

1.0 Revision History

NORTHERN ARIZONA UNIVERSITY Network Acceptable Use Policy for Faculty and Staff	DOCUMENT NO.	ITS -105
	Effective Date	January 10, 2006
	Revision Date	
	Revision No.	
	Producer: Information Technology Services	

2.0 Purpose

Access to Northern Arizona University computing and network resources is a privilege which imposes certain responsibilities and obligations and which is granted subject to university policies and codes, and local, state and federal laws. All users of these shared resources must act responsibly and comply with specific policies and guidelines governing their use. The purpose of this policy is to promote the efficient, ethical and lawful use of Northern Arizona University's computer and network resources.

3.0 Definitions

- 3.1 Computing and network resources include both wired and wireless connectivity.
- 3.2 Network access includes connecting to the Northern Arizona University network on campus, through a university modem pool, remote computer lab, or another Internet Service Provider.
- 3.3 Student workers and temporary employees are considered staff for the purposes of this policy and must adhere to its provisions.
- 3.4 Strong passwords are those that use at least eight characters, includes a combination of letters, numbers, and symbols and is easy for you to remember, but difficult for others to guess.

4.0 Applicability

This policy applies to all staff, faculty, and affiliate users of Northern Arizona University computing and network resources, whether use is initiated from a computer and/or network device located on or off campus.

5.0 Policy

Faculty, staff and affiliates using computer resources belonging to Northern Arizona University must act in a responsible manner, in compliance with law and University policies, including the Acceptable Use Guidelines set forth in this Policy, and with respect for the rights of others using a shared resource. The right of free expression and academic inquiry must be balanced by the rights of others to privacy, freedom from intimidation or harassment, protection of intellectual property, ownership of data, and security of information.

6.0 Acceptable Use Guidelines

The specific usage guidelines that follow are not intended to be comprehensive, but rather to establish and clarify the intent of this Policy. Situations not enumerated here will inevitably arise, and they should be interpreted according to the spirit of this policy.

Each person using Northern Arizona University's computer and network resources must:

- 6.1 **Take no actions that violate the ABOR Policy Manual, Northern Arizona University Personnel Policy Manual, or other applicable law or policy, including this Policy.** This is not a comprehensive list of applicable Federal, State and University policies. In the event of a conflict between policies, the more restrictive use policy shall govern.

See the [Northern Arizona University Personnel Policy Manual](#) for more information. (Note: The manual is a large PDF file; downloading it over a dialup connection is not recommended.)

- 6.2 **Use security measures to protect the integrity of information, data, and systems.** Users must protect their computer systems and accounts by using strong passwords, installing anti-virus software consistent with management directives and by keeping such software, as well as the operating system and application security patches, up to date. Users are responsible for safeguarding their identification codes and passwords, and for using them only as authorized. Examples of misuse include: unauthorized use of a account; obtaining a password that you are not authorized to use; giving out your password to an unauthorized person; or using the campus network to gain unauthorized access to any computer system, and using a "sniffer" or other methods in an attempt to "crack" passwords.
- 6.3 **Not forge or misrepresent your identity.** Concealing or masking the identity of the sender of electronic communications by altering the source of an email message to make it appear as if the message was sent by someone else is a violation of this policy.
- 6.4 **Use computer and network resources efficiently.** Computing resources are the property of Northern Arizona University, not of

the individual user, are costly, are finite and must be shared. Employees may use the University's computer and network resources for incidental personal purposes, provided that such use does not (A) unreasonably interfere with the use of computing and network resources by other users, or with the University's operation of computing and network resources; (B) interfere with the user's employment or other obligations to the University; (C) violate this policy or other applicable policy or law; or (D) violate University licensed software contractual limitations and restrictions. The University retains the right to set priorities on use of the system, and to limit recreational or personal use when such use could reasonably be expected to cause, directly or indirectly, strain on any computing facilities, or to interfere with research, instructional or administrative computing requirements, or to violate applicable policies or laws.

