COLLEGE POLICY

Policy No. & Title: **C-210 Network Acceptable Use**
Policy Sponsor: Vice President, Finance
Reference Cmtee: Policy & Procedure Committee
Effective: 2023-07-01
Next Review: 2027-04-30

Purpose
The College is committed to providing a working and learning environment where all persons treat others with consideration and respect. Such consideration and respect extend to the use of the College's network and associated infrastructure; whereby those resources are made available to employees in support of their business-related activities, and to students in support of their learning, research, and job search objectives.

Against this background, this policy seeks to establish the expectations and guidelines regarding acceptable use of the College's network and associated infrastructure including all its associated physical and hosted instances.

Scope
This policy applies to all College students, employees, delivery partners, affiliates, volunteers, and contractors.

Definitions
Networked Infrastructure: The College's networked infrastructure includes all physical and virtual (cloud based) instances of, but is not limited to, servers, computers, printers and other peripherals, networking and communications devices, cables, scanners, photocopiers, telephones, and various software including the Learning Management System (LMS).

Spamming: The repetitive posting of the same text or nonsensical posts that have no substance and are often designed to annoy users.

Bumping The posting on old threads to keep them near the top of a list.

POLICY
Principles:

- The individual bears the primary responsibility for the manner in which they use the College's infrastructure. Likewise, the individual is responsible for the material they choose to access, send, or display.
- Access to the College's infrastructure is a privilege. Access is revocable at any time and without notice.

- Users understand their files and email are not completely private. The College System Administrators do not routinely access user files; however, they do have access to all user accounts, files, and email, and may access them at any time.
- Users are not permitted to connect any hardware devices to any networked infrastructure in the College, except with the College's authorization.
- Any personal devices brought to the College or connected to the College's networked infrastructure, whether for employment or learning purposes, is the sole responsibility of the individual; and the College assumes no responsibility for such devices, their use, or any subsequent loss or damage.
- Students are not allowed to bring any hardware or software into the college that is not approved by the College.

Note: To support environmentally friendly practices, users are asked to limit the amount of printing and to use paperless options where possible.

Application

1) **Appropriate** uses of the College's networked infrastructure are ones that:
   a) Support education the learning process
   b) Help students become knowledgeable, responsible professionals
   c) Respect for the rights of others
   d) Respect for the property of others
   e) Take consideration for others using shared systems, equipment, and facilities
   f) Respect confidentiality in the use of passwords
   g) Respect others' rights to privacy
   h) Use hardware and software only for the purposes for which they are intended
   i) Adhere to "netiquette" in communications via the network and Internet.

2) **Inappropriate** uses of the College's networked infrastructure are ones that:
   a) Grant any user unauthorized access, or to alter, destroy, remove and/or disclose data, information, equipment, software, or systems.
   b) Grant any user unauthorized the ability to duplicate, distribute or alter any licensed software, including software licensed by the College and licensed software accessed while using the networked infrastructure.
   c) Attempt to gain unauthorized access to any networked infrastructure or data or attempt to disrupt the normal operation of any networked infrastructure —at the College or anywhere on the Internet.
   d) Deliberately view or download content from undesirable sites from outside of the classroom and direct instructor supervision for the purpose of illustration and education of complex topics. Undesirable sites (as defined solely at the discretion of the College) are those that contain, but are not limited to:
      i. Hatred to minorities or any other group of people
      ii. Hacking and cracking information
      iii. Criminal or illegal activity
      iv. Content considered to be offensive

e) Use the College's e-mail system to attack other computer systems, falsify the identity of the source of electronic mail message, send harassing, obscene, threatening, or other unwanted electronic mail, attempt to read, delete, copy, or modify the electronic mail of others without their authorization, send "for-profit" messages, chain letters or other unsolicited "junk" mail.

f) Tamper with the College's networked infrastructure or building wiring or installing any type of electronic equipment or software that could be used to capture or change information intended for someone else.

g) Participate in a "denial of service" attack on any other computer, whether on or off campus.

h) Use College networked infrastructure for personal gain or illegal activities such as theft, fraud, copyright infringement, piracy, unsolicited email, electronic mail distribution abuse, or distribution of obscene material.

i) Use College networked infrastructure for file sharing, or any other activity that will negatively impact the availability of resources (e.g., large file downloads, peer-to-peer networking).

