Academic Affairs Manual (ACD)

ACD 125: Computer, Internet, and Electronic Communications Information Management Policy

Effective: 9/28/2000 **Revised**:11/1/2016

Purpose

To govern the use of ASU computing and communications resources and to manage and secure ASU data and other information assets

Sources

University Technology Office

University Senate

Applicability

Students

Faculty

Administrative, classified, and university staff

Academic professionals

Courtesy affiliates

Contents

Policy

Introduction

This policy defines the boundaries of acceptable use of ASU computing and communication resources, including computers, data storage systems, mobile devices, electronic data, networks, electronic mail services, electronic

information sources, voice mail, telephone services, and other communication resources. In addition, this policy reflects the goal of ASU to foster academic freedom while respecting the principles of freedom of speech and the privacy rights of ASU students, faculty, employees, courtesy affiliates, and guests.

ASU's computing and communication resources are the property of ASU. They are to be used for the advancement of ASU's educational, research, service, community outreach, administrative, and business purposes. Computing and communication resources are provided for the use of faculty, staff, currently admitted or enrolled students, and other properly authorized users. When a user's affiliation with ASU ends, ASU will terminate access to computing and communications resources and accounts. ASU may, at its discretion, permit the user to have the access to accounts and e-mail forwarded or redirected for a limited period of time.

The University Technology Office (UTO) is responsible for the maintenance and security of ASU's central computing and communications resources. This includes recommendations for effective practices by its users, which include faculty, staff, students, and affiliates. This policy is designed to aid the university community in protecting the confidentiality, availability, and integrity of university information resources.

Users of ASU's computing and communications resources are required to comply with this policy, other applicable ASU and Arizona Board of Regents' (ABOR) policies, and state and federal laws. When necessary, enforcement will be consistent with other applicable ABOR policies and ASU administrative policies and procedures.

Requirements and Prohibited Uses

Requirements for the Use of ASU Computing and Communications Resources

1. Users must comply with all applicable local, state, and federal laws and regulations, and with ASU and ABOR policies.
2. Users must respect academic freedom and free speech rights.
3. Users must be truthful and accurate in personal and computer identification.
4. Users must respect the rights and privacy of others, including intellectual property and personal property rights.
5. Users must not compromise the integrity of electronic networks, must avoid restricted areas, and must refrain from activities that may damage the network, or transmitted or stored data.
6. Users and individuals responsible for system administration must maintain the security of accounts and are required to protect and regularly change their account passwords according to standards maintained by the UTO.
7. Users, once aware of a security concern, must notify the Information Security Office of information security concerns including, but not limited to, breaches of sensitive data or compromised accounts.
8. Users are responsible for the protection, security, and integrity of university data and resources under their control according to the standards maintained by the UTO. See the Information Security Standards for more information.

Prohibited Uses of ASU Computing and Communications Resources

1. Unlawful communications, including threats of violence, obscenity, child pornography, and harassing communications, are prohibited.
2. Use of ASU computer resources for private business or commercial activities, or for fund-raising or advertising on behalf of non-ASU organizations, is prohibited.
3. The unauthorized reselling of ASU computer resources is prohibited.
4. Unauthorized use of university trademarks or logos and other protected trademarks and logos is prohibited.
5. ASU Web pages may link to commercial Web sites, but any link that generates, or has the potential to generate, revenue to ASU or to any individual or company, including click trade or banner advertising, must be approved by Purchasing and Business Services.
6. College and department Web sites may include links to commercial Web sites to provide information related to the mission or function of the college or academic or administrative unit. Any link that generates, or has the potential to generate, revenue to the college or academic or administrative unit must be approved through Purchasing and Business Services.

7. Any alteration of addresses, uniform resource locator (URL), or other action that masks the asu.edu domain as a host site is prohibited unless authorized by the UTO.
8. Unauthorized anonymous and/or pseudonymous communications are prohibited. All users are required to cooperate with appropriate ASU personnel or other authorized personnel when investigating the source of anonymous messages.
9. Misrepresenting or forging the identity of the sender or the source of an electronic communication is prohibited.
10. Unauthorized attempts to acquire and use passwords of others are prohibited.
11. Unauthorized use and attempts to use the computer accounts of others are prohibited.
12. Altering the content of a message originating from another person or computer with intent to deceive is prohibited.
13. Unauthorized modification or deletion of another person's files, account, or news group postings is prohibited.
14. Use of ASU computer resources or electronic information without authorization or beyond one's level of authorization is prohibited.
15. Interception or attempted interception of communications by parties not authorized or intended to receive them is prohibited.
16. Making ASU computing resources available to individuals not affiliated with ASU without approval of an authorized ASU official at or above the level of dean/university librarian or director is prohibited.
17. Compromising the privacy or security of electronic information is prohibited.
18. Infringing upon the copyright, trademark, patent, or other intellectual property rights of others in computer programs or electronic information (including plagiarism and unauthorized use or reproduction) is prohibited. The unauthorized storing, copying, or use of audio files, images, graphics, computer software, data sets, bibliographic records, and other protected property is prohibited except as permitted by law.
19. Interference with or disruption of the computer or network accounts, services, or equipment of others is prohibited.
20. The propagation of computer "worms" and "viruses," the sending of electronic chain mail, denial of service attacks, and inappropriate "broadcasting" of messages to large numbers of individuals or hosts are prohibited.
21. Failure to comply with requests from appropriate ASU officials to discontinue activities that threaten the operation or integrity of computers, systems, or networks, or that otherwise violate this policy is prohibited.
22. Revealing passwords or otherwise permitting the use by others (by intent or negligence) of personal accounts for computer and network access without authorization is prohibited.
23. Altering or attempting to alter files or systems without authorization is prohibited.
24. Scanning of networks, networked devices, or applications for security vulnerabilities without specific authorization by the UTO is prohibited.
25. Attempting to alter or connect any computing or networking components (including, but not limited to, bridges, routers, DHCP servers, wireless access points, and hubs) on the ASU network without approval of the UTO is prohibited.
26. Installation or alteration of wiring, including attempts to create network connections, or any extension or retransmission of any computer or network services without the approval of the UTO is prohibited.
27. Conduct leading to disruption of electronic networks or information systems is prohibited.
28. Conduct leading to the damage of ASU electronic information/data, computing/networking equipment, and resources is prohibited.

