

1.0 Purpose

- 1.1 To fulfill the UNB's information and communication technologies (ICT) intended uses of enabling and supporting teaching, learning, research and administration by requiring that the technologies be used **legally, ethically, securely, responsibly and respectfully.**

2.0 Applicability

- 2.1 All distant and on-campus users of ICT including, faculty, staff, students, retirees, alumni, visitors and guests.
- 2.2 All UNB information and communication technologies that are financed by UNB funds or by funds administered by UNB including hardware, software, electronic data, UNB identities, UNB intranet components

3.0 Definitions

Due to the evolving nature of ICT, these ICT categories are defined by representative examples. The list of examples is not intended to be comprehensive.

- 3.1 Hardware - computers, copiers, mobile devices and data projectors
- 3.2 Software - licensed, purchased or developed in-house
- 3.3 Electronic data - website content or institutional information
- 3.4 UNB identities - login IDs, email addresses and internet domain names
- 3.5 UNB intranet components - cables, hubs, and the information flowing through them

4.0 Implementation

The following information is intended to provide models of acceptable use of ICT and is not intended to be a comprehensive list. The Information Technology Services Department is committed to helping all users meet these obligations, whether through direct support or through training and awareness initiatives. *Except where demonstrably required for teaching purposes, accessing, displaying, storing, or reproducing pornographic material is strictly prohibited.*

Acceptable Use of Information and Communication Technologies

Information Technology Services

Policy

- 4.1 To use ICT **legally and ethically** users must:
- 4.1.1 Limit any download, copy or distribution of materials such as publications, software, music or movies to the terms of the applicable license agreement or the Canadian Copyright Act.
 - 4.1.2 Maintain confidentiality and privacy of the information to which they have access and view, collect or use only authorized information.
- 4.2 To use ICT **securely** users must:
- 4.2.1 Protect identities and information in accounts by selecting secure passwords, preventing others from viewing or obtaining passwords, logging out when accounts are not in use and ensuring important information is backed up.
 - 4.2.2 Secure ICT infrastructure and data by ensuring the latest software security patches are installed, and protecting equipment from viruses, pop-ups and other malicious software.
 - 4.2.3 Safeguard information confidentiality by using secure access methods such as UNB's virtual private network (VPN). When communicating confidential information electronically choose appropriate communications methods depending on information value, use and sensitivity. Many electronic methods, such as email, are inherently insecure.
- 4.3 To use ICT **responsibly** users must:
- 4.3.1 Be accountable for all activity in personal or sponsored accounts, using the accounts and information available through the accounts only for the purposes for which they were intended. Personal activities such as, but not limited to, on-line gambling, or viewing pornographic material is strictly prohibited and must not take place on UNB owned technology. This policy recognizes that certain activities which might otherwise be prohibited may be authorized for research or other legitimate purposes. However, it is the responsibility of the individual user to obtain pre-authorization prior to and during such periods of required use, limited to such authorized purposes.
 - 4.3.2 Exercise good ICT stewardship and care by not endangering ICT infrastructure and by using resources efficiently and effectively. For example, to avoid spills that could damage equipment, drink from covered

containers and avoid eating around computers; to prevent accidentally compromising or disabling a computer, install only authorized software; to avoid consuming unnecessary storage, delete outdated files; to save paper, print only when necessary and consider using duplex printing; and to minimize costs and obtain best value from staff and vendor support, follow approved ICT standards.

4.3.3 Contribute to ICT reliability by attaching only approved hardware such as standard computers, printers, flash drives and similar devices to the network. Unplugging cables, plugging in unauthorized devices or similar activity may leave equipment and infrastructure in an unusable state. Most routers, hubs, and wireless printers are not approved.

4.3.4 Prevent others from misinterpreting actions or intentions by not possessing software or tools that could be used for unacceptable uses such as gaining unauthorized access to accounts or equipment.

4.4 To use ICT **respectfully** users must:

4.4.1 Be professional and courteous in UNB electronic communication such as voicemail, email, texting, and tweeting.

4.4.2 Be sensitive to what people can see and hear in public spaces and computer labs. Information such as confidential, approved personal, or acceptable, but potentially offensive material should be viewable only by the user. In public work spaces noise, whether from talking, computer sound or through headphones should be quiet and behaviour should be conducive to a work environment.

4.4.3 Share resources that aren't user specific. For example use network bandwidth and lab computers only for course work, academic work, UNB research or administrative uses. If in a lab, use only one lab machine at a time; if others are waiting give them an opportunity to use a computer as soon as course work is completed.

UNB may monitor its information and communication technologies at any time in order to determine compliance with its policies, for purposes of legal proceedings, to investigate misconduct, to locate information, or for any other business purpose.

5.0 Interpretation and Questions

5.1 Consequences and Appeal

5.1.1 If a violation has occurred or is suspected, ITS may remove user ICT access with or without notification. If possible, practical, and legal, ITS will contact the affected user to resolve the issue and eliminate the need to remove access. Depending on the circumstances, violators may be subject to UNB disciplinary action, or legal action.

5.1.2 Students or users from academic departments who wish to appeal ICT access restrictions should appeal initially to their Faculty Dean; users from administrative departments should appeal to the senior administrator for their unit. The Dean or senior administrator will consult with the AVP-ITS as part of the appeal process. Final arbitration is the responsibility of the Vice President Fredericton (Academic) or Vice President Saint John.

5.2 **Questions** about this policy should be directed to the Assistant Director of IT Security at the Information Technology Services (ITS) Department.