Acceptable Technology Use Policy
For
North Arkansas College

IT Services Division

Table of Contents

North Arkansas College's Technology Use Policy

Introduction

North Arkansas College is committed to provide technology that is well-maintained, relatively current, and well connected. As with any service, there are guidelines as to how the technology is to be used. This document provides those guidelines on the administration of the college's technology resources, appropriate use, and outlines sanctions for those who violate any of the policies or guidelines outlined.

Mission:

The mission of North Arkansas College is to provide high quality, affordable, convenient opportunities for learning and cultural enrichment in response to community needs. The use of technology at the college is one tool that the college can use to fulfill its mission to the community.

Privacy and academic freedoms:

The administration of North Arkansas College will make every effort to insure the privacy of its students, staff, faculty, and other constituents. The college's computing technology is primarily for the academic endeavors and general education of its users and the support for those functions. The college will strive to create an atmosphere of intellectual freedom for research and communication within the guidelines set forth in this document.

Laws referenced:

All federal and state laws, as well as college regulations and policies, are applicable to the use of technology resources. These include, but are not limited to, the Family Education Rights and Privacy Act, 20 U.S.C. § 1232g 34 CFR Part 99; the Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510 et seq.; the Arkansas Freedom of Information Act, Ark. Code Ann. §§ 25-19-101 et seq.; the Arkansas Criminal Statutes on Pornography of 1993, § 5-68-201 through 5-68-303; the Arkansas Internet Use Policies, AR Code Ann § 25-4-110 (c); and state and federal computer fraud statutes, 18 U.S.C. § 1030 and Ark. Code. Ann. §§ 5-41-101 et seq. Illegal reproduction or download of software and other intellectual property protected by U.S. copyright laws and by licensing agreements may result in civil and criminal sanctions.

Administration

North Arkansas College, in accordance with state and federal law and according to the policies set forth by the administration of the college may control access to its information and the devices on which this information is stored, manipulated, and transmitted.

The college also has the responsibility to develop or acquire, maintain, and enforce the appropriate security procedures to ensure the integrity and privacy of individual and institutional information, however stored; uphold all copyrights, patents, licensing agreements and other rules of organizations that supply the college with informational resources.

The responsibility for administering the college's technology resources rests with the IT Services Division along with other administrative units of the college.

Responsibilities of IT staff

A) System Administrator
   1. A system administrator is defined as any person designated, on any campus, to maintain, manage, and provide security for shared, multi-user computing resources, which include all computing devices, networks, servers, and peripherals
   2. System administrators shall perform their duties fairly and ethically, in cooperation with the user community and the college's administration. They shall also adhere to this code and all other college policies and regulations along with all state and federal laws, policies and standards.
   3. System administrators shall also respect the privacy of users to the greatest extent possible and shall refer all disciplinary matters to the appropriate college officials

B) IT Staff
   1. IT, or Information Technology, Staff is defined as any person who is delegated responsibility to create and maintain user accounts; maintain computing, network, or associated equipment; and provide technical assistance to the users of the shared, multi-user computing resources.
   2. The IT staff shall perform their duties fairly and ethically, in cooperation with the user community and the college's administration. They shall also adhere to this code and all other college policies and regulations along with all state and federal laws, policies and standards.
   3. IT staff shall also respect the privacy of users to the greatest extent possible and shall refer all disciplinary matters to the appropriate college officials.

C) System Maintenance

1. Access is necessary for maintenance of computers, networks, data, and storage systems; to maintain the integrity of the computer, network, or storage system; or to protect the rights or property of the college or other users. Authorized personnel may routinely monitor and log usage data, such as network session connection times and end-points, CPU and disk utilization for each user, security audit trails, and network loading. In all cases, the privacy rights of users shall be protected to the greatest extent possible.
2. Every reasonable effort will be made to ensure a secure and stable computing environment. This includes, but is not limited to, the installation of antivirus software, antispyware, and appropriate authentication standards on every computing device per Arkansas State standards SS-70-004, SS-70-005, and SS-70-002 respectively.

D) User Accounts

1. Staff and Faculty:
   Staff and Faculty user accounts are generated after successfully completing the hiring process through Human Resources. Creation of this account forms an agreement that the user will abide by Northark policies and procedures and the Arkansas State Act 1287 of 2001, AR Code Ann § 25-4-110 (c).
2. Students:
   User accounts are automatically generated for students when they successfully enroll. The creation of this account forms an agreement that the user will abide by Northark policies and procedures and the Arkansas State Act 1287 of 2001, AR Code Ann § 25-4-110 (c).
3. General public and guests:
   Guest computer accounts are available for checkout at the college's libraries for use within the library labs. Individual computer and email accounts are not generated for guests of the college except for the following exceptions:
   i. Students who are taking classes at partner institutions that will be using North Arkansas College facilities for their research or study.
   ii. Visiting professors and instructors from other institutions who plan to use the college's facilities for an extended period of time while teaching or pursuing related academic goals.