Prohibited Access

ASU may restrict access from within its network to any sites in furtherance of this policy. A user may contact UTO to request access to a restricted site or to report that a site was restricted in error.

Information Posted to ASU Computers or Web Pages

Restriction on Use of ASU Web Pages

ASU Web pages may be used only for ASU business and only authorized individuals may modify or post materials to these pages. No other pages may suggest that they are university Web pages. If confusion is possible, pages should contain a disclaimer and links to ASU sites.

Responsibilities of Individuals Posting Materials

By posting materials and using ASU computing facilities, the user represents that he or she has created the materials or that he or she has the right to post or use the materials. The storage, posting, or transmission of materials must not violate the rights of any third person in the materials, including copyright, trademark, patent, trade secrets, and any rights of publicity or privacy of any person. The materials posted must not be defamatory, libelous, slanderous, or obscene.

Prohibition against Commercial Use

The site may not be used for unauthorized commercial purposes.

University Control of ASU Web Pages

The use of the site is at the sole discretion of ASU. ASU does not guarantee that the user will have continued or uninterrupted access to the site. The site may be removed or discontinued at any time at the discretion of ASU in accordance with ASU policy, or as needed to maintain the continued operation or integrity of ASU facilities.

ASU makes reasonable efforts to protect the integrity of the network and related services, but ASU cannot guarantee backup, disaster recovery, or user access to information posted on personal computers or Web pages.

Access to services and file storage may be approved for emeriti, retired staff, alumni, and guests.

Electronic Mail and Electronic Communications

Conditions for Restriction of Access to Electronic Mail

Access to ASU e-mail is a privilege that may be wholly or partially restricted without prior notice and without consent of the user:

1. if required by applicable law or policy
2. if a reasonable suspicion exists that there has been or may be a violation of law, regulation, or policy

   or

3. if required to protect the integrity or operation of the e-mail system or computing resources or when the resources are required for more critical tasks as determined by appropriate management authority.

Access to the e-mail system may require approval of the appropriate ASU supervisory or management authority (e.g., department head, system administrator, etc.).

Conditions for Permitting Inspection, Monitoring, or Disclosure

ASU may permit the inspection, monitoring, or disclosure of e-mail, computer files, and network transmissions when:

1. required or permitted by law, including public records law, or by subpoena or court order
2. ASU or its designated agent reasonably believes that a violation of law or policy has occurred

   or

3. necessary to monitor and preserve the functioning and integrity of the e-mail system or computer systems or facilities.

All computer users agree to cooperate and comply with ASU requests for access to and copies of e-mail messages or data when access or disclosure is authorized by this policy or required or allowed by law or other applicable policies.

ASU Responsibility to Inform of Unauthorized Access or Disclosure

If ASU believes unauthorized access to or disclosure of information has occurred or will occur, ASU will make reasonable efforts to inform the affected computer account holder, except when notification is impractical or when notification would be detrimental to an investigation of a violation of law or policy.

Prohibition against Activities Placing Strain on Facilities

Activities that may strain the e-mail or network facilities more than can be reasonably expected are in violation of this policy. These activities include, but are not limited to: sending chain letters; "spam," or the widespread dissemination of unsolicited e-mail; and "letter bombs" to resend the same e-mail repeatedly to one or more recipients.

Confidentiality

Confidentiality of e-mail and other network transmissions cannot be assured. Therefore all users should exercise caution when sending personal, financial, confidential, or sensitive information by e-mail or over the network.

Electronic Information as Arizona Public Record

Most electronic information (e.g., e-mail) produced in the course of university business is considered an Arizona public record, and must be stored or deleted in accordance with Arizona public records law. Consult with the university archivist for guidance on procedures for external storage or deletion of public records.

Privacy and Security

Routine Logging and Monitoring

Certain central service and network activities from workstations connected to the network are routinely logged and monitored. These activities include but are not limited to:

1. use of passwords and accounts accessed
2. time and duration of network activity
3. access to Web pages
4. access to network software
5. volume of data storage and transfers

   and

6. server space used for e-mail.

