Acceptable Use of Technology Resources

Technology resources at New Brunswick Community College (NBCC) support the educational, instructional, research, and administrative activities of the college, and using these resources is a privilege. As a user of these services and resources, you have access to sensitive data and to internal and external networks and systems therefore it is expected that you use these resources in a responsible, ethical, and legal manner.

- Users are given authorization to use technology resources to fulfill the functions of their jobs.
- All Users will have a personal responsibility for safeguarding all proprietary information, which includes but is not restricted to sensitive documents and information, from disclosure to unauthorized parties.
- Users are obligated to follow NBCC Information Security Management Systems (ISMS) Policy [Policy 2808] and any processes or procedures supporting ISMS while using NBCC Technology Resources.


**PURPOSE**

This guideline supports the high-level policy statements defined in the Information Security Policy. The purpose of this guideline is to clearly illustrate what is considered to be acceptable and unacceptable use of NBCC’s information systems, and to ensure that there is as much clarity as possible about the boundaries of acceptable and unacceptable use of the technology resources to which users have access.

**SCOPE AND LIMITATIONS**

This policy document applies to all NBCC Users (staff and faculty), contractors, suppliers and other individuals affiliated with Third Parties who have access to NBCC technology resources and information systems.

- It is the responsibility of the user to know the guidelines outlined in this policy and to conduct activities accordingly.
- Each user is personally responsible for the control of his/her equipment, including the installed software.

**1.0 DEFINITIONS**

None

**2.0 IMPLEMENTATION**

**2.1 Personal Use**

The primary purpose for NBCC’s Information systems is for College business use. Users will make limited, infrequent, or incidental use of NBCC systems for personal use.

Personal Use of NBCC Information Systems will:
• Adhere to NBCC Security Policies and Guidelines;
• Not interfere with NBCC Business, individual’s productivity, or their colleague’s productivity;
• Not adversely affect NBCC’s ability to provide effective Computer Systems; and
• Not adversely impact on NBCC’s computing costs.

The email system is provided to support NBCC’s business activities. Personal email, (i.e. communication between individuals or parties which is not in support of NBCC’s business activities), whilst not prohibited, will be kept to a bare minimum and will be carried out in a manner which does not negatively affect the use of NBCC’s systems for business purposes.

2.2 Monitoring

• For security and network maintenance purposes, authorized individuals within NBCC will monitor equipment, systems, and network traffic at any time.
• NBCC shall scan all email and internet traffic for malicious software. Any email that contains malware or any website which is a known source of malware shall be blocked.
• Emails that contain potential harmful attachments shall be blocked, e.g. executable files as attachments, shall be blocked.
• Non-business chain emails or other promotional emails circulated within the organization shall be removed.

2.3 Data and Confidentiality

• The user is responsible for confidentiality and protection of personal data stored on NBCC’s Information Systems. Personal files are not the responsibility of NBCC IT staff.
• Users will exercise caution over disclosing their or a co-worker’s contact information (Email address / Phone No) outside of NBCC to prevent abuse of email services.
• Users are responsible for handling NBCC Information and Technology Resources as per its level of data classification.
• Users will not share any NBCC information which is classified as "Internal" or "Confidential" outside NBCC unless authorized. Information that users consider sensitive or vulnerable will be classified as per the data classification rules, and controls will be placed that are apt for such classification.
• Users shall not use third party cloud storage services like Google Drive, iCloud Drive or personal One Drive etc. for storing NBCC Information.
• Users shall not use public email services like Gmail, Hotmail etc. for sending/receiving business emails.

2.4 Property and Compliance

• Users will adhere to all intellectual property and copyright law. Users will always obtain copyright holder’s permission before downloading information from the internet or other public computer systems.
• Users will not install any pirated, unauthorized software on NBCC Information Systems.
• All software installed on college owned resources requires the pre-approval of the IT department.
• No student related information of any kind and no confidential information regarding NBCC will be shared outside NBCC unless authorized, including sharing over social media.
• Use of NBCC Technology Resources is governed by Federal and Provincial laws related to data, information security and privacy.
• All intellectual property rights in computer data, computer files and databases created or altered during the course of employment will be property of NBCC. On termination of employment, users will return all copies of such data, files, and databases in their possession.

2.5 Security

• Users will not circumvent user authentication or security of any host, network, or account.
• Users will inform the IT helpdesk of any circumstance that may indicate a breach of security or other risk to the integrity of NBCC’s information system.
• Users should only visit trusted internet sites to avoid malware and viruses.
• Users should not open any suspicious email messages, attachments or click on suspicious links in emails. If a user suspects an email is suspicious, they will report it using “Report a Phish” button in Outlook.