D) Data Storage

1. North Arkansas College will provide adequate space for storing electronic data. This includes but is not limited to hard drive space on local machines (please note that in the computer labs, this is for temporary storage only– all local drives are restored at each reboot), hard drive space on shared server resources, and removable media options.
2. The college also utilizes several techniques to retain data integrity. These techniques include, but are not limited to, utilizing RAID array disk mirroring and striping, network replication, and regular scheduled backups.

3. The college, nor the IT staff cannot be held responsible for data loss in the event of a hardware or removable media malfunction.

Ownership of Data and Equipment

A) User Accounts
    1. Individual users of the college's computing system do not own their accounts, but are given the privilege of exclusive use. The use of college computing resources for the storage or transmission of data does not alter any ownership interest of the user pertaining to the data.

B) Computing Equipment
    1. All technology equipment including but not limited to computer workstations, network devices, cabling, peripherals, and furniture are the property of North Arkansas College and the State of Arkansas. Use of these resources are granted to further the academic mission of the college and the support thereof.

C) Email and Data
    1. College officials may access user email or electronic data under one or more of the following conditions:
        a. The user consents either verbally or in writing to such access
        b. There is a valid search warrant or court order, or a request for electronic records that are open to public inspection under the Arkansas Freedom of Information Act.
        c. There exists an emergency situation in which the physical safety and/or well-being of person(s) may be affected or college property may be damaged or destroyed. Responsibility for authorizing access to this data or service rests with the President, Director of IT Services, or an appropriate Vice President. This responsibility may also include an authorized designee appointed by any of the three positions.
        d. There exist reasonable grounds to believe that a violation of law or Northark policy is occurring or has occurred. Responsibility for authorizing access rests with the President, Director of IT Services, or the appropriate Vice President. This responsibility may also include an authorized designee appointed by any of the three positions.
        e. Necessary access for maintenance of computers, networks, data, and storage systems; to maintain the integrity of the computer, network, or storage system; or to protect the rights or property of the college or other users. Authorized personnel may routinely monitor and log usage data, such as network sessions, end-points, CPU and disk utilization for each user, security audit trails, and network bandwidth usage. In all cases, the privacy rights of users shall be protected to the greatest extent possible.

D) Maintenance Window

1. Access to computing systems and network services may be interrupted during times of maintenance. It is the goal of the IT staff to provide a system with a high level of uptime, but upgrades, updates and other preventative maintenance must be performed to preserve data and system integrity. This maintenance window will occur during off-peak times except in the event of an emergency.
2. If an unscheduled maintenance must occur, the IT staff will make every attempt to notify the college's users at least 30 minutes before disabling a service or access.

E) The Arkansas Freedom of Information Act

1. The electronic files, including e-mail files, of college employees are potentially subject to public inspection and copying under the state Freedom of Information Act ("FOIA"), Ark. Code Ann. §§ 25-19-101 et seq.
2. The FOIA defines "public records" to include "data compilations in any form, required by law to be kept or otherwise kept, which constitute a record of the performance or lack of performance of official functions which are or should be carried out by a public official or employee [or] a governmental agency. . . ." Ark. Code Ann. § 25-19-103(1). All records maintained in public offices or by public employees within the scope of their employment are presumed to be public records and should be saved by the originating author or principal parties. Id. Various exceptions apply. See Ark. Code Ann.§ 25-19-105.

F) Education Records

1. Records containing information directly related to a student are confidential and protected from public disclosure by the Family Educational Rights & Privacy Act, 20 U.S.C. § 1232g, and the Arkansas Freedom of Information Act, Ark. Code. Ann. § 25-19-105(b)(2).
2. No one shall access any such records maintained in an electronic format or disclose or distribute their contents in any manner inconsistent with federal and state law and college regulations.

Use of Computing Resources

This section does not cover every situation involving the proper or improper use of college technology resources; however, it does set forth some of the responsibilities that a person accepts if he or she chooses to use those resources. The purpose of this section is to establish rules for the benefit of all users and encourage responsible use of technology resources.

The technology resources at North Arkansas College are primarily to be used to support and further the academic pursuits of its students and provide support to conduct the daily operations of the college. Any use of the technology resources for personal gain or to conduct a private or personal business is strictly prohibited, except for scholarly pursuits such as faculty publishing activities or students applying for financial aid. The following section will outline other potential misuses that are prohibited.

