College of New Caledonia
CNC

Procedure Information	
Related to Policy No:	AD-IT-6.02
Approved by:	Executive Committee
Approval Date:	March 7, 2019
Executive Responsible:	VP Finance & Corporate Services
Administrator Responsible:	Chief Information Officer
Date of Next Review:	March 2024

Acceptable Use of CNC Information Technology
PROCEDURES

Definitions

1. Users: Faculty, staff, administrators, students, contractors, and any other individuals who use CNC facilities, accounts, email, internet, systems and services.

2. Accounts: Any password protected login for CNC systems provided by the College of New Caledonia, accessed either on campus or remotely, as a result of studying, working, or being physically present on campus.

3. CNC systems: All services, devices, and facilities that are owned, leased or provided by CNC and that are used to store, process or transmit electronic information. These include, but are not limited to:
    - computers and computer facilities;
    - shared and network drives;
    - computing hardware and equipment;
    - mobile computing devices such as laptop computers, smartphones, and tablet computers;
    - electronic storage media such as USB memory sticks and portable hard drives;
    - communication and collaboration software and networks;
    - enterprise resource planning software (Colleague);
    - third-party cloud solutions;
    - email systems;
    - telephone and other voice systems; and
    - software.

4. Single Sign-On (SSO): An authentication process that allows a user to access multiple applications (ie. Outlook, Colleague, EasyR, and SharePoint) with one set of login credentials.

Procedures

Some of the College of New Caledonia's IT systems are accessed through CNC's SSO computer ID and account authentication systems and must be used in a responsible fashion. The College also provides access to collaboration software, including third-party systems, in order to engage in College-related duties and activities. Using any of the aforementioned in ways that disrupt others, or interfere with their intended purpose, is not permitted.

Examples of prohibited behaviours include, but are not limited to:

- tampering with files, passwords, or accounts of others
- threatening, harassing, or discriminatory behaviour
- representing others when sending or receiving communication
- unauthorized use or access to accounts or facilities
- knowingly or negligently altering, disabling, or introducing a virus to any CNC computer or network
- sharing or downloading unauthorized data that contains personal information of others
- illegal activities, such as theft, fraud, slander, libel, defamation of character, stalking, identity theft, online gambling, spreading viruses, spamming, and plagiarism/copyright infringement
- usage that conflicts with existing CNC policies and/or any usage that conflicts with CNC's mission, goals, and values, or any other activity which would in any way bring discredit, disrepute, or litigation upon CNC
- copying, destroying, altering any data, documentation, or other information without authorization, or physical damage or unauthorized alteration of hardware
- accessing, downloading, or printing inappropriate content
- engaging in any activity that could compromise the security of CNC host servers or computers
- allowing unauthorized or third parties to access CNC's network and resources.

CNC email communications must be conducted with respect to CNC's standards of conduct. Account holders should be aware that all email messages and email data may be subject to freedom of information requests in accordance with the Freedom of Information and Protection of Privacy Act. It is the responsibility of users to protect private information that they have access to, in accordance with the Freedom of Information and Protection of Privacy Act.

Abuse of accounts

All users of CNC systems are required to comply with applicable laws, including but not limited to the Canadian Criminal Code, the Canadian Copyright Act, the B.C. Civil Rights Protection Act, the B.C. Freedom of Information and Protection of Privacy Act, and the B.C. Human Rights Code.
Users are also required to comply with and familiarize themselves with this policy and other applicable CNC policies, including but not limited to the Respectful Workplace policy, the Information Disclosure policy, and Standards of Ethical conduct policy.

College policies and current legal standards apply to all accounts. Under authorization from the appropriate College authority, ITS staff can disable an account and/or investigate complaints or suspicions of misuse.

The ITS department may access and monitor employee use of CNC email and internet systems by monitoring email server and internet network performance and retained logs, backups and archives on the College server. These records may be audited, are subject to provincial, and/or federal laws and may be used as evidence. While individual usage is not routinely monitored, unusual or high volume activities may warrant more detailed examination. Instances may include:

- For the purposes of producing the email in response to a legal requirement or other lawful investigation
- For the purpose of determining, as part of an investigation by CNC, whether there has been unacceptable use of email to abuse or harass other persons

- For the purpose of investigating allegations of misconduct or to provide materials to external investigative authorities lawfully investigating possible criminal conduct.

Responsibilities

Administrators should monitor and initiate investigations into any suspected inappropriate usage of CNC systems. Administrators should respect employees' privacy as much as possible while maintaining the appropriate use of all computer-based technology.

Employees should use systems for business purposes only and be aware that any information they transmit/receive may be monitored for appropriate business use.

Disciplinary action

Any violation of this policy will be treated in accordance with CNC employment terms, Collective agreements, and applicable policies. Violations of this policy may result in one or more of the following:

- Temporary or permanent revoking of access to CNC systems, internet resources, accounts, email and/or other IT resources
- Temporary or permanent revoking of CNC devices
- Disciplinary action according to applicable policies and collective agreements, up to and including suspension, expulsion or termination of employment.

Links to Other Related Policies, Forms, Documents and Websites

Acceptable Use of CNC Information Technology policy
Respectful Workplace policy
Information Disclosure policy
Administrative Personnel policy
Use of Mobile Communication Devices for Business Purposes policy
Resignation, Retirement and Completion of Employment policy
Standards of Ethical Conduct policy
Standards of Conduct: Student Responsibility and Accountability policy

Procedure Amendment Log

Amendment Number:	Date:
0	March 2019
1	June 22, 2021
2	