Information Technology Acceptable Use

Policy Name Information Technology Acceptable Use	**Responsible Owner** VP Finance and Corporate Services	**Created** 2014 June
Policy Number A-3.09	**Approval Body** Policy Committee	**Last Reviewed/Revised** 2016 February
Category Administration	**Replaces** N/A	**Next Review** 2031 November

TABLE OF CONTENTS

PURPOSE

Northern Lights College's information, network, and other information technology (IT) services are shared resources that support teaching, learning, research, operations, and service delivery.
When used responsibly, these resources create a secure, respectful, and efficient digital environment that enhances collaboration, protects personal and institutional information, and ensures reliable access to technology that enables the success of students, employees, and the broader NLC community.

SCOPE

Northern Lights College 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.

This policy applies solely to NLC-owned systems and services and does not grant the College authority over users' personal devices beyond the scope of their interaction with NLC resources**.** Any materials that 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.

DEFINITIONS

Accounts – Any set of credentials that NLC provisions for its users to access NLC Systems or Devices.

Devices- Any electronic device or peripheral that NLC IT provides for its users

Information Technology Resources – Any Accounts, Devices or Systems NLC provides for its users.

Systems- Any on-premises or cloud hosted software platform that NLC IT provides for its users.

POLICY STATEMENT

Information Technology resources are provided primarily to support and further the College's vision, mission and values.

Information technology resources must never be used to access, create, view, store, display, or transmit material that is harassing, obscene, abusive, illegal, pornographic, or discriminatory, or that otherwise violates a person's right to work and study in an environment free from discrimination and harassment. This includes, but is not limited to, content that contravenes applicable laws, and College policies.

Users are responsible and accountable for their actions and statements in the electronic working and learning environment.

Users must maintain the integrity and security of Northern Lights College's information technology systems. Tampering with or accessing files, storage media, passwords, or accounts belonging to others is strictly prohibited. Users may not impersonate another individual, misrepresent their identity, or attempt to bypass or subvert network or system security controls. Account credentials must remain confidential, and users are fully responsible for all activity conducted under their assigned accounts. Workstations and devices must be secured when unattended to prevent unauthorized access or use.

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 Information Technology Resources. As a public institution, employees of NLC should be aware that all documents, e-mail messages, Teams messages, text messages, or other correspondence directed to, or transmitted by or through College owned equipment or systems 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.

Employees must ensure any device, either personal or NLC owned, that contains NLC information or has access to NLC information is password protected i.e. a screen lock on mobile devices.

Downloading, installing, or using unauthorized, unlicensed, or unapproved software, files, or applications on Northern Lights College systems or devices is strictly prohibited. All software and digital tools used on college-owned or network-connected equipment must be properly licensed and approved through the appropriate NLC processes. Users must not modify, delete, or install programs in a way that could compromise system performance, security, or compliance with college standards.

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.

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 NLC Information Technology Resources.

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 all access to Information Technology Resources, identify suspicious 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, information security and software problems.
- Information technology employees will compile and release otherwise confidential information when this is requested in accordance with this Policy.

Northern Lights College reserves the right to protect its information technology resources, infrastructure, and reputation from misuse. College network administrators may, without prior notification, remove or restrict a user’s access if their activities are suspected of violating legislation, regulations, College policy, or compromising College assets.

The College may take one or more of the following actions against any user whose activities breach this policy or applicable laws:

- Restrict or revoke access to any or all College computing facilities, systems, or services;

- Disconnect, quarantine, or otherwise contain any equipment that poses a threat to the network, normal operations, or the reputation of the College;
- Initiate legal action, which may result in civil or criminal proceedings;
- For students, pursue disciplinary action under the *Standards of Non-Academic Conduct*;
- For employees, impose disciplinary measures up to and including termination of employment.

SUPPORTING FORMS, DOCUMENTS, WEBSITES, 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 ACTS AND REGULATIONS

- 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) .