NORQUEST COLLEGE

STANDARD	ACCEPTABLE USE
Owner: **BTS**	Approved Date: **January 23, 2023**

SUMMARY

This standard outlines the acceptable use for individuals utilizing NorQuest provided computer equipment and is in place to protect both the user and NorQuest. Inappropriate use of computer equipment exposes NorQuest to risks including virus attacks, compromise of network systems and services, availability of services and bandwidth in the pursuit of the organizational goals and legal issues. This standard enforces the principle of defense in depth and monitoring the effectiveness of security controls, while ensuring compliance with organizational, legal and regulatory requirements.

BTS has the responsibility to ensure appropriate practices are adopted to conform to this standard and the Digital Security Policy that it supports.

APPROVAL

Approved by:	Dave Melanson	**Position:**	Director, Business Technology Services (BTS)
Signature:	David Melanson	**Date:**	January 20, 2023
Approved by:	Jill Matthew	**Position:**	VP, Administration & Chief Financial Officer
Signature:	B. Jill	**Date:**	Jan 23/2023

SCOPE

All users, employees, contractors, consultants, third party business associates, temporary/other workers and Board of Governors at NorQuest must adhere to this standard as it applies to the digital assets of the organization.

AUTHORITY

This standard has been created under the authority of Corporate Services and Finance & Business Technology Services (BTS) which maintains the right to ensure that this standard is adhered to.

ENFORCEMENT

Any NorQuest user found to have violated this standard may be subject to disciplinary action including, but not limited to, termination of employment. Any violation of the standard by a temporary worker, contractor or vendor may result in, but not limited to, the termination of their contract or assignment with NorQuest. As obligated by provincial and federal laws, NorQuest will notify appropriate law enforcement agencies when it appears that any applicable laws have been violated.

EXCEPTIONS

A request for exception to this standard must be submitted for approval to the Director of BTS by following the process as described in the Digital Security Exception Request Procedure. Granted exceptions will be for up to a one year term and will be reviewed annually at which time the exception may be revoked, revalidated or extended for another one year term. Exceptions will be maintained by BTS.

STANDARD

1. General

1.1. NorQuest College provides computing/IT resources to students, employees and authorized guests in order to effectively operate the college and provide appropriate education support and services.

1.2. Using college computing/IT resources for any private or commercial gain other than those sanctioned by the college in writing is strictly prohibited.

1.3. Users are permitted to use NorQuest computing resources for limited personal purposes provided that they exercise good judgment and such use is lawful and does not injure, harm or tarnish the image, reputation and/or goodwill of NorQuest and any of its users; and, provided that such use does not violate the college code of conduct, interfere with the performance of their regular duties, or disrupt college operations.

2. User ID's/Identity

2.1. Each individual using NorQuest College computing/IT resources is responsible for all activities performed under their assigned user identity.

2.2. Users shall not attempt to mask, obscure or falsify their identity or utilize an unauthorized identity while using NorQuest computing/IT resources.

2.3. Impersonating a college employee or student by using their e-mail or internet address or electronic signature is strictly prohibited.

3. Endpoints

3.1. It is prohibited for the user to (without explicit permission in writing):

3.1.1. change or alter in any way registry settings or system files;

3.1.2. load or install software on the local desktop. If the user has a business need for specific software to be installed on their local machine, they must follow established procedures by making the request through the Service Desk;

3.1.3. set-up file sharing (e.g. Bit torrent or similar technologies);

3.1.4. activate any form of Personal Area Network (PAN) on their local desktop or computing device;

3.1.5. store music, videos or other copyrighted materials that have not been sanctioned/purchased or otherwise authorized for use by the College on their local desktop or network.

3.2. Users must never connect any unauthorized networking technology to their workstation, laptop or wired network ports.

3.3. Users must either lock, or log out of, their workstations or laptops when leaving them unattended.

4. Network

4.1. Users shall not modify assigned network settings to gain access to computer resources and/or data.

4.2. Use of network inspection/scanning/capture technologies is strictly prohibited.

4.3. Users shall not intentionally introduce malicious programs onto the network or college computing/IT devices (e.g., viruses, worms, Trojan horses, e-mail bombs, key-loggers, etc.).

4.4. Introducing unauthorized computing devices onto college networks, including but not restricted to web servers, ftp servers, email servers, game servers and computers equipped with peer-to-peer file sharing software through which files are made available to other users, are prohibited unless authorized by BTS.

4.5. Obtaining configuration information about a network or system for which the user does not have administrative responsibility is strictly prohibited.

5. Software

5.1. Software that has been licensed to NorQuest for business use must not be installed on personal equipment without the express prior approval of the Director of BTS or designate.