j) The installation of network electronic equipment inside the classroom that isn't specifically approved by the IT department, or by an instructor for the purpose of illustration and teaching; or outside the classroom under any circumstances. Network electronic equipment includes, but is not limited to routers, remote access devices, modems, wireless access points, or any other device that allow unauthorized access to the College's networked infrastructure.

k) The use of laptops, personal computers, or other devices on the College network unless explicitly authorized by the College. Laptop computers and mobile devices may be brought into the campus, but they may only be connected to either the College's sanctioned Wi-Fi network, or to a data connection available inside of a classroom.

l) Move, modify, substitute, or otherwise abuse any piece of computer, presentation or networking hardware unless expressly authorized by the College.

m) Theft of resources - the removal of hardware or software without permission

n) Alter hardware or software configurations without permission.

o) Use another individual's account, equipment or passwords or the granting to another individual access to the same.

p) Download and/or install any unauthorized software, games, shareware, tools, or utilities.

q) Deliberate over-extension of the resources of a system or interference with system processing (e.g., slowing down the system by downloading huge files).

r) Use computer systems which interfere with the normal operations of other users, both students and staff.

s) Infect the College's networked infrastructure with viruses or malware.

t) Disclose confidential passwords and/or access devices or information for accounts, equipment, telephone voice mail, and/or email.

u) Use networked infrastructure for commercial purposes not supported by the College.

v) Use networked infrastructure to download, exchange, distribute, send, display, or print pornographic, abusive, derogatory, or harassing messages or images.
w) Violate copyright.
x) Propagate any kind of malicious, unethical use or racist or hate literature.
y) Violate local, provincial, or federal laws.
z) Use networked infrastructure to play games, browse the Internet, message, use social media and/or any other unauthorized act during scheduled class/lab time.
aa) Printing non-school related materials.
bb) Display an inappropriate background on a computer monitor.

Electronic Mail (e-mail) Use

3) E-mail is the primary form of communication at the College, therefore:
   a) E-mails sent to co-workers, students, and external clients be professional and concise.
   b) E-mails should be clear in their content and neatly presented for ease in reading.
   c) All employee e-mail must have the College standard e-mail signature, customized to the specific contact information of the individual user (see C-210p Acceptable Network Use – Procedure (e-mail signature)).
   d) Tag Lines added to the bottom portion of e-mails should be limited in use. Tag lines related to the College may be added to enhance the e-mail. Topics such as new address, new phone numbers, information regarding a change in a business location, name change etc., are an appropriate use of tag lines.
   e) Tag lines espousing religious, ethnic, political, or illegal views are prohibited from use.
   f) All tag lines must be reviewed and approved by the staff member's manager.
   g) If a complaint is made in relation to a tag line, the line may be removed by the IT department without notice to the employee.

File Naming Convention

4) To ensure files can be found on the College's networked infrastructure, the College has adopted a file naming convention.
   a) All student files are to be saved in their appropriate directory and include the file naming abbreviations found in C-210p Acceptable Network Use – Procedure (Student file uploads).

Web Forum

5) The College supports a sense of community among students and has a variety of mediums for such communication. Examples include but are not limited to email, Microsoft Teams, Brightspace, etc. Everyone must adhere to the following guidelines:
   a) Messages that are potentially libelous, obscene, vulgar, sexually orientated, racist, hateful, threatening, or otherwise violate any law are not permitted.
   b) Messages or posts that contravene a) may result in personal repercussions for individual members, for which the College will take responsibility. Linking to other sites that contain or lead to such content is also not permitted.
   c) If discussing political events or individuals, comments/posts should be based on undisputed facts, rather than speculation or conjecture.

d) Users are expected to behave in a reasonable manner and with a spirit of goodwill, and opinions should be posted and read in good faith.
e) The normal language used in all communications is English, and users are requested to ensure that they contain correct punctuation and spelling.
    i. The use of other languages is acceptable when used to assist anyone who does not adequately understand English.
    ii. If abbreviations are used, users should be fully prepared to explain what they mean in a polite manner if asked.
f) The use of foul language and profanity will not be tolerated. This guideline also applies to external links.
g) Soliciting or volunteering to share copyright materials, materials that could be used to cheat, or the discussion of any form of law-breaking activities is not permitted.
h) Selling of certification vouchers is not permitted.

Related Policies
A-130 Copyright

Supporting Documents/Forms
C-210p Network Acceptable Use - Procedure