2.6 Passwords and Login-IDs

• Every user will have a unique login ID and password to access information systems of NBCC. Users will be responsible for setting their passwords as per the Access Control Guidelines and ensuring that their password is protected.
• Access to computer accounts is limited to your individual network account and only employees are permitted to use NBCC owned technology resources.
• In order to prevent unauthorized use, users will ensure that they do not divulge their password to any other person including any co-worker.
• Users will not write down their passwords on sticky notes but protect them by committing them to memory.
• Users will not leave their computer unattended. Passwords should be protected as per NBCC password guidelines and not shared with anyone. The security of your computer is your responsibility and should be locked when it is not in use.
• Users will adhere to password guidelines as outlined in Access Control Policy.

2.7 Devices – Laptops, Smartphones and Tablets

• To prevent any unauthorized access to personal computers, users will always lock the Desktop/Laptop when not in use, and set require password protection on resume.
• Users will not leave smartphones/tablets unattended in unsecure areas.
• Users will not use NBCC provided laptops or mobile devices in any way that may be considered insecure.
• Users will report the loss or theft of laptop or mobile devices immediately.
• NBCC laptops will be protected by NBCC authorized anti-malware solution and users will not tamper with any security settings or security software on NBCC devices.
• Any hardware changes or repairs to NBCC provided laptops or mobile devices shall be done only by NBCC IT.
• NBCC uses cloud storage for storing user data. In order to preserve cloud storage, users will avoid storing large videos on cloud synced folders.
• Use of personal mobile devices is allowed, however, in order to access NBCC services like email and OneDrive the personal devices should be registered with NBCC Mobile Device Management (MDM) solution. Refer to NBCC “Use of Mobile Devices SOP” on NBCC@Work.
• Only MAM managed apps should be used for accessing NBCC information. Refer to NBCC “Use of Mobile Devices SOP” on NBCC@Work.

2.8 Prohibited Activities

• Engaging in any illegal activity while utilizing NBCC information systems.
• Violating the rights of any person or NBCC 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 NBCC.
• Copying copyrighted material without authorization including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music or install any copyrighted software for which NBCC or the end user does not have an active licence.
• Introduction of malicious programs into the network or server (e.g. viruses, worms, Trojan horses, email bombs, etc.) or use NBCC's information systems to transmit malicious programs to other parties.
• Hacking into or obtaining access to any systems or accounts that is not permitted (including systems or accounts outside of NBCC) or attempt to do the same or otherwise breach or attempt to breach any computer or network security measures.
• Transmitting (or attempt to transmit) usernames, passwords or other information related to the security of NBCC's information systems to third parties.
• Using the Company information systems to download, transmit, distribute or process any material which may be considered to be offensive including, without limitation, material which is or may be considered to be racist or sexist, or otherwise discriminatory or to amount to harassment, victimization or bullying or otherwise to be potentially offensive, upsetting or derogatory to any group or individual which may be considered to be pornographic, obscene, or indecent (in all cases, even if you do not personally consider it to be so).
• Sending or forwarding threatening, harassing or abusive messages, or any messages that may be construed by the recipient as such, as a result of the language used, frequency of messages received or size of message, font or typeface used (e.g. some emojis may be perceived as offensive when used in an email or chat) or otherwise.
• Carrying out or assisting others in carrying out any type of security scan.
• Executing any form of unauthorized network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
• Providing information about, or lists of, NBCC employees or students to parties outside the college.
• Introducing “Dark Objects” or “Dark Shadows” into NBCC computer network. These items are files that could be hidden within the encryption algorithm of any e-mail.
• Using another User's login ID and password.
• Changing the configuration of your hardware or software without the prior approval from IT Department except for cosmetic changes such as colour, font, and resolution or display output device.
• Sending or forwarding:
  o Non-business-related messages to large numbers of newsgroups e.g. joke, sale items, etc.
o Any material, commentary, opinion, or view to any third party which may be defamatory, or which may lead to legal proceedings being issued against NBCC.

- Sending email or other electronic communication that attempts to hide the identity of the sender or represent the sender as someone else or maliciously amend messages received before forwarding that message on to another party.
- Revealing own account password to others or allow use of your account by others. This includes family and other household members when work is being done at home.
- Using or forging email header, footer, or disclaimer information for inappropriate or nonbusiness related activities.
- Using the Company information systems for your own personal financial gain or for the financial or business advancement of any third party.
- Posting any confidential or Internal information of any kind (including personal opinions etc.) regarding NBCC to any external bulletin board and social media on the Internet.
- Participating in or passing on to any other person any form of non-business chain emails. Any such mail will be deleted as soon as it is detected.
- Monitoring or intercepting files or electronic communications of other Users or read, delete, or copy the contents of another person’s email mailbox without their consent or appropriate authority.

3.0 Related Documents

Information Security Management Systems (ISMS) Policy (2808)