A. Background and Definitions

Niagara College is committed to protecting all students, employees, partners and the College from illegal or damaging actions by individuals, either knowingly or unknowingly. Effective security is a team effort involving the participation and support of every College student, employee and affiliate who deals with information and/or information systems. It is the responsibility of every connected user of the College’s network or electronic resources to know these guidelines and conduct their activities accordingly.

Confidential Information: For the purposes of this policy, confidential information may include, but is not limited to; student and sensitive corporate data, credit card information, customer/recruitment lists, College internal communications, corporate strategies, competitor sensitive trade secrets, courseware, and research data.

Data Owner: The individual (usually the department head) responsible for the oversight, quality, data governance and accessibility of specific College data assets, including the metadata for those data assets.

Disruption: For the purposes of this policy, a Disruption includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service and forged routing of information for malicious purposes.

Security Breach: This includes, but is not limited to, accessing data, or logging into a server or account that the individual is not expressly authorized to access unless these tasks are within the scope of regular duties or academic program.

User: For the purposes of this policy, User includes students and all employees who have been issued a Niagara College network account, and authorized guests.

B. Purpose

This policy outlines the acceptable use of computer, network and related electronic equipment at Niagara College. These rules are in place to protect students, employees and the College by...
reducing exposure to risks, such as viruses and malware attacks that compromise College data, network systems and services, as well as legal issues.

C. Policy Statements

1. This policy assumes that all College-purchased information technology (IT) related systems and software, including but not limited to, computer equipment, mobile phones, software, operating systems, storage media, access technologies and network accounts, are the property of the College. These systems are to be used for academic, administrative or operational purposes in serving the interests of the College, students, employees, and authorized guests in the support of teaching, learning, research and normal business operations.

2. General Use and Ownership
   a) Data created and saved on College systems, remains property of the College. Users should not assume their saved data will not be seen by others. Senior IT support staff or other managers may be authorized to access data if an issue arises. Authorized individuals within the College may also monitor equipment, systems and network traffic at any time or access files for security and network maintenance.
   b) The College reserves the right to audit networks and systems at any time to ensure compliance with this policy, while logging user activities and maintaining usage statistics for legal and compliance purposes.
   c) Users are responsible for exercising good judgement regarding the reasonableness of personal use of College IT equipment, systems and networks. Personal use should never impact another User in any way.

3. Security and Proprietary Information
   a) Users are to take all necessary steps to prevent unauthorized access to Confidential Information.
   b) It is highly recommended that information considered to be sensitive or vulnerable be encrypted. If it is College-owned data, the decryption key(s) must be provided to the area supervisor and IT Security Officer, or designate for safe keeping.
   c) Confidential Information or data is not to be transferred or downloaded to a portable device, external service, or cloud service for off-site use without approval from the Chief
Technology Officer (CTO) or designate or the Data Owner responsible for the information.
d) Passwords and network accounts are not to be shared. Users are responsible for the security of their passwords and network accounts.
e) Cyber security awareness training is mandatory for all college employees;
f) All desktops, laptops, tablets, mobile phones, and other College-issued devices are set with a password-protected screensaver with the automatic activation feature set at 15 minutes or less. This should not be disabled or blocked from operating.
g) Users are responsible to secure their devices by logging off or locking them when the device will be unattended.
h) All computers or mobile devices used by students, employees and/or visitors, connected to the College network, regardless of ownership, should be continually executing virus-scanning software with a current virus database when possible.
i) Users are to use extreme caution when opening emails, links and attachments received from unknown senders to avoid potentially compromising College systems and information. The IT Service Desk is to be notified immediately if the User believes their account or computer system may have been compromised.

4. Unacceptable Use
The following activities are strictly prohibited:
a) Violations of the rights of any person, company or institution protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of pirated or other software products that are not appropriately licensed for use by the College;
b) Using College resources to import or export software, technical information, encryption software or technology, in violation of international or regional export laws;
c) Intentional introduction or the use of malicious programs into/onto the network or College server infrastructure (e.g. viruses, worms, key loggers, Trojan horses, email bombs, etc.);
d) Revealing your account password to others or allowing use of your network account or College IT equipment by others;
e) Making fraudulent or other business offers of products, items, or services originating from any College issued network account that are not related to College operations;
f) Affecting Security Breaches or disruptions of network communication;
POLICY GROUP: NC200 – Information Technology  
POLICY TITLE: Information Technology Acceptable Use & Security Awareness

5. **Unacceptable Communications Activities**
   a) Sending unsolicited email, other text or social media messages, including the sending of junk mail or other advertising material to individuals who did not specifically request such material (e.g. email spam or spim). This also includes knowingly violating the Canadian Anti-Spam legislation using College resources;
   b) Any form of harassment via email, telephone or messaging, whether through unacceptable language, frequency or size of messages;
   c) Unauthorized use or forging of email header information;
   d) Solicitation of email for any other email address, other than that of the poster’s account, with the intent to harass or to collect replies;
   e) Creating or forwarding chain letters, Ponzi or other pyramid schemes of any type; and
f) Posting the same or similar non-business-related message to large numbers of social media or news groups using a Niagara College network or social media account unless that account is authorized to do so.

6. Failure to Comply
Violation of this policy could result in reputational damage, legal action and/or financial loss to the College. Failure to comply with this policy may result in the suspension or revocation of a user account, including immediate suspension of an account pending investigation.

a) Students found in violation of this policy may be subject to disciplinary sanctions up to and including expulsion pursuant to the Student Code of Conduct.

b) Employees found in violation of this policy may be subject to disciplinary sanctions up to and including termination pursuant to the Employee Code of Conduct.

c) When it has reason to believe that College issued IT equipment, systems or software have been used to commit a criminal offense, the College will inform the police.

D. Related Documents

Policy: NC400 Social Media
NC600 Employee Code of Conduct
NC800 Student Code of Conduct

E. Document History

<table>
<thead>
<tr>
<th>Date</th>
<th>Approval/Review/Key Change(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>February 2, 2021</td>
<td>New policy to merge three former practices:</td>
</tr>
<tr>
<td></td>
<td>• Computer &amp; Network Use</td>
</tr>
<tr>
<td></td>
<td>• Computer Security</td>
</tr>
<tr>
<td></td>
<td>• Use of Mass Email</td>
</tr>
</tbody>
</table>