A) Authorized Use

1. No one shall (a) connect with or otherwise use any college computer, network, or other technology resource without proper authorization; (b) assist in, encourage, or conceal any unauthorized use, or attempted unauthorized use, of any college computer, network, or other technology resource; or (c) misrepresent his or her identity or relationship to the college to obtain access to technology resources.
2. Users shall use only those computing and network resources that have been authorized for their use and must identify computing work with their own names or an approved means of identification so that responsibility for the work can be determined and users contacted, if necessary.
3. Users shall not install any software on any college computer without authorization from IT Services or authority from other controlling entities. This includes but is not limited to shareware and/or freeware.

A) User Accounts

1. Users shall not subvert restrictions associated with their accounts, such as quotas and levels of access.
2. Users should follow the procedures for accessing college technology systems as outlined in Northark user account documents and any on-line help.
3. No one shall give any password for any college computer or network to any unauthorized person, nor obtain any other person's password by unauthorized means. Users are responsible for the use of their accounts and shall not allow others access to their accounts, through password sharing or otherwise. Users should take advantage of system-provided protection measures to prevent such access.
4. When a user ceases being a member of the campus community within the college (i.e. no longer is a student or employee), his or her account and access authorization shall be disabled or the role of the account will change to restrict access. A user shall not use facilities, accounts, access codes, privileges, or information for which he or she is not authorized.

B) Security and other related matters

1. No one shall (a) knowingly endanger or compromise the security of any college computer, network facility, or other technology resource

or willfully interfere with others' authorized computer usage, (b) attempt to circumvent data protection schemes, uncover security loopholes, or decrypt secure data; (c) modify, reconfigure or attempt to modify or reconfigure any software or hardware of any college computer or network facility in any way, unless specific authorization has been obtained; or (d) use college computer resources and communication facilities to attempt unauthorized access to or use of any computer or network facility, no matter where located, or to interfere with others' legitimate use of any such computing resource. This includes the use of network sniffing and discovery tools.

2. No one shall attempt to access, copy, or destroy programs or files that belong to other users or to the college without prior authorization, nor shall anyone use college technology resources for unauthorized monitoring of electronic communications.
3. No one shall create, run, install, or knowingly distribute a computer virus, Trojan Horse, Worm, or other surreptitiously destructive malware, e-mail, or data via any college computer or network facility, regardless of whether demonstrable harm results.
4. Users shall not store confidential information on computers without protecting it appropriately. The college cannot guarantee the privacy of computer files, e-mail, or other information stored or transmitted by computer; moreover, the college may access such information in accordance with Part II of this code. Persons who have access to confidential or sensitive information shall disclose it only to the extent authorized by the Family Educational Rights & Privacy Act, the Arkansas Freedom of Information Act, and other applicable laws, and only in connection with official college business.
5. Users shall not knowingly or recklessly perform any act that will interfere with the normal operation of computers, servers, peripherals, or networks and shall not intentionally waste or overload computing resources.

C) Intellectual Property

1. No one shall copy, install, use, download, view, or distribute through college technology resources any photographs, logos, images, graphics, graphic elements, audio, video, software, html markup, data files, or other information in violation of U.S. copyright, trademark, patent laws, federal or state laws, or applicable licensing agreements, or college policy. It is the user's responsibility to become familiar with the terms and requirements of any such laws or agreements. This subsection does not apply to any material that is in the public domain.

D) Communications

1. Users assume full responsibility for messages that they transmit through college computers and network facilities.

2. No one shall use the college's computing resources to transmit fraudulent, defamatory, or obscene messages, or any material prohibited by law.
3. No one shall use the college's computing and network resources to: (a) annoy, harass, threaten, intimidate, terrify, or offend another person by conveying offensive language or images or threats of bodily harm to the recipient or the recipient's immediate family; (b) repeatedly contact another person to annoy or harass, whether or not any actual message is communicated, and the recipient has expressed a desire for the contact to cease; (c) repeatedly contact another person regarding a matter for which one does not have a legal right to communicate (such as debt collection), once the recipient has provided reasonable notice that he or she desires such contact to cease; (d) disrupt or damage the academic, research, administrative, or related pursuits of another person; or (e) invade the privacy, academic or otherwise, of another person or threaten such an invasion.
4. Users shall comply with this code as well as the regulations and policies of all other public forums through which they disseminate messages.
5. Users shall not (a) initiate or propagate electronic chain letters; (b) engage in spamming or other indiscriminate mass mailings; (c) forge communications to make them appear to originate from another person, e.g., spoofing or phishing; or (d) engage in resource-intensive activities unrelated to college functions, e.g online gaming or extended use of online audio and/or video programs and chat sessions not related to academic pursuits.
6. Users shall conduct all communications in an ethical way and comply with the Internet and computing standards of etiquette.

E) Priorities for Computer Lab Usage
1. In college libraries and general-access computer labs, or in any other environment in which users must share computing resources, priority shall be given to users engaged in activities directly related to the college's mission, e.g., completing course assignments or engaging in research.
2. Areas that maintain computer labs (e.g. Library) may adopt policies to regulate the use of online or printing activity.
3. Printer use is governed through a print management system and all print activity is monitored and users are charged on a per-print basis.

