| ALGONQUIN COLLEGE DIRECTIVE | NO. OF PAGES<br>6 | DIRECTIVE NO.<br>A16 |
|---|---|---|
| | ORIGINATOR<br>College Information Technology Management Committee (CITMC) | |
| | APPROVED BY<br>President's Executive Committee (PEC) | |
| TITLE<br>ACCEPTABLE USE OF ALGONQUIN COMPUTER NETWORKS AND ACCOUNTS | EFFECTIVE DATE<br>1998.03.02 | REPLACES<br>New |

## POLICY

Algonquin College is committed to the creation of a technology-supported learning and working environment for all students and staff. To this end, the College has established the following standards with respect to the use of College networks and computer accounts.

## GENERAL

Computing and networking facilities at Algonquin College are provided for the use of Algonquin staff and students in support of the mission of the College. All staff and students are responsible for seeing that these computing facilities are used lawfully, ethically, and courteously.

The College is responsible for securing its facilities to a reasonable and economically feasible degree against unauthorized access and/or abuse. This responsibility includes informing users of expected standards of conduct and the resultant penalties for not adhering to them.

## RESPONSIBILITIES

The users of the network are responsible for respecting and adhering to local, provincial, federal and international laws, the Internet service provider's Acceptable Use Policy, as well as the policies of the College. Computers and networks can provide access to resources on and off campus, as well as the ability to communicate with other users worldwide. Such open access is a privilege, and requires that individual users act responsibly. Users must respect the rights of other users, respect the integrity of the systems and related physical resources.

## USER ID

Authorized users of College network facilities shall be issued a unique User ID. Prior to being issued a unique User ID, users shall agree in writing to uphold the User Agreement appended to this policy (Appendix A). The User Agreement may be amended from time to time as deemed appropriate by the College. Authorized users are solely responsible for all actions, including electronic messaging, taken while the User ID is in use. Authorized users are responsible for maintaining the confidentiality of their passwords and the security of their accounts.

## PENALTIES

Any attempt to violate the provisions of this policy, regardless of the success or failure of the attempt, will result in disciplinary action. Disciplinary action may range from reprimand to loss of account privileges to maximum penalties afforded under College policies, which could include expulsion of a student from the College or the termination of employment for staff. Any attempt to circumvent local, provincial, federal, or international laws through the use of College owned facilities may result in litigation against the offender by the appropriate authorities. If such an event should occur, the College will fully comply with authorities to provide any information necessary for the litigation process.

Violation of Computer/Internet use could result in a criminal offence. Such violations would include: Unauthorized use of a Computer (Criminal Code section 342.1), Mischief (Criminal Code section 430.(1.1), Corrupting Morals (Criminal Code section 163), Making/Distributing/Selling/Possession of Child Pornography (Criminal Code section 163.1).

## PRIVACY

The College respects users' privacy and under normal circumstances will not access users' accounts. However, the College reserves the right to examine the contents of users accounts should the need arise. Such circumstances might include suspected misuse of the facilities or protection of the integrity of the system.

## PROVISION OF INFORMATION

Information provided on college facilities is subject to a number of Provincial and College policies including but not limited to: Freedom of Information, Copyright, Confidentiality of Records, and Corporate Graphic Image.

Information providers must use official College data provided by the department that is normally responsible for maintaining that data. For example, the Registrar is responsible for program and course information. Information providers, therefore, must use the Registrar's data sources rather than create their own. Use of the College word-mark must comply with the College Graphic Image policy. Information provided must not consist of illegal or offensive material.

Storage media remains the property of the College and the College retains the right to examine those contents at any time.

## ACCESS CENTRES

All students in good standing who are entitled to use the Access Centres are responsible for complying with the following regulations:

1. The principal use for Access Centres is for educational and academic purposes.

2. Computers are not to be used for recreational purposes when Access Centre workstations are at full capacity. Game playing and the use of chat lines are not allowed between 7:00 a.m. and 7:00 p.m., Monday to Friday.

3. No pornographic, discriminatory, or offensive material is to be displayed, transmitted, or downloaded in the Centres.

4. All users must log out before leaving the Centres.

5. Only software provided by the college is to be used in the Centres.

6. Centres are not to be used for commercial purposes.

7. Students are not to change the configuration of the machines. Problems regarding configurations should be referred to the Lab Monitors.

8. No food or drink is to be taken into the Centres.

9. No amplification devices are to be plugged into computers.

10. No loud talking or any other disturbance is permitted in the Centres.

## ACCESS CENTRE CONTROL PROCEDURES

1. Users who have complaints about Access Centre operations or about other users, should address them to Lab Monitors or to Security staff.

2. Lab Monitors may be required to draw users' attention to the provisions of this policy. If a user fails to comply with the Lab Monitor's request, the Monitor will report the situation to College Protection Services.

3. College Protection Services, which includes the Security and Police Liaison functions for the College, are authorized to enforce this policy in the event of non-compliance. Access centre users must comply with directions of Lab Monitors, staff and Protection Services. Account holders should review the Penalties section of this policy for the possible consequences of non-compliance.

4. Users who wish to complain may refer to the Ombudsperson, the Students' Association, the Manager, Educational Technology Services or the Vice President, Student Life and Human Resources.

5. The Access Centres may be closed from time to time, in whole or in part, for maintenance. As much notice as possible will be given to users.

## RELATED POLICY

Student Misconduct (Directive E27)

*(original signed by)*
President

**APPENDIX A**

**ALGONQUIN COLLEGE**
**USER AGREEMENT**

In Consideration of the issuance to me of an Algonquin College Internet account User ID, I agree that:

**GENERAL:**

. I am the sole person authorized to use this User ID.
. I am solely responsible for all actions taken under my User ID while my User ID is valid.
. I will not allow others to use my User ID.
. I will not sell/lease/rent my account to another.
. I will not apply for a User ID under false pretenses.
. I will not use the facilities and/or services for commercial purposes.
. I will not delete, examine, copy or modify files and/or data belonging to other users without their prior consent.
. I will not evade or change resource quotas.
. I will not deliberately impede other users through mass consumption of system resources.
. I will not take any unauthorized, deliberate action which damages or disrupts a computing system, alters its normal performance, or causes it to malfunction, regardless of system location or time duration.

**ELECTRONIC MESSAGING SYSTEMS**

. I am responsible for all electronic mail originating from my User ID.
. I will not forge, or attempt to forge, electronic mail messages.
. I will not attempt to read, delete, copy, or modify the electronic mail directed to other users without prior consent.
. I will not send, or attempt to send harassing, obscene and/or other threatening e-mail to another user.
. I will not send unsolicited “for-profit” messages or chain letters.
. I will not send unauthorized network broadcast messages.

**NETWORK SECURITY**

. I will not attempt to use College Systems or Networks in attempts to gain unauthorized access to remote systems.
. I will not use College networks to connect to other systems in evasion of the physical limitations of the remote system.
. I will not decrypt system or user passwords.

. I will not copy system files.
. I will not intentionally attempt to “crash” Network systems or programs.
. I will not attempt to secure a higher level of privilege on Network systems than authorized.
. I will not willfully introduce computer “viruses” or other disruptive/destructive programs into the College network or into external networks.

I have read and understood this User Agreement and I agree to use my account(s) in accordance with this document.

I accept full legal responsibility for all of the actions that I commit using the College’s network according to any and all applicable laws.

I understand that from time to time the College network and attached equipment may fail unexpectedly while I am using them, and I will not hold the College responsible for lost time or data.

_____ _____

**Date** **Signature**