- 6.5 Not harass or intimidate others.** The University, in general, cannot and does not wish to be the arbiter of content maintained, distributed or displayed by users of the University's computing and network resources. For example, the University, in general, cannot protect users from receiving e-mail they may find offensive. Unlawful or unauthorized use of University computer and network resources can expose the individual user and the University to damages claims and potential criminal liability. Unlawful or unauthorized uses may include, but are not limited to: harassment and intimidation of individuals on the basis of race, color, national origin, sex, religion, sexual orientation or disability; accessing, creation, display or transmission of obscenity, child pornography or material harmful to minors as defined by law; threats; theft; attempting unauthorized access to data; attempting to breach security measures on any electronic communications software or system; attempting to intercept electronic communication transmissions without proper authority; and violation of intellectual property or defamation laws. Do not use computer systems to send, post, or display libelous or defamatory messages, text, graphics, or images. Computer communication, including individual websites on university servers, should be respectful of others and should be consistent with Northern Arizona University values of civility, integrity and diversity, as well as the provisions of this policy.
- 6.6 Use University computer resources and networks for legitimate academic or administrative purposes.** Incidental

personal use is permissible to the extent that it does not violate other provisions of this policy, interfere with the performance of employee's duties, or interfere with the education of students at the University. Use of your computer account or the network for commercial activities that are not approved by appropriate supervisory University personnel consistent with applicable policy, or for personal financial gain (except as permitted under applicable academic policies) is prohibited. Examples of prohibited uses include using your computer account for engaging in unauthorized consulting services, illegally downloading copyrighted music, videos, or other material, software development, advertising products/services, and/or other private commercial activity. Compliance with specific regulations required of all state employees and agencies regarding lobbying and political activity must be followed by all university employees and affiliates and are detailed in the Northern Arizona University Personnel Policy Manual, Policy 5.10, Subject: Lobbying/Political Activity.

- 6.7 Respect copyright and intellectual-property rights.** Users must adhere to the U.S. Copyright Law and the terms and conditions of any and all software and database licensing agreements. Any form of original expression fixed in a tangible medium is subject to copyright, even if there is no copyright notice. The law also makes it unlawful to circumvent technological measures used by copyright owners to protect their works. Copyright infringement exposes the user, and possibly the University, to heavy fines and potential civil and criminal liability. Examples of materials potentially covered by copyright protection include music, movies, graphics, text, photographs, artwork and software distributed in any media -- including online. The use of a copyrighted work (such as copying, downloading, file sharing, distribution, public performance, etc.) requires either (A) the copyright owner's permission, or (B) an exemption or a fair use defense under the Copyright Law.
- 6.8 Make only appropriate use of data to which you have access.** Authorized University personnel (e.g. system, network and database administrators, among others) may have access to data beyond what is generally available. Privileged access to data may only be used in a way consistent with applicable laws, University policies, and accepted standards of professional conduct. Those who have access to databases that include personal information shall respect individual privacy and confidentiality, consistent with

applicable laws and University policies regarding the collection, use and disclosure of personal information. Examples of sensitive data that must be safeguarded are data protected by federal and state laws, including without limitation the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA), as well as any retained personal financial data.

6.9 Understand Limitations on Privacy Expectations. Users should be aware that state laws and University policies, guidelines and regulations may limit the protection of certain aspects of individual privacy. Both the nature of electronic communications and the public character of the University's business make certain uses less private than users may anticipate. For example, in certain circumstances, the University may permit the inspection, monitoring or disclosure of e-mail, consistent with applicable laws, by University personnel or law enforcement officers. The University also may be required to disclose e-mail and other electronic data and documents pursuant to the Arizona public records laws.

6.10 Respect and adhere to other departmental/college/Internet Service Provider's acceptable use policies. When using a University computer system and/or network to connect to a non-University system or network, adhere to the prevailing policies governing that system or network. This does not in any way release your obligation to abide by the established policies governing the use of the University's computer software, systems and networks.

7.0 Roles and Responsibilities

The roles and responsibilities of University employees subject to this Policy are set forth above.

8.0 Compliance

Violations of this Policy are subject to sanctions prescribed in, but not limited to, the following policies: Arizona Board of Regents (ABOR) Policy Manual, and the Northern Arizona University Personnel Policy Manual. Some potential sanctions are listed in Section 5 of the university personnel policy manual.

Employees who misuse Northern Arizona University's computing and network resources or who fail to comply with the University's written usage policies,

regulations and guidelines are subject to one or more of the following consequences:

- Temporary loss of computer/network access during incident investigations
- Disciplinary actions taken by the employee's supervisor up to and including termination of employment
- Legal prosecution under applicable Federal and State laws

9.0 References

- 9.1** Northern Arizona University Personnel Policy Manual (http://www.hr.nau.edu/m/images/stories/docs/policy_manual.pdf)
- 9.2** ABOR Policy Manual (<http://www.abor.asu.edu>)
- 9.3** U.S. Copyright Law (<http://www.copyright.gov/title17/>)