

TYPE: INFORMATIONAL & INSTRUCTIONAL TECHNOLOGY

POLICY TITLE: Technology Use Policy

The technology resources at Northeast Wisconsin Technical College support the instructional, research and administrative activities of the College. Examples of these computing sources include, but are not limited to, the central computing services, the campus wide network, local-area networks, electronic mail, Web access, and access to: the Internet, voice mail, ITV, Cable Channels, departmental networks, the public computing lab/classrooms and other related services.

Users of these services and facilities have access to valuable College resources, to sensitive data and to external networks. Consequently, it is important for all users to behave in a responsible, ethical and legal manner. In general, appropriate use means respecting the rights of other computer users, the integrity of the physical facilities and all pertinent license and contractual agreements.

College proprietary material should not be placed on social network or similar sites. The privacy interests of College faculty, staff and students should be respected when accessing College technology resources or conveying material via such resources. Use of camera phones or any photographs is prohibited when others would have a reasonable expectation of privacy.

This document establishes more specific guidelines for the use of all College computing resources. These guidelines apply to all users of computing resources owned or managed by Northeast Wisconsin Technical College, including but not limited to College faculty and visiting faculty, staff, students, guests of the administration, external individuals or organizations and individuals accessing external network services, such as the Internet, via the College's computing facilities.

The policies described in this document apply to all computing systems owned or managed by Northeast Wisconsin Technical College or using the College network. By using the technology resources at Northeast Wisconsin Technical College, it is assumed that the user agrees to abide by the policies that govern the use of the resources.

Appropriate Computing Behavior

The following list, while not exhaustive, provides specifics for responsible and ethical behavior to which the College expect you to comply:

1. Use only the computers, computer accounts and computer files for which you have authorization.
2. Do not use another individual's electronic ID or account, or attempt to capture or guess other user's passwords.
3. Users are individually responsible for all use of resources assigned to them; therefore, sharing of accounts is prohibited.

4. Obey established guidelines for any computers or networks used both inside and outside the College. For example, individuals using College public computing labs/classrooms must adhere to the policies established for those lab/classrooms; individuals accessing off-campus computers via external networks must abide by the policies established by the owners of those computers as well as policies governing use of those networks.
5. Do not attempt to access restricted portions of the network, an operating system, security software, or accounting software unless authorized by the appropriate College administrator or owner.
6. Users are prohibited from copying or removing software from the College computer system.
7. Users may not use the College information system to gain unauthorized access to any system or data. Breaking into computers is explicitly a violation of College policy, no matter how weak the protection is on those computers.
8. Tapping into telephone or network lines is a clear violation of College policy.
9. Abide by all state and federal laws. Respect the privacy and personal rights of others.
10. Do not access or copy another user's electronic mail, data, programs, or other files without permission.
11. Use of College Information Systems that violates any College policy is prohibited.
12. Copying material bearing copyrights or patents without proper licensing or authority is prohibited. Both College policies and the law expressly forbid the copying of software that has not been placed in the public domain or distributed as "freeware." "Shareware" users are expected to abide by the requirements of the shareware agreement. Respect the Copyright Law as it applies to images, texts and sounds in the production of electronic information. The ease with which electronic materials can be copied, modified and sent over the Internet makes electronic materials extremely vulnerable to unauthorized access, invasion of privacy and copyright infringement. The unauthorized use or distribution of copyrighted works (including Web page graphics, sound files, trademarks and logos) is prohibited and may provide the basis for disciplinary action, civil litigation and criminal prosecution. Further explanation of NWTC's copyright information can be found at <http://nwtc.libguides.com/copyright>
13. Using College computing resources to harass other individuals deliberately is explicitly prohibited. Following are examples of harassment:
 - a. Using the computer to annoy, harass, terrify, intimidate, threaten, offend or bother another person by conveying obscene language, pictures, or other materials, or threats of bodily harm to the recipient or recipient's family;
 - b. Using the computer to contact another person repeatedly with the intent to annoy, harass, or bother, whether or not any actual message is communicated, and/or where no purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease;
 - c. Using the computer to contact another person repeatedly regarding a matter for which one does not have the legal right to communicate, once the recipient has provided reasonable notice that he or she desires such communication to cease;
 - d. Using the computer to disrupt or damage the academic research, administrative, or other pursuits of another;
 - e. Using the computer to invade the privacy, academic or otherwise, of another or to threaten invasion of privacy of another.

14. Be sensitive to the needs of others, and use only your fair share of computing resources. For example, users of shared resources, such as the central computer or the public lab/classrooms, should use these facilities for only the most essential tasks during periods of peak demand.
15. Broadcasting non-sanctioned messages to large numbers of individuals and sending chain letters are examples of activities that cause network congestion and interfere with the work of others, and thus are not allowed.
16. Treat computing resources and electronic information as a valuable College resource.
17. Protect data and the systems use. For example, back up files regularly. Set a password that is not easily guessed and change it regularly. Make sure to understand the access privileges set for files and the computer system.
18. Do not destroy or damage any computing equipment, networks or software. The willful introduction of computer viruses, worms, Trojan horses, or any other infection into the NWTC computing environment or into other computing environments via the College's network violates College standards and regulations.
19. Using the College information system for political lobbying is prohibited.
20. Activities that would jeopardize the College's tax exempt status are prohibited.
PERSONAL FINANCIAL GAIN: Use of College computing resources for personal financial gain is prohibited.
21. Stay informed about the computing environment. The computing environment is continually evolving, as new products are introduced and others become obsolete.

