C-2

CANADORE COLLEGE

OPERATIONAL POLICY MANUAL

TITLE: Computing and Network Resources Acceptable Use Policy (AUP)

EFFECTIVE DATE: March 24, 2015

---

1. SCOPE

1.1 Authority

This policy is issued under the authority of the President.

1.2 Application

This policy is applicable to the entire Canadore College community using any device (eg. computer or mobile device) connected to the college data and telecommunication network from any access point, internal or remote. This policy includes all privately owned computers connected to the Canadore College network. In this context, the college community includes: all registered students, both full-time and part-time; all paid employees, full-time, part-time and casual; all others associated with the college including board members, retirees, or volunteers, and such visitors as are granted temporary user status by the college.

2. PURPOSE AND PRINCIPLES

2.1 Canadore College encourages the use of computing, network and telecommunication resources to enhance the learning and working environment of the college community. However, access to the computing, network and telecommunication environment at Canadore College is a privilege to be used in effective, ethical, secure and lawful ways that support the values of the College. The College will endeavor to create an atmosphere that balances respect for individual users with respect for college facilities and college and community standards.

2.2 Security and safeguarding College data, computing, network and telecommunication assets are the primary objectives of this policy.

2.3 The College will not act as censor of information available on our campus network, but will investigate properly identified allegations arising within the members/users to ensure compliance with applicable federal and provincial laws and with college policies and procedures.

2.4 Misuse of the college's computing, network and telecommunication resources may result in: a) immediate loss of access privileges, b) long-term outcomes including temporary or permanent loss of access privileges, and/or c) disciplinary action up to and including dismissal by the college. Violations of law will result in immediate loss of privileges and will be reported to the appropriate college and law enforcement authorities.

3. POLICY

3.1 Computing, network and telecommunication resources are provided primarily to support and further the college mission.

3.2 College community users are expected to comply with provincial and federal laws and Canadore College policies and procedures.

3.3 Members of the College community are responsible and accountable for their actions and statements in the electronic working and learning environment.

3.4 Members are expected to use reasonable restraint in consumption of these valuable shared resources, and to use them in ways that do not interfere with the study, work or working environment of other users.

3.5 Generally, with respect to computing and telephone accounts established for students and employees, there is a presumption of privacy. However, ITS (Information Technology Services) staff has access to all email, including data in transit and stored, telephone records and if an infraction is suspected, the information will be forwarded to the appropriate administrative staff to be investigated in accordance with the applicable college process.

3.6 College users accessing external networks are bound by their policies, and the more restrictive policy of either Canadore or the external network will apply.

4. UNACCEPTABLE USES

4.1 Unacceptable uses as outlined here are not limited to these examples. If an activity is suspected as being unacceptable, it should be reported to the Director of Information Technology. It will be reviewed for appropriateness and a recommendation will be forwarded to the Vice President, Finance and Corporate Services.

4.1.1 Unauthorized access: This may include using unauthorized user names, passwords, computer addresses or identities, or modifying assigned network settings to gain access to computer/telecommunication resources and/or data and telephone records, or otherwise attempting to evade, disable or □ crack□ security provisions of college or external systems. Access is limited to Canadore College owned computers and mobile devices exclusively. No personally owned computers of employees, students or guests are to be connected to the Canadore Administrative network without prior authorization by ITS. Exceptions to this include: 1) approved programs where student-owned computers and network access is an integrated component of the curriculum and approved by ITS, and 2) students, vendors, suppliers or guests who may choose to connect to the Canadore Student wireless network.

4.1.2 Vandalism of data: Deliberate alteration or destruction of computer files is a Criminal Code offence 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.

4.1.3 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, the playing of computer games, the downloading of audio and video files and the introduction of viruses or chain letters.

4.1.4 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. Users who exceed established limits must secure the approval from their immediate Supervisor/Manager and the Manager, Information Technology.

4.1.5 Sharing of accounts: 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 an appropriate college authority.

4.1.6 Commercial uses: The college system(s) (e.g. email) 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 institutions policy on these matters.

4.1.7 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.

4.1.8 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.

4.1.9 Long distance telephone: Long distance telephone services are provided for the exclusive use of conducting college-related activities. Long distance activities are monitored. This service should not be used for personal calls or for the profit of individuals.

4.1.10 Hostile atmosphere: The display of sexually explicit or violent images in public spaces and/or the initiation of unsolicited communication with sexual content contravene the college's sexual harassment policy.

4.1.11 Harassment: Harassing or defamatory material may not be sent by electronic means, including email and voice mail, or posted to news groups.

5. ROLES AND RESPONSIBILITIES

5.1 The President

The President is responsible for the overall management and operation of the College. The President is to ensure that the policy is implemented and that compliance is monitored.

5.2 Vice President, Finance and Corporate Services

The Vice-President, administrative services, is responsible for the effective implementation of this policy and to resolve any disputes arising over policy interpretation.

5.3 College Departments

5.3.1 Information Technology Services is responsible for ensuring compliance of this policy.

5.3.2 No other college department or personnel can authorize anyone to disregard this policy or its regulations and procedures.

6. EVALUATION

This policy will be reviewed every three years.