5.2. Copying – All software protected by copyright must not be copied except as specifically stipulated by the owner of the copyright or otherwise permitted by copyright law. Protected software may not be copied except pursuant to a valid license or as otherwise permitted by copyright law.

5.3. Licensing – The number and distribution of software copies must be handled in such a way that the number of simultaneous users does not exceed the number of original copies purchased, unless otherwise stipulated in the purchase contract.

5.4. Copyrights – In addition to software, all other copyrighted material (text, images, icons, programs, videos, music, etc.) must be used in conformance with applicable law. Legitimately, copied material must be properly attributed.

5.5. Users shall not break or otherwise circumvent Technical Protection Measures (TPM's) or any other security on software or other digital materials used at the college.

6. EMAIL & Electronic Communications

6.1. The provisioning of NorQuest e-mail is to accomplish the mission of the organization and will be used for such purposes.

6.2. Before launching e-mail attachments, users must verify their source. If the source is unknown or cannot be verified, users should call the Service Desk for assistance.

6.3. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material is prohibited and may be in violation of Canada's Anti-Spam Legislation (CASL).

6.4. Creating or forwarding "chain letters", or other "pyramid" schemes, of any type is prohibited.

6.5. Making a political comment by institution email is prohibited.

6.6. E-mail content should reflect the values of NorQuest and therefore should not be of a questionable, obscene or inappropriate nature, or convey any information that could be injurious to the institution.

6.7. E-mail must not jeopardize the institution's commitment to confidentiality and security of information. All e-mail sent over the Internet must follow institution guidelines regarding protection of privacy and security of information and attachments.

6.8. The Service Desk must be notified immediately when the source of an e-mail is unclear, or where harm towards NorQuest or possible threat to digital security is suspected.

6.9. Files being worked on by a user must not be e-mailed to their home, sent to a personal e-mail address for access outside of the work environment or copied to some form of removable digital media. If users must work on files at home, the primary method is accessing the files via the institution's Virtual Private Network (VPN).

6.10. Users must not save any NorQuest related information contained in documents or e-mail communication to their home or other computers.

6.11. The use of personal e-mail accounts while at work (Hotmail, Gmail, etc.) is permitted on a limited basis. The user must not use personal email to conduct business on behalf of NorQuest.

7. Internet

7.1. Web browser access is strictly prohibited to sites that:

7.1.1. poses a risk to the security and performance of the college network;

7.1.2. potentially incurs legal liability to the institution or the individual user;

7.1.3. damages the institution's reputation, or;

7.1.4. violates the Code of Conduct or College Values.

7.2. Sites that may be blocked and/or monitored for access are:

7.2.1. banner ad service sites;

7.2.2. web-based chat sites or services;

7.2.3. hacking sites;

7.2.4. violent or offensive sites;

7.2.5. cloud based storage sites or services;

7.2.6. remote proxies;

7.2.7. gambling sites;

7.2.8. sites containing pornographic, adult or sexually explicit material;

7.2.9. sites where content is illegal (breach of criminal law); and,

7.2.10. sites that are otherwise deemed to be incompatible with our Code of Conduct and Values.

7.3. The use of NorQuest resources to store, display, or disseminate child pornography or hate crimes is strictly prohibited. As obligated by provincial and federal laws, NorQuest will notify appropriate law enforcement agencies when access to child pornography or hate crime web sites has occurred.

7.4. College computing resources must not be used for the creation, transmission, storage, access or viewing of materials which in any way contribute, support or promote actions which are prohibited on the basis of harassment and/or discrimination including but not limited to the categories of: Harassment, Sexual Harassment, Pornographic, Racial/Ethnic/Cultural Harassment, Discrimination, Hate Literature, Systemic Harassment/Discrimination & Reprisal

7.4.1. This restriction is not intended to interfere with legitimate and appropriate uses for teaching purposes.

8. Information Handling / Data Access

8.1. Users shall not attempt/access college data that that is beyond their expressed approved permissions.

8.2. Users shall not modify/remove data or files owned by someone else without written permission.

8.3. All college data or records are to be stored on NorQuest owned or approved network drives and shall **NOT** be stored on local drives (on your PC, laptop or other digital device) or unapproved cloud-based services to ensure appropriate backup and data custody can be maintained.

8.4. Users must ensure that files containing confidential data are stored in appropriately secure locations.

8.5. All storage devices such as CDs, USB memory sticks, Smartphones, cell phones, laptops and other removable media containing institution data must be securely maintained by the user. This means that the device shall be either kept in your possession or locked in a storage location like an office filing cabinet, lockable desk drawer or safe when not in use.

8.6. While in transit, institution data storage devices should be secured as noted in the Data Transmission Standard.

8.7. Users must take appropriate precautions to ensure that college information is only disclosed to individuals authorized to receive that specific information.

