TECHNOLOGY RESOURCES POLICY

Quick Links Page Navigation:

Overview

NTCC sets forth some important guidelines and restrictions regarding any and all use of the Campuses' Technology Resources. This policy is not exhaustive of all user and institutional responsibilities but is intended to outline certain specific responsibilities that each user and institution acknowledges, accepts, and agrees to follow when using the Technology Resources provided by and/or through the NTCC campuses, as well as those Technology Resources existing throughout the world to which the NTCC provides and/or enables access -Internet access and other computer usage. The NTCC campuses provide Technology Resources for authorized users to support the academic, educational and administrative purposes of the campus. No use of the Technology Resources should conflict with the primary academic, educational and administrative purposes of the NTCC or with applicable laws and regulations. As a condition for access to the Technology Resources, each user is personally responsible for ensuring that each and all of these guidelines are followed.

Technology Resources are defined as including all NTCC owned and/or licensed information technology, technology and related resources, which include computers, printers and related hardware, licensed software, communications, internet access and all other related resources.

Permissible Use of Technology Resources

- Use Technology Resources only for authorized purposes in accordance with the Campus' policies and procedures, with federal, state and local laws, and with related laws and authorities governing the use of Technology Resources, software, email and/or similar technology.
- Maintain passwords in confidence and inform the instructor if a breach occurs since log-on IDs and passwords act as electronic signatures.
- Maintain confidential information particularly that prescribed by law, in accordance with appropriate security measures.
- Comply with use policies for Technology Resources throughout the world to which NTCC provides access.
- Be considerate in the use of shared Technology Resources, coordinating with Technology Services for "heavy use" operations that may unduly slow operations for other Users.
- Accept full responsibility for any publication resulting from Technology Resources and/or publishing Web pages and similar resources, including ensuring that all copyrights have been authorized for use.

Impermissible Use of Technology Resources

- Obtain or use another's log-on ID or password or otherwise access Technology Resources to which authorization has not been validly given.
- Copy, install or use any software, data files or other technology that violates a copyright or license agreement.
- Transmit or participate in chain letters, hoaxes, scams, misguided warnings, pyramid schemes or any other fraudulent or unlawful schemes.
- Utilize Technology Resources, including the Internet and/or email, to access, create, transmit, print or download material that is defamatory, obscene, fraudulent, harassing (including uninvited amorous or sexual messages), threatening, violent, or offensive, such as slurs, epithets, or anything that may be construed as harassment or disparagement based on race, color, national origin, sex, sexual orientation, age, disability, or religious or political beliefs or to access, send, receive, or solicit sexually-oriented messages or images or any other communication prohibited by law or other directive.
- Intentionally copy, download, install or distribute a computer virus, worm, "Trojan Horse" program, or other destructive programs, or otherwise harm systems or engage in any activity that would disrupt services, damage files, or make unauthorized modifications.
- Monopolize or disproportionately use shared Technology Resources, overload systems or networks with endless loops, interfere with others' authorized use, degrade services or otherwise waste computer time, connection time, disk space, printer paper or similar resources.
- Modify or reconfigure any component of Technology Resources without proper LCTCS authorization.
- Accept payments, discounts, free merchandise or services in exchange for any services provided through use of the Technology Resources, unless properly authorized by the NTCC; or otherwise conduct a for-profit, commercial business without properly coordinating with NTCC officials.
- Endanger the security of any Technology Resources or attempt to circumvent any established security measures, such as using a computer program to attempt password decoding.
- Send unsolicited mass mailings or "spamming." Mass mailings to clearly identified groups for official purposes (for example, disseminating administrative announcements, notifying students of educational opportunities) may not be sent without proper authorization.
- Transmit personal comments or statements or post information to newsgroups or Usenet that may be mistaken as the position of the NTCC.
- Utilize Technology Resources to develop, perform and/or perpetuate any unlawful act or to improperly disclose confidential information.
- Install, store or download software from the Internet or Email to NTCC Technology Resources unless such conduct is consistent with the Campus' academic, educational and administrative policies or otherwise properly approved by the Chancellor.
- Copy, impair or remove any software located on any Technology Resources or install any software on any Technology Resources that impairs the function, operation and/or efficiency of any Technology Resources.
- Connect or install any unauthorized hardware or equipment including but not limited to laptops, external drives, etc. to any Technology

Resources or network access points without prior written approval from the Chancellor.

Monitoring and Penalties

Use of the NTCC Technology Resources is a privilege, not a right. NTCC reviews and monitors its Technology Resources for compliance with policies, applicable laws and related directives and discloses transactions to investigating authorities and others as warranted. Users should not have any expectation of privacy when using and storing information on the NTCC's Technology Resources and the NTCC specifically reserves the right to review and copy any data or other information stored on any Technology Resources, without notice to any user, by use of forensic computers or otherwise. Violations of this policy may result in penalties, such as terminating access to Technology Resources, NTCC disciplinary action, civil liability and/or criminal sanctions. All Users are specifically prohibited from encrypting files on any Technology Resources or taking any steps that block the NTCC's access to files, other than the use of NTCC passwords or approved encryption programs, unless such conduct is consistent with the NTCC's academic, educational and administrative policies or otherwise properly approved by the LCTCS.

NTCC may monitor all usage of the Internet on or through Technology Resources and all other use of the NTCC's Technology Resources, including, without limitation, reviewing a list of any and all sites accessed by any user and all emails transmitted and/or received on any Technology Resources.

Proprietary Rights and Licenses

Except as may be specifically agreed otherwise by the NTCC, any and all software and materials contained on any NTCC Technology Resources is solely owned by the NTCC, except to the extent that any such materials are licensed to the NTCC by a third-party vendor. Users are forbidden from taking any action that would be in violation of any standard license agreement for any software licensed to the NTCC and contained on any LCTCS Technology Resources, including without limitation, making any unauthorized copies of any such software.

Management has developed and accepted a Security Policy for the Northshore NTCC Information Systems. Anyone requesting access to the NTCC's Information Systems must read and acknowledge this statement.

- If student is unsure whether an action details a security violation, you should report it and discuss with student's instructor and/or administration
- Each User is responsible for the security of NTCC's Information Systems.
- Each User accessing NTCC's Information Systems is bound by the procedures, such as password and account log-on procedures, detailed in the Security Policy.
- Each User should lock his/her workstation by a form of screensaver password, or logout, when away from the workstation.
- Each User should be aware of social engineering, the manipulation to gain information for the purpose of perpetrating fraud or damage to the system.
- Each User should be aware that NTCC personnel may monitor any and all activities without the user's direct consent or knowledge.