation of the College may be immediately disconnected, quarantined, or otherwise contained

STAKEHOLDERS

Board of Governors and NLC Executive
Director, Information Technology Services
NLC Administration
Instructors and Teaching Faculty
IT Staff
Users

RELATED POLICIES

- A-3.05 Modification of IT Infrastructure
- H-1.13 Code of Conduct (Standards of Ethical Conduct)
- A-3.02 Communications, General
- A-5.16 Copyright
- A-5.01 Records Management & Retention
- A-5.15 Student Discrimination, Bullying and Harassment Prevention
- A-3.04 Information Technology Password

RELATED REFERENCES

- BC College and Institute Act
- BC Freedom of Information and Protection of Privacy (FOIPOP) Act
- BC Personal Information Protection (PIP) Act
- BC Human Rights Code
- The Criminal Code of Canada
- Canada Copyright Act.
- "An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act (S.C. 2010, c. 23)" commonly referred to as the Canada Anti-Spam Law (CASL)

History

Created/Revised/Reviewed	Date	Author	Approved By
Created	June 4, 2014	Kelly Hein	Admin Committee
Revised	February 12, 2016	Peter Armstrong	Policy Committee

Next Scheduled Review Date

February 2021