8.8. It is strictly prohibited to take individually identifiable information or records from NorQuest's facilities or systems to your residence or another non-work environment. This includes:

8.8.1. student records;

8.8.2. NorQuest systems, business or research records;

8.8.3. health related information;

8.8.4. user records; or,

8.8.5. anything that includes personal information unique to an individual.

These files must be accessed via an institutionally provided storage mechanism or VPN to the NorQuest network and not stored on the laptop or device.

8.9. All files must be scanned for malicious software before being loaded onto institution networks, storage devices, workstations or laptops.

9. Instant Messaging

9.1. Skype for Business functions as the institution approved IM client and is for internal business use.

9.2. Access to public IM networks for College business is prohibited.

9.3. Parties to a conversation may save a copy of the IM conversation. Conversations will be saved in a folder in the users Outlook client.

9.4. The exchange of user credentials (usernames or passwords), confidential or personally identifiable information in an IM session is prohibited.

9.5. Sending messages that could be interpreted as being improper or injurious to NorQuest, such as junk, spam or chain messages, or information relating to pyramid schemes over IM is prohibited.

9.6. All IM conversations may be monitored and/or logged.

10. Service Desk Laptops (loaner laptops)

10.1. All files copied to Service Desk Laptops (SDL's) must be removed before the SDL is returned to the Service Desk.

10.2. Before configuring a SDL for network access (for example, Cisco AnyConnect VPN), users must obtain Service Desk approval.

10.3. Users must not load software onto SDL. The Service Desk must approve and load all software onto a SDL.

10.4. All SDL's must be returned the day they are expected. Special authorization from the Service Desk must be obtained for extending SDL sign-outs past their due dates.

11. Smart Phones

11.1. Users are permitted to install approved applications from trusted sources (e.g. Google Play or iTunes) on their institutionally issued Smartphone, provided the applications do not impact institutionally installed applications.

11.2. The user is reminded, in relation to data that may be stored on your Smartphone, that it is strictly prohibited to take individually identifiable information or records from NorQuest's facilities or systems to your residence or another non-work environment. (NOTE: Business contact information is not considered individually identifiable information under privacy legislation).

11.3. Users must not attempt to disable any of the security features as provisioned (or updated from time to time) by NorQuest or jailbreak the devices.

11.4. Users issued a NorQuest Smartphone are responsible for the security of the device regardless of where the device is used (for example, in the office, at a user's place of residence or in any other location such as a hotel, conference room, car or airport).

11.5. The camera functions on NorQuest issued Smartphones are available for users to use; however, taking photos or video of NorQuest data is strictly prohibited.

DEFINITIONS

1. **Commercial Gain** - A gain, usually financial in nature, accruing to the benefit of a business/corporation or other entity either registered or unregistered, not to the benefit of the college.

2. **Jailbreak** – modify (a smartphone or other electronic device) to remove restrictions imposed by the manufacturer or operator, e.g. to allow the installation of unauthorized software.
3. **Network inspection/scanning/capture technologies** – are software or hardware devices that capture network packets or frames that are used on the communications network of NorQuest College.
4. **Private Gain** - A gain, usually financial in nature, accruing to the benefit of an individual, not to the benefit of the college.
5. **Technical Protection Measured (TPM)** - include technology that provides digital locks preventing individuals from undertaking a variety of actions, such as copying, printing or making alterations, or controlling viewing; and, often operate alongside Rights Management Information associated with copies of works that usually identify the owner or author of the work and define the types of permitted access and/or track usage.
6. **Virtual Private Network (VPN)** - is a network that is constructed over a public network — usually the Internet — to connect remote users or regional offices to a company's private, internal network. A VPN secures the information using encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted. This type of network is designed to provide a secure, encrypted tunnel in which to transmit the data between the remote user and the company network, and thus the name "Virtually" private network.

REVISION HISTORY

Date	Version	Author	Summary of Changes
Mar 15, 2017	0.1	Curtis L. Blais	Initial Draft
Mar 16, 2016	0.2	Curtis L. Blais	Minor wording updates
Aug 9, 2017	0.3	Curtis L. Blais	Updated scope text
Sep 24, 2017	0.3a	Curtis L. Blais	BTS/Faculty Comment Updates
Dec 5, 2017	1.0	Curtis L. Blais	Signed Version
Nov 2, 2021	1.1	Curtis L. Blais	Updated the Dept/Div. to match current organization.
Jan 20, 2023	1.2	Dave Melanson	Data classification changed from Confidential to Public after being reviewed by Compliance
Jan 23, 2023	1.3	Dave Melanson	Signed Version