



# COLLEGE OF THE NORTH ATLANTIC

## OPERATIONAL PROCEDURE

### TOPIC: ELECTRONIC INFORMATION SYSTEMS -- USE

<b>Procedure No.</b>	IS-501-PR	<b>Division</b>	Information Systems
<b>Supersedes</b>	n/a	<b>Board Policy Ref.</b>	GP-GR-807, GP-A-104 & GP-RR-904
<b>Related Policies</b>	IS-501, IS-502 & IS-504	<b>Effective Date:</b>	November 4, 2016 (R5)

## PROCEDURE

### 1.0 Acceptable Use Agreement

All users of the College's electronic information systems will comply with the guidelines and agreement governing acceptable use. See Appendix for a copy of the agreement. By virtue of using the College's electronic information systems, the College's employees, students, contractors, subcontractors and volunteers agree to abide by the provisions of all policies, procedures and Acceptable Use Agreement governing the use of the College's electronic information systems.

All academic and administrative managers will be responsible ultimately for ensuring compliance.

### 2.0 Software Usage Policy

All users of software will abide by the intellectual property obligations of the College as agreed to in the purchase and/or lease of such software as per the following guidelines:

- 2.1 For each piece of software installed on a system in a department where original distribution media was acquired, there must be an original set of distribution media kept in that department in an accessible yet secure place. Exceptions to this will be where network versions of software are installed on file servers where this software was installed by the Information Systems

- department. In these cases, Information Systems will keep licence documents and/or distribution diskettes.
- 2.2 For each piece of software installed on a system in a department where a licence document only was acquired, there must be a licence document kept in that department in an accessible yet secure place.
  - 2.4 The academic or administrative manager for each respective department will be ultimately responsible for all software licences acquired by that department.
  - 2.5 The breaking of the seal on a piece of software represents an official agreement that the College will abide by the terms and conditions laid out by the software developer.
  - 2.6 It will be illegal to copy software packages from one system in a department to another system in any department unless an additional licence is purchased.
  - 2.7 The Information Systems department will not install software on user's systems unless the user department can demonstrate proof of purchase.
  - 2.8 Some software developers demonstrate leniency when a user purchases a software package and installs that package on two or more systems as long as there is absolutely no likelihood that the software package will be running on the two systems at one time. For example, it may be permissible for an employee to purchase a software package and install it in his/her office and on his/her system where it is impossible to run both copies of the package simultaneously. The user department may consult Information Systems who in turn will check with software suppliers regarding policies of this nature.
  - 2.9 It will be illegal to transfer licensed software from a network file server to a system in a department.
  - 2.10 When a department purchases a network licence for a software product which does not contain mechanisms to ensure maximum user capacity, the department manager will ensure that there is sufficient capacity in that licence to accommodate the maximum number of simultaneous users of that software product.

- 2.11 Employees may not install personally owned software, shareware, or downloaded applications on the System or their desktop or laptop computer.
- 2.12 Employees who violate this policy or procedures will be subject to disciplinary action by the College.

### **3.0 Student & Faculty Web Pages**

Faculty, staff, and students may establish personal home pages on College systems subject to the following and as per Policy IS-502 and Policy IS-504:

- A. Such home pages will be established on systems and locations designated by the Network Operations Centre.
- B. The use of personal home pages will respect the College's conflict of interest guidelines, specifically:
  - Personal home pages shall not advertise any goods or services provided by the individual or his/her family,
  - Personal home page shall not provide web design and implementation on the College's system for an outside individual or organization.
- C. Content of the personal web pages will comply with the College's Acceptable Use Policy. Pages which contain sexually explicit, objectionable or libellous material or profanity may be deleted without warning to the owner.

### **4.0 Network Access for Non College Groups**

The College's computer and telecommunications systems will be used by the College community. Under circumstances where the College forms partnerships with others for the development of joint economic and/or educational goals, the College may provide network access as an in kind contribution to the partnership.

In these cases, the provision of network (Internet) access is subject to the following:

- A. All individuals given network access will agree to and sign the Acceptable Use Agreement.

- B. All individuals given network access will accept legal responsibility, which will hold the College blameless from abuse of the network.
- C. Access will be provided only where it does not impact upon the operation of the College.
- D. Individuals and/or groups given access shall be “not for profit” and will not be given funding for network access.
- E. Individuals and/or groups given access shall not use College resources for any commercial use.
- F. All accounts for individuals and groups will be established by the Information Technology support person at the site in collaboration with the President or delegate.
- G. The College’s Network Operations Centre will monitor accounts for acceptable use. Inappropriate use will result in the withdrawal of network access.
- H. Where other members of the partnership have network access through their own facilities, the College will not provide additional access.
- I. Network access will be consistent with the goals and objectives of the partnership.
- J. Any individuals or groups given access to the College system must have no expectation of privacy in any email or files which are stored on or have transitted through the computer system.
- J. The College will not be held responsible for additional costs, such as telephone charges, communications equipment rental, etc., required to provide access.

