IT 01  Acceptable Use of Computer Networks and Accounts

Classification: Information Technology

Responsible Authority: Director, Information, Institutional Research and Technology Services (IIRTS)

Executive Sponsor: Vice President, Business Development

Approval Authority: President’s Executive Committee

Date First Approved: 1998.03.02

Date Last Reviewed: 2011.11.23

Mandatory Review Date: 2016.11.23

PURPOSE
To establish standards for the use of College networks and computer accounts.

SCOPE
All College employees and students

DEFINITIONS

Access Centre
A computer facility or lab operated by the College or by a department which provides computing resources or network access to students and employees

User ID
Identifying credentials that allow a user to access a computing resource. Generally a user ID is associated with a password which makes up a user credential

User Agreement
A set of principles and guidelines that govern the use of a network or computing system resource

Authorized User
A user who, through his/her user credentials, has been authorized to use a computing resource

User Credentials
A valid user ID and password, combined within an authentication system or method that grants the user access to a system or resource.

Authentication System
A system or method that matches an expected password to a provided password and grants or denies access to a resource through user credentials

POLICY
IT01 Acceptable Use of Networks & Accounts

1. The users of the College network are responsible for respecting and adhering to local, provincial, federal and international laws, 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.

2. 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 1). The User Agreement may be amended from time to time as deemed appropriate by the College. Authorized users are responsible for maintaining the confidentiality of their passwords and the security of their accounts. Authorized users are solely responsible for all actions, including electronic messaging, taken while the User ID is in use.

3. 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 employees.

4. 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.

5. Violation of Computer and 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);
   - Corrupting Morals (Criminal Code section 163);
   - Making, Distributing, Selling, or Possession of Child Pornography (Criminal Code section 163.1).

6. The terms “of use” cover any device connected to the College network, including personal devices that use the User ID and password to connect that device to the network or in situations where network access is granted without a User ID and password such as connecting to a network jack. The user of the device is solely responsible for adhering to this policy and related policies and laws for any device they connect to or cause to be connected to the College networks in any fashion directly or indirectly.

7. Each user of the College network is responsible for ensuring the security of his/her passwords and access to network connection. The sharing of access, through peer-to-peer technology, network access hosting, proxy hosting or other technologies including Bluetooth networking is not to take place on the College network except where it supports academic learning. Similarly, the accessing of another user’s account and network privileges where the other party is unaware of the access is strictly prohibited.

8. PRIVACY
8.1 The College respects the privacy of users 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.

9. PROVISION OF INFORMATION

9.1 Information created, stored and consumed on or by 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
   - College Corporate Image

9.2 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 wordmark must comply with the College Graphic Image policy. Information provided must not consist of illegal or offensive material.

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

10. ACCESS CENTRES

10.1 The College provides computer Access Centres and labs throughout its campuses. All students in good standing who are entitled to use the Access Centres are responsible for complying with the posted regulations for that Access Centre. Present standards are included in IT01: Appendix 2 and IT01: Appendix 3.

**PROcedures**

<table>
<thead>
<tr>
<th>Action</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 Requesting, Changing or Suspending Access Credentials for Staff</td>
<td></td>
</tr>
<tr>
<td>1.1 Enter changes in employment status of employee into HR/PAY. The changes are picked up automatically in the nightly batch cycle and appropriate account credentials will be created or suspended depending on status.</td>
<td>Human Resources</td>
</tr>
<tr>
<td>1.2 Instruct the user to immediately change his/her password on receiving an email from Information Technology Services advising of the creation of a new account or the resumption of a suspended account.</td>
<td>Immediate Supervisor</td>
</tr>
<tr>
<td>1.3 Immediately change his/her password to a strong password known only to him/her.</td>
<td>Account User</td>
</tr>
<tr>
<td>2.0 Requesting, Changing or Suspending Access Credentials for Students</td>
<td></td>
</tr>
</tbody>
</table>
IT01 Acceptable Use of Networks & Accounts

2.1 Enter changes in student’s enrolment status into GeneSIS. Any change in enrolment status entered into GeneSIS will be picked up automatically in the nightly batch cycle and appropriate account credentials will be created or suspended depending on status. A letter will be generated for new student accounts and mailed to the student.

2.2 Access his/her account via the ACSIS web portal by providing personal data known only to him/her.

2.3 Immediately update his/her password to a strong password known only to him/her.

SUPPORTING DOCUMENTATION
Appendix 1 Algonquin College User Agreement
Appendix 2 Access Centre Rules and Regulations
Appendix 3 Access Centre Control Procedures

RELATED POLICIES
SA 07 Student Conduct
AD 02 Freedom of Information
AA 34 Copyright
AA 35 Confidentiality of Student Records
AA 29 Protection of Student Information
AD 09 College Corporate Image

RELATED MATERIALS
Criminal Code of Canada
http://www.efc.ca/pages/law/cc/cc.html

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, or Possession of Child Pornography (Criminal Code section 163.1)

Freedom of Information and Protection of Privacy Act (FIPPA)
http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90f31_e.htm
ALGONQUIN COLLEGE USER AGREEMENT

On being issued an Algonquin College Internet Account User ID, I agree that:

GENERAL:
1. I am the sole person authorized to use this User ID.
2. I am solely responsible for all actions taken under my User ID while my User ID is valid.
3. I will not allow others to use my User ID.
4. I will not sell, lease or rent my account to another.
5. I will not apply for a User ID under false pretenses.
6. I will not use the facilities and/or services for commercial purposes.
7. I will not delete, examine, copy or modify files and/or data belonging to other users without their prior consent.
8. I will not evade or change resource quotas.
9. I will not deliberately impede other users through mass consumption of system resources.
10. 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:
1. I am responsible for all electronic mail originating from my User ID.
2. I will not forge, or attempt to forge, electronic mail messages.
3. I will not attempt to read, delete, copy, or modify the electronic mail directed to other users without prior consent.
4. I will not send, or attempt to send harassing, obscene and/or other threatening e-mail to another user.
5. I will not send unsolicited “for-profit” messages or chain letters.
6. I will not send unauthorized network broadcast messages.

NETWORK SECURITY:
1. I will not attempt to use College Systems or Networks in an attempt to gain unauthorized access to remote systems.
2. I will not use College networks to connect to other systems in evasion of the physical limitations of the remote system.
3. I will not decrypt system or user passwords.
4. I will not copy system files.
5. I will not intentionally attempt to “crash” Network systems or programs.
6. I will not attempt to secure a higher level of privilege on Network systems than authorized.
7. I will not willfully introduce computer “viruses” or other disruptive/destructive programs into the College network or into external networks.
IT01 Acceptable Use of Networks & Accounts

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.
ACCESS CENTRE RULES AND REGULATIONS

1. The College provides computer Access Centres mainly 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 Services 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 incident to College Security Services.

3. College Security 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 Security 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 Ombudsman, the Students’ Association, the Director, Information, Institutional Research and Technology Services or the Vice President, Business Development.

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.