

## Computer Use Policy

Arkansas Northeastern College owns and operates a substantial number of computers which are provided for the use of ANC students, faculty, and staff in support of the programs of the College and are to be used for education, research, academic development, and public service only. All users are responsible for using the computing facilities and machines in an effective, efficient, ethical and lawful manner. Unacceptable use is prohibited, and is grounds for discipline or legal sanctions under federal, state, local laws and college regulations.

All users must read, understand, and comply with the guidelines established by the College. By using any of these systems, users agree that they have read, understand, and will comply with these guidelines. Arkansas Northeastern College reserves all rights, including termination of service, to the computing resources to which it provided access. Users of ANC computing systems are responsible for maintaining the following:

1. An environment in which access to all ANC computing resources are shared equitably among users.
2. An environment conducive to teaching, learning, and conducting business. A user who uses the College's computing systems to harass, or make defamatory remarks, shall bear full responsibility for his or her actions. Further, by using these systems, users agree that Arkansas Northeastern College's role in managing these systems is only as an information carrier, and that they will never consider transmission through these systems as an endorsement of said transmission by Arkansas Northeastern College. When accessing the Internet, users are advised that they may encounter material which may be considered offensive or objectionable in nature or content. Users are further advised that Arkansas Northeastern College does not assume responsibility for the contents of any of these outside networks. The user agrees to comply with the acceptable use guidelines for whichever outside networks or service they may access through ANC systems. Further, the user agrees to follow proper etiquette on outside networks. The user agrees never to attempt to transmit, or cause to be transmitted, any message in which the origination is deliberately misleading. The user agrees that, in the unlikely event that someone does transmit, or causes to be transmitted, any message that is inconsistent with an environment conducive to learning or with a misleading origination, the person who performed the transmission will be solely accountable for the message, not Arkansas Northeastern College, which is acting solely as the information carrier.
3. An environment free of illegal or malicious acts. The user agrees never to use the system to perform an illegal or malicious act. Any attempt to increase the level of access to which he or she is authorized, or any attempt to deprive other authorized users of resources or access to any Arkansas Northeastern College computer system shall be regarded as malicious and may be treated as an illegal act.
4. A secure environment. Any user who finds a possible security lapse on the system is obliged to report it to the appropriate faculty or staff. Knowledge of passwords or of loopholes in computer security systems shall not be used to damage computing resources, obtain extra resources, take resources from another user, gain unauthorized access to resources or otherwise make use of computing resources for which proper authorization has not been given.
5. Users must be sensitive to the public nature of shared facilities. Behavior reflects both upon the individual and the College. Computing and networking resources should be used only in accordance with this policy. Any intentional behavior with respect to the electronic environment that interferes with the missions or activities of the College community will be regarded as unethical, and may lead to disciplinary action under standard College rules for misconduct. Examples of inappropriate and unacceptable use of the computer system include, but are not limited to, the following:

\*Creating

\*Displaying

\*Downloading

\*Printing

\*Transmitting

This includes, but is not limited to, displaying sexually explicit, graphically disturbing, or sexual harassing images or text, and any information which violates the College's sexual harassment policy.

6. Installation and/or use of any software that maintains a permanent Internet connection. This includes Weatherbug, Weathercast, streaming audio, radio stations, music netcast channels, time synchronization programs, stock tickers, news tickers, etc.
7. Installation and/or use of any peer-to-peer file sharing application that infringes on copyrighted material including; Kazaa, Bearshare, Swapper, Napster, Limewire, Audiogalaxy, Xolox, or any Point-to-Point based sharing software.

8. Chat room and messengers. The resources are not available for users to socialize. This includes, but is not limited to, any World Wide Web site designed as a chat room or any IRC site, unless the use of the chat room has been approved by the MITS department as a legitimate business or academic use.
9. Knowingly or carelessly running or installing on any computer system or network, or giving to another user, a program intended to damage or to place excessive load on a computer system or network or to deprive authorized person of computer access.
10. Using a user-id or account belonging to another individual, or allowing your account to be used by another individual.
11. Attempting to access data being transferred through the network or files on any computer connected to the network without the owner's permission. Deliberately wasting/overloading computer resources. This includes, but is not limited to, printing out multiple copies of a document or printing out large documents that may be available on-line and that might impact significantly on other user's printing resources.
12. Use of E-mail or messaging services to harass, intimidate, or otherwise annoy another person, for example, by broadcasting unsolicited messages or sending mail that is known to be unwanted. (SPAM) This also applies to material originating from this campus but sent to other sites or persons on the Internet.
13. Violation of software copyrights and usage licensing agreements.
14. Violation of usage policies and regulations of the networks of which the College is a member or has authority to use.
15. Illegally providing, receiving, or distributing any copyrighted material or intellectual property without express consent of the owner of the copyright. This includes, but is not limited to, music, videos, documents, or articles.
16. Use of computing facilities for financial gain or commercial purposes.

An individual's computer use privileges may be suspended immediately upon the discovery of a possible violation of these policies. Such suspected violations will be reported to the Vice President for Student Affairs.

Violations of these policies will be dealt with in the same manner as violations of other College policies and may result in disciplinary review. In such a review, the full range of disciplinary sanctions is available including the loss of computer use privileges. Violations of some of the above policies may constitute a criminal offense and subject the student to civil or criminal liability.