F) Pornography
1. The viewing, printing, or distribution of pornographic or obscene images is prohibited to all users of the college computing system. Images, graphics, and language associated with the Arts and medical disciplines are excluded.

Enforcement and Sanctions

A) System administrators are responsible for protecting the system and users from abuses of this code. Pursuant to this duty, system administrators may (1) formally or informally discuss the matter with the offending party, (2) temporarily revoke or modify access privileges, or (3) refer the matter to the appropriate disciplinary authority.
B) Any violation of this code may result in the revocation or suspension of access privileges. Imposition of such a sanction is within the discretion of the IT Services Department or the appropriate academic or administrative unit.
C) Any offense that violates local, state, or federal laws may result in the immediate loss of all college computing and network privileges, may cause student or employee to be placed on disciplinary probation, suspended or expelled, and may be referred to the appropriate law enforcement agencies.

Summary

Technology is a necessary part of the educational environment. While you may be required to use a computer and associated technologies, it should be understood that usage of your computer account is a privilege. All users are expected to use common sense, ethical behavior, and proper etiquette when accessing software and other resources while at Northark, different web sites, and other activities related to technology. User accounts, passwords, files and data to which one's name is associated should be guarded carefully. All users are expected to follow the guidelines set forth in this and other college documents concerning technology usage and are expected to be aware of any and all consequences resulting from misuse of said technology resources. Malicious behavior, downloading and/or viewing of pornographic material is prohibited as well as the installation of malicious software. The use of computers and Internet are not to be used to harass, intimidate, or defame anyone. Sanctions for violating this policy may include revocation of privileges, suspension, expulsion, or arrest, depending on the action and level of violation.

Definitions:

Backup - **(v.)** To copy files to a second medium (a disk or tape) as a precaution in case the first medium fails.

Freeware - Copyrighted software given away for free by the author. Although it is available for free, the author retains the copyright, which means that you cannot do anything with it that is not expressly allowed by the author.

Hacking – A way to modify a program, often in an unauthorized manner, by changing the code itself.

Logs - A file that lists actions that have occurred

Peripheral - A computer device, such as a CD-ROM drive, printer, or other external device that is not part of the essential computer, i.e., the memory and microprocessor.

Phishing - (fish´ing) **(n.)** The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

RAID - (rād) Short for ***R****edundant* ***A****rray of* ***I****ndependent (or* ***I****nexpensive)* ***D****isks*, a category of disk drives that employ two or more drives in combination for fault tolerance and performance.

Server - (ser´ver) **(n.)** A computer or device on a network that manages network resources

Shareware – **(n.)** Software distributed on the basis of an honor system. Most shareware is delivered free of charge, but the author usually requests that you pay a small fee if you like the program and use it regularly

Spyware - Any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes.

Trojan Horse - A destructive program that masquerades as a benign application

Virus - A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes and can also replicate themselves.

Worm - A program or algorithm that replicates itself over a computer network and usually performs malicious actions, such as using up the computer's resources and possibly shutting the system down.

Definitions provided by Webopedia, http://www.webopedia.com/

References:

Flynn, N. (2000). *E-Policy Handbook : Designing and Implementing Effective E-Mail, Internet and Software Policies.* Retrieved August 12, 2006 from http://site.ebrary.com.library.capella.edu/lib/capella/

Jenkins, G., & Wallace, M. (2002). *IT policies & procedures: Tools & techniques that work*. Paramus, NJ: Prentice Hall.

North Arkansas College. (2006). Computer Use Policy. Retrieved August 12, 2006 from http://www.northark.edu/Departments/MCS/computer_use_policy.htm

Overly, M. (1999). *E-policy: How to develop computer, E-mail, and Internet guidelines to protect your company and its assets*. (e-book) New York: AMACOM

State of Arkansas. (2006). Standard Statement - Data and System Security. Retrieved August 12, 2006 from http://www.techarch.state.ar.us/domains/security/standards/SS-70-001_dataclass_standard.pdf

State of Arkansas. (2003). Policy Statement – Acceptable Use. Retrieved August 12, 2006 from http://www.techarch.state.ar.us/domains/information/policy/PS-50_Internet_Use.pdf

State of Arkansas. (2003). Model Internet Appropriate Use Policy. Retrieved August 12, 2006 from http://www.techarch.state.ar.us/domains/information/best_practices/Model_Use_Policy.pdf

State of Arkansas. (2003). Internet Appropriate Use Guidelines for the State of Arkansas. Retrieved August 12, 2006 from http://www.techarch.state.ar.us/domains/information/best_practices/InternetPolicy.htm

University of Arkansas. (2001). Code of Computing Practices. Retrieved August 12, 2006 from http://compserv.uark.edu/policies/code.htm