Responsible Executive: Chief Information Officer
Responsible Office: Information Technology Resources
Effective Date: June 1, 2006
Last Revised: August 19, 2022

STANDARDS FOR THE APPROPRIATE USE OF INFORMATION TECHNOLOGY RESOURCES

The capitalized terms used herein are defined in the Appropriate Use of Information Technology Resources policy.

1. Use Only the IT Resources You Are Authorized to Use.

1.1. Use of Northern Arizona University's Information Technology Resources ("IT Resources") is restricted to Authorized Users only. It is a violation of law and/or University policy to assist, encourage, or conceal from a proper authority any unauthorized use, or attempted unauthorized use, of the University's IT Resources.

1.2. Misrepresenting a person's identity or relationship to the University when obtaining access privileges for or when using the University's IT Resources is prohibited. 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 someone else sent the message is a serious violation of University policy.

1.3. It is a violation of University policy to access, or attempt to access, another person's University IT user account, or to use another person's account access credentials or data without express written authorization from the Chief Information Officer ("CIO") or their designee.

2. Only Use the University's IT Resources for Authorized Purposes. Use of University IT Resources is restricted to purposes consistent with the University's mission. All users shall serve as good stewards of the University's IT Resources as they are costly, finite and shared. The University's IT systems constitute neither a public forum nor a limited public forum. The University reserves the right to set priorities on use and to limit uses that could unreasonably constrain the availability or degrade the performance of IT Resources, or that could create undue system or institutional risk, interfere with University operations, or violate applicable laws, regulations, policies, standards, contracts or licensing agreements**.**

2.1. Personal Use of IT Resources. Incidental personal use of University IT Resources is permissible to the extent such use does not violate the *Appropriate Use Policy* ("AUP") or these appropriate use standards, does not unduly impede the University's mission, purposes and goals, and does not:

- unreasonably interfere with the use of computing and network resources by other Authorized Users or with the University's operation of computing and network resources;
- interfere with the Authorized User's duties and obligations to the University;
- violate University software contractual or licensing limitations or restrictions; or
- violate any other applicable law, regulation, policy, contract or agreement.

2.2. Commercial Uses. University IT Resources must not be used for commercial purposes without explicit written authorization from the President or their designee.

2.3. Political Uses. In accordance with Arizona law, Arizona Board of Regents ("ABOR") Policy 6-905 and Human Resources Policy 5.10 regarding lobbying and political activity, the University's IT Resources shall not be used for electoral purposes, personal political gain, or pursuit of public office.

2.4. Marketing and Trademark Uses. All IT Resource use shall occur in full compliance with ABOR and University policies regarding advertising, sales of commercial goods, and solicitations. The University has established an independent licensing program to control the use of the name, abbreviations, symbols, emblems, logos, mascots, slogans, and other terminology associated with the University. Unauthorized use of these representations may constitute trademark infringement. Any unauthorized production or sale of registered marks or names is a violation of the federal Lanham Trademark Act of 1946 and the federal Trademark Counterfeiting Act of 1984.

2.5. University Copyrights, **Patents and Intellectual Property Uses.** All uses of the University's IT Resources shall comply with federal and state copyright laws and ABOR policies and must respect the copyrights, trademarks, and intellectual property rights of the University and all others. Illegally copying, downloading, installing, distributing, infringing, or otherwise using any software, data, images, video, text, or other materials in violation of copyrights, trademarks, service marks patents, other intellectual property rights, contracts, or license agreements is prohibited.

2.6. Use of Data. Privileged access to data may only be used in a manner that is consistent with applicable laws, policies, and accepted standards of professional conduct. Employees who have been granted access to sensitive data (as defined in the *Data Classification and Handling* policy) must respect all individual privacy rights and guarantees of confidentiality consistent with applicable laws and 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 and regulated research data such as Controlled Unclassified Information ("CUI").

3. Abide by All Applicable Laws, Regulations, Policies and Contractual and Licensing Agreements. Unlawful or unauthorized use of University IT Resources can expose the individual user and the University to civil liability damage claims as well as 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, gender, sexual orientation or disability; accessing, creation, display or transmission of obscenity, child pornography or material harmful to minors as defined by law; threats; theft; unauthorized attempts to gain access to data; attempted breaches of IT or software security measures on any electronic communications system; attempting to intercept electronic communication transmissions without proper authority; and violation of intellectual property or defamation laws.

3.1. Copyright. All users are subject to the United States Copyright Act of 1976, as amended (Title 17, United States Code), and the Technology, Education and Copyright Harmonization (TEACH) Act of 2002, including ensuring that the restrictions that apply to the reproduction of electronic works and software are adhered to and that the bounds of copying permissible under the fair use doctrine are not exceeded. 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. 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.

3.2. Broadcast, Transmission and Export Uses. Any works or publications printed, disseminated, transmitted or broadcast using University IT Resources shall conform to applicable export and broadcast laws and regulations. It is the user's responsibility to know what restrictions certain works may be subject to, and to apply University IT Resource methods for adequately protecting those works.

4. Take Reasonable Care to Protect the Integrity of the University's IT Resources.

4.1. Access credentials shall only be issued to Authorized Users. Authorized Users are responsible for the protection of their Account, including, but not limited to, passwords, keys, pins, codes, badges, multi-factor tokens, etc.