Detailed Session Logging

In cases of suspected violations of ASU policies, especially unauthorized access to computing systems, the appropriate system administrator, after consultation with the University Technology Officer/designee or other university offices if appropriate, may authorize detailed session logging. This may involve a complete keystroke log of an entire session. In addition, the system administrator of the facility concerned may authorize limited searching of user files to gather evidence on a suspected violation.

Responsibility for Data Security

Software and physical limitations, computer viruses, and third-party intrusions can compromise security of data storage and communications. ASU takes reasonable precautions to minimize risk. Users must notify appropriate ASU officials including their immediate supervisor and the Information Security Office of information security concerns including, but not limited to, breaches of sensitive data or compromised accounts.

Computing resources are managed by individual users, departments, or the UTO, depending on a variety of business factors. The UTO is not obligated to maintain backups of any file for any particular length of time. Users must protect and back up critical data. Individual users and departments should develop policies and practices, coordinated with the

UTO as needed, to ensure regular backups of data and to implement steps to ensure that all critical data is compatible with all current generations of computing equipment, storage media, and media readers.

Restriction of Access to Sensitive Data

All ASU departments should ensure that access to sensitive data is restricted to those employees who have a need to access the information. Passwords that provide access to sensitive information should be changed on a regular basis.

Right to Examine Computers and Equipment

University-owned computers and equipment may be examined to detect illegal content and to evaluate the security of the network.
Networks, networked devices, and applications may be scanned for vulnerabilities as authorized by the UTO.

Violations and Enforcement

Reporting Violations

Any actual or suspected violation of the rules listed above should be brought to the system administrator of the equipment or facility most directly involved. In the case of a serious violation, a report must be made to the Information Security Office.

ASU Response to a Reported Violation

Upon receiving notice of a violation, ASU may temporarily suspend a user's privileges or move or delete the allegedly offending material pending further proceedings.

A person accused of a violation will be notified of the charge and have an opportunity to respond before ASU imposes a permanent sanction. Appropriate cases will be referred to the ASU disciplinary authority appropriate to the violator's status (e.g., Office of Student Life or employee's supervisor) or to appropriate law enforcement authorities.

In addition to sanctions available under applicable law and ASU and ABOR policies, ASU may impose a temporary or permanent reduction or elimination of access privileges to computing and communication accounts, networks, ASU-administered computing rooms, and other services or facilities.

If ASU believes it necessary to preserve the integrity of facilities, user services, or data, it may temporarily suspend any account, whether or not the account user is suspected of any violation. ASU will provide appropriate notice to the account user. Servers and computers that threaten the security of university systems will be removed from the network and allowed to reconnect only with the approval of network administration.

Applicable Law and Policies

ASU students and employees are bound by all applicable laws and ABOR and university policies. For ease of reference, some frequently referenced policies in ASU manuals are listed in the cross-references at the end of this policy. Some frequently referenced policies not in ASU manuals are listed in the section below. This list is not intended to be exhaustive nor to limit the applicability of any other law or policy.

Frequently Referenced Policies not in ASU Manuals

1. Student Academic Integrity Policy
2. Conditions of Faculty Service
3. Conditions of Professional Service
4. Intellectual Property Policy
5. Procurement Procedures
6. Information Security Standards

Cross-References

For related information about the conditions of administrative service, see the *Academic Affairs Policies and Procedures Manual*—ACD 504, "*Conditions of Administrative Service* at ASU."

For related information about student behavior, see the *Student Services Manual*— SSM 104–01, "*Student Code of Conduct* and Student Disciplinary Procedures."

For related information about disability accommodations, see:

1. the *Academic Affairs Policies and Procedures Manual*—ACD 405, "Individuals with Disabilities"

   and

2. the *Student Services Manual*—SSM 701–06, "Accommodations in Campus Computer Labs for Students with Disabilities."

For related information about use of university property, see the *Academic Affairs Policies and Procedures Manual*—ACD 123, "Misuse of University Assets"

For related information about appropriate and inappropriate political activity, see:

1. the *Academic Affairs Policies and Procedures Manual*—ACD 205–01, "Political Activity and Lobbying"

   and

2. the *Staff Personnel Policies and Procedures Manual*—SPP 813, "Code of Conduct for Business Activities."

For related information about preventing the loss of trademark rights, see the *Purchasing and Business Services Policies and Procedures Manual*—PUR 222, "Trademark Licensing."

For related information about sexual harassment, see:

1. the *Academic Affairs Policies and Procedures Manual*—ACD 402, "Romantic or Sexual Relationships Between Faculty Members and Students"

   and

2. the *Student Services Manual*—SSM 304–04, "Nondiscrimination—Sexual Harassment."

For related information about personnel records, including the use and release of personal records, see:

1. the *Academic Affairs Policies and Procedures Manual*—ACD 811, "Access to and Release of Official Personnel Records
   Information"
2. the *Staff Personnel Policies and Procedures Manual*—SPP 1101, "Personal Records"

   and

3. the *Student Services Manual*—SSM 107–01, "Release of Student Information."