Approval History	
Approved by President	April 20, 1998
Revision 1	October 8, 1999
Revision 2	March 20, 2000
Revision 3	November 20, 2000
Revision 4	April 22, 2008
Revision 5	November 4, 2016



## ACCEPTABLE USE AGREEMENT

### General Provisions:

1. Computer facilities are owned by the College and will be used for College-related activities only. Hence only faculty, staff and students may access College computer facilities. In special circumstances, others may be granted access with approval of the Executive Team.
2. All access to the College computer systems, including the issuing of accounts and passwords, will be approved by the appropriate provincial IT Manager. All access to the administrative systems (e.g. PeopleSoft, SIRSI, etc.) will be approved by the authorized College office that has overall responsibility for the collection, maintenance and use of the information.
3. All access to network services such as electronic messaging, PeopleSoft, Sirsi, D2L, etc. through the use of College computing facilities will be governed by these policies.
4. Computer equipment and accounts will be used only for the purposes for which they are assigned and will **not** be used for commercial purposes or non-College related activities.
5. An account assigned to an individual will **not** be used by others and an individual will be held responsible for any action or policy violations committed using the account. The individual will be responsible for the proper use of the account, including proper password protection and ensuring that while logged into the account only he/she will have access to the account. Any individual caught using another user's account will be subject to discipline.
6. Authorized support personnel from computing services will monitor the use of facilities to ensure system integrity and system performance
7. Electronic data communications facilities will be for College-related activities only. Threatening, harassing, libellous, sexually explicit messages, messages sent for the purposes of data-bombing and commercial purposes and unwanted messages will **not** be sent. Users sending such messages will be subject to disciplinary measures.
8. Any attempt to degrade the performance of a computer system or to deprive authorized personnel of resources or access to any College computer system will not be acceptable and any user attempting such will be subject to disciplinary measures.

9. Loopholes in computer security systems or knowledge of a special password will not be used to damage computer systems, obtain extra resources, take resources from another user, gain access to system or use systems for which proper authorization has not been given. The existence of such loopholes/special passwords must be immediately reported to the system manager.
10. Users are permitted to use designated computer resources only in a manner consistent with these guidelines. **All** user files located on CNA's computer resources are subject to the ATIPPA and therefore may be subject to search and review. Generally, CNA will give notice before conducting a search.
11. Current students (those currently enrolled in a program within the College) are permitted to utilize designated computer resources in the non-commercial support of their studies and/or research **only** and must utilize them in a manner which complies with the policies and procedures of the College and this Acceptable Use Agreement. Student files and accounts may be deleted without warning when a student has terminated their program with the College.

#### Internet Provisions

1. The College has software and systems in place that monitor and record all College network usage.
2. The College reserves the right to inspect any and all files stored on any storage device comprising a component of the College network (including memory sticks/thumb drives, floppy disks or other external storage media connected to College resources) in order to assure compliance with policy.
3. Sexually explicit material may not be displayed, archived, stored, distributed, edited or recorded using the College network or computing resources, unless it is being used for educational purposes. Persons needing to use such materials must inform the College's IT manager.
4. The College **may** block access to websites and applications without notice particularly where access to such sites and applications negatively impact on network performance.
5. Use of any College resources for illegal activity is grounds for discipline and the College will cooperate with any law enforcement activity. The College will not necessarily inform the user of its cooperation with law enforcement.
6. Any software or files downloaded via the Internet into the College's network become the property of the College. **The College reserves the right to move or remove such content without notice. This action by the College in no way relieves the user of accountability for his/her action.**

7. No user may use College facilities knowingly to download or distribute pirated software or data.
8. No user may use the College's Internet or Local Area Network facilities to deliberately propagate any virus, worm, Trojan horse or trap-door program code.
9. Only those employees or officials who are duly authorized to speak to the media, to analysts or in public gatherings on behalf of the College may speak/write in the name of the College to any website, blog, newsgroup, chat room or groups such as Facebook.
10. Users releasing protected information via the use of network based resources – whether or not the release is inadvertent-- may be subject to disciplinary action.
11. The College tolerates non-business or non-study related research or browsing using the Internet during meal time or other breaks, or outside of work/class hours, provided that all other usage policies are followed, such usage is kept to a minimum and such usage does not interfere with work duties. The College reserves the right to revoke this privilege at any time, particularly if network traffic so generated interferes with the smooth flow of the College's Business or Academic applications. **Under no circumstances will the College tolerate any activities using its computer resources and systems which carry potential criminal, civil or quasi-judicial penalties.** Employees are encouraged to review the provincial government's policies governing Internet usage.
12. Users may not download or install any applications (e.g. Skype, file-sharing software etc.) using the College electronic information system.
13. Users may **not** use College Internet facilities or College Local Area Networks to download TV shows, movies, music, entertainment software or games or to play games against opponents over the Internet/LAN.
14. Users may not upload any software licensed to the College or data owned or licensed by the College.

### Violation of Policy

Offences will be dealt with in the same manner as violations of other College policies and may result in disciplinary action in accordance with existing Collective Agreement, Terms and Conditions of Employment or the Code of Discipline for Students. In such a review, the full range of disciplinary actions available, including loss of computer privileges for a specified

period of time, dismissal from the College and legal action may be considered. Violations of some of the above policies may constitute a criminal offence.