4.2. Users shall not share or distribute access credentials unless the respective account was specifically created for such purposes.

4.3. Only those persons with proper authorization shall modify or reconfigure University IT Resources.

4.4. It is a violation of the AUP policy to tap a telephone line or run a network “sniffer” or vulnerability scanner without the express written authorization of the CIO.

4.5. Persons shall not create, install, or knowingly distribute a virus, key logger, malware, or other surreptitiously invasive program on any University IT Resource or IT facility without the express written authorization of the CIO.

4.6. Authorized Users are advised to use only those systems officially licensed or sanctioned by the University. Users are strongly cautioned about using free software or social internet sites for conducting official University business. This includes, but is not limited to, software identified on federal executive orders prohibiting its use. There may be substantial risks to the protection of information on such sites and individuals may be held personally liable for damages or violations resulting from such uses.

4.7. The unauthorized disclosure of information to the public is prohibited.

5. Respect the Privacy and Personal Rights of Others. In furtherance of the AUP, the right of free expression and academic inquiry must be balanced against or tempered by the rights of others to privacy, freedom from intimidation or harassment, protection of intellectual property, and the stewardship of data, information and State resources. Moreover, all University IT Resources and network facilities are subject to A.R.S. §§ 39-101, *et seq.* regarding public records and A.R.S. § 38-431.01 regarding open meetings. Authorized Users, therefore, have no expectation of privacy of materials stored on or transmitted via University IT Resources. The University does not guarantee the privacy or confidentiality of computer files, electronic mail, or other information stored on or transmitted via its IT Resources.

5.1. Limitations on Privacy Expectations. Users of IT Resources should be aware that various laws, regulations, or policies 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 email, consistent with applicable laws, by University personnel or law enforcement officers. The University also may be required to disclose email and other electronic data and documents pursuant to the Arizona public records laws.

5.2. Unauthorized Copy. It is a violation of these standards and the AUP to access or copy another user's electronic mail, data, programs, or other files without express written authorization of a university official authorized by the Office of General Counsel, CIO, or the Chief Human Resources Officer.

5.3. Conditions for Permitting Inspection, Monitoring, or Disclosure. The University reserves the right to access and examine any of its IT Resources or devices attached to University IT Resources upon reasonable belief that federal or state laws have been violated or where the University's contractual obligations or its operations may be impeded; in order to preserve the integrity of its systems, monitor resource utilization, ensure compliance with institutional and operational standards, to cooperate with internal investigations or to comply with lawfully issued subpoenas or civil discovery orders; and in cases of emergency. All Authorized Users must cooperate and comply with all reasonable University requests for access to and copies of electronic mail messages or data when such access or disclosure is authorized by the AUP or allowed or mandated by applicable law, regulation or policy. The University may permit the inspection, monitoring, or disclosure of email, computer files, and network transmissions when:

- required or permitted by law, including public records law, or by subpoena or court order;
- to prevent disruption to and misuse of University electronic communications resources, services, and activities;
- the University or its designated agent reasonably believes that a violation of law or policy has occurred; or
- it is otherwise necessary and appropriate to monitor and preserve the functioning and integrity of computer systems or network facilities.

5.4. Routine Logging and Monitoring. Certain IT Resource utilization activities from devices connected to the network are routinely logged and monitored to ensure the reliability and security of University IT Resources and related services. These activities include, but are not limited to:

- use of passwords and accounts accessed;
- time, duration and location of network activity;
- accessing of various IT Resources such as servers or data storage; and
- volume of data storage and transfers

5.5. IT Resource and Data Inspections. In cases of suspected violations of the applicable law or policy, and, in particular, in cases of suspected unauthorized access to computing systems, System Administrators, after appropriate consultation with the Director of Information Security Services or their designee, and other University offices or officials as may be appropriate, may authorize detailed inspection of University IT Resources or other devices attached to the University's information or communication networks.

6. Do No Harm. The University, in general, cannot and does not wish to serve as the arbiter of content maintained, distributed, or displayed by users of the University's IT Resources. For example, the University, in general, cannot protect users from receiving email or telephone calls they may find offensive. All communication in all forms, however, should be respectful of others and should be consistent with the University's professional values of civility, integrity, respectfulness and diversity, as well as the provisions of the AUP and these standards for the appropriate use of IT Resources. Accordingly:

- Authorized Users shall take full responsibility, and will be fully accountable, for their use of the University's IT Resources;
- IT Resources shall not be used to send, post, or display libelous or defamatory messages, text, graphics, or images, or to transmit or participate in any communications prohibited by law, including, but not limited to, fraudulent, harassing, obscene, or threatening messages;
- IT Resources shall be disposed of according to established procedures, and no technology shall be implemented, used or disposed of in such a way that causes harm to persons or animals, or violates environmental protection laws; and
- research use of IT Resources shall conform to conditions of institutional approval through the University's Institutional Review Board for projects utilizing human and animal subjects.

Please contact the Chief Information Officer with any inquiry or feedback regarding these standards for the appropriate use of the University's Information Technology Resources.