Services change as the number and needs of users change. The College publishes information in a variety of ways, including Web pages, electronic messaging, general news items that users are prompted to read, news groups associated with particular compilers or software packages, on-line documents about software, guidelines, directives, terms of use, policy and procedures, and in some cases, e-mail to individuals.

Users are responsible for staying informed about changes in the computing environment and are expected to adapt to changes in the College computing environment.

Viewing or Distributing Obscene or Pornographic Materials

Users may not access, download, store, or transmit obscene or pornographic materials through the College's Information System or using any College resources.

Recreational Use

- The PC equipment in the Digital Lounge on the Green Bay campus and in the student lounge areas on the Marinette and Sturgeon Bay campuses is set up for recreational use. Within the bounds of appropriate and decent use, these machines are available for recreational use by current students.
- Outside of the digital lounge, recreational use of the College Information System, including playing computer games for recreation, is discouraged. Recreational use that interferes with learning or the business of the College is prohibited.

- Other than that which is in the student lounges, NWTC will not install equipment or software that is intended for recreational use and such equipment or software will be removed from systems and disposed of at the convenience of the College.

Data Integrity & Security

IIT provides reasonable security against intrusion and damage to files stored on the central computing services. The College will not be responsible for any damages suffered while using the College Information Systems, including loss of personal data due to system outages, operational errors, unauthorized access by other users, media failure, fire, floods, etc.

Users will use all available methods to protect their files, including the frequent changing of their passwords, encryption of data, and storing back-up copies of information off site. In the event that data have been corrupted as a result of intrusion, IIT should be notified immediately.

Upon request, IIT staff will assist in implementing procedures to maximize security. It is recommended that users will change their passwords every semester. All servers connected to the NWTC network will be managed by IIT and stored in IIT environments.

Privacy

Users should be aware that their use of College computing resources is not private and the College does routinely monitor the usage of its computing resources. The College maintains tools to assess the use of these resources for compliance of this policy. As directed, IIT may also specifically monitor the activity and accounts of individual users of the College's computing resources.

IIT maintains several controls over its ability to monitor usage and access the systems across the College. IIT will only initiate a report on the individual actions of its users when requested by the appropriate authority; requests for tracking staff must have the permission from the VP of Human Resources; requests for tracking students must have the permission from the VP of Student Services.

Members of IIT staff are forbidden to log on to a user account or to access a user's files unless the user or supervisor gives explicit permission (for example, by setting file access privileges). IIT staff is also forbidden to edit any data unless it is a mass data operation that requires the technical expertise of the IIT staff and the process is initiated and monitored by the administrator in charge of the data.

The CIO may upon his or her authority investigate or access computer usage if a service is suspected of causing disruption to the technology infrastructure or is in violation of College policy, state or federal law.

Information obtained is admissible in legal proceedings or in a College hearing. In accepting a user account, the user agrees to these terms of technology use.

Violations

Violations of these terms of technology use may result in revocation of technology privileges and/or in disciplinary action up to and including dismissal, as well as civil liability and/or criminal prosecution.

Inappropriate use, whether intentional or not, may result in civil and/or criminal liability, and/or a violation of the Electronic Communications Privacy Act of 1986, the Family Educational Rights and Privacy Act, the Health Insurance Privacy and Protection Act, Wisconsin wiretap and/or privacy laws, defamation, copyright and/or trademark infringement laws, sexual harassment and discrimination laws, and/or other applicable federal or state laws and regulations.

Laptop Checkout

NWTC allows for laptops to be checked out according to the Library Laptop Checkout Policy which can be found at: http://nwtc.libguides.com/faculty_services for faculty.

Disclaimer

1. All systems, hardware, software, and data are the property of NWTC and subject to audit by the College and other legal authorities.
2. NWTC may, at its own discretion, examine, move, or delete files, including electronic mail, for purposes of system maintenance or if the files are determined to be intentionally or unintentionally disruptive to the system or system users.
3. The College makes no warranties of any kind whether expressed or implied, for the reliability or integrity of the Information Services it is providing. Information Systems are provided on the best effort basis.
4. The College will not be responsible for any damages suffered while using the College Information Systems, including loss of personal data due to system outages or operational errors.
5. NWTC is not responsible for offensive or objectionable materials that any user has obtained with the College Information System.

Exemptions

Exemptions to sections of this policy will be granted when the specific section(s) directly conflicts with the completion of approved College curriculum. Exemption requests must be documented by the instructor, approved by the instructional supervisor and Chief Information Officer.

Documented exemption requests will be kept on file in IIT and reviewed with the requesting department on an annual basis.

Approved 09/29/08

Revised 5/7/07

Revised 2/5/07

Revised 4/19/04
Approved 12/20/00