Acceptable Use Policy

APPROPRIATE USE OF COMPUTING FACILITIES

Introduction

Computing and networking play increasingly important roles in education, research, and administration in the University. We anticipate many benefits from the use of technology by students, faculty, and staff.

We have formulated our policy on the appropriate use of computing and networking facilities to ensure the proper use of these resources. The intent of this policy is to allow the greatest use of our computing facilities consistent with the general principles that govern our academic community.

Access to computer systems and networks owned or operated by the University of Science and Arts of Oklahoma imposes certain responsibilities and obligations and is granted subject to University policies, and local, state, and federal laws. Appropriate use always is ethical, reflects academic honesty, and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of data, system security mechanisms, and individuals' rights to privacy and to freedom from intimidation, harassment, and unwarranted annoyance.

This document contains the University of Science and Arts of Oklahoma Policy for the Appropriate Use of Computer Facilities. Please read this policy carefully. Additional policies may govern the use of particular resources. Be sure to familiarize yourself with these guidelines.

Appropriate Use of Computer Facilities Policy No. 1 February 1, 1996 (modified 11/01/02)

USAO maintains computing and networking facilities for the purpose of conducting and fostering the instructional and research activities of the University. The Appropriate Use of Computer Facilities policy was designed to ensure the proper use of computing facilities consistent with the general principles that govern our academic community. To maximize usefulness of Computer Facilities to instructional and research activities, the University provides access in the most open manner permitted by the providers of the Computing Facilities.

In this policy, the term, "Computer Facilities," is defined to include computers, computer networks, connections to external computer networks, and subscriptions to external computer services. "Licensed Software" collectively refers to copyrighted and proprietary programs, data and documentation. "Software" collectively refers to the programs, data, and documentation developed from the University's instructional and research activities by the Faculty, Students, and Staff of the University.

In making appropriate use of resources you must:

- Use resources only for authorized purposes.
- Protect your user ID from unauthorized use. You are responsible for all activities on your user ID or system.
- Access only files and data that are your own, that are publicly available, or to which you have been given authorized access.
- Use only legal versions of copyrighted software in compliance with vendor license requirements.
- Be considerate in your use of shared resources. Refrain from monopolizing systems, overloading networks with excessive data, or wasting computer time, connect time, disk space, printer paper, manuals, or other resources.
- Be considerate of other users. Occasional use of Computer Facilities for game playing may be allowed for the purpose of improving computer literacy. Unless the game playing is required for a class, you must restrict your use of games to vacant workstations and must immediately yield the terminal/computer to another authorized non-game user.

The following activities involving use of Computer Facilities are prohibited:

- Transmitting or receiving copyrighted materials (software, music, movies, etc.) not legally obtained.
- Using another person's user ID, password, files, system or data. You may be required to show identification to verify that you are using the correct user ID. A user ID which is found to have been used by other than its rightful owner may be suspended.
- Communicating any information concerning any password, identifying code, personal identification number or other confidential information without the permission of its owner or the controlling authority of the Computer Facility to which it belongs;
- Using computer programs to decode passwords or access control information.
- Attempting to circumvent or subvert system security measures.
- Engaging in any activity that might be harmful to systems or to any information stored thereon, such as creating or propagating viruses, disrupting services, or damaging files.
- Transmitting unsolicited information which contains obscene, indecent, lewd or lascivious material or other material which explicitly or implicitly refers to sexual conduct;
- Creating, modifying, executing or retransmitting any computer program or instructions intended to obscure the true identity of the sender of electronic mail or electronic messages, collectively referred to as "Messages," including, but not limited to, forgery of Messages and/or alteration of system and/or user data used to identify the sender of Messages;
- Using mail or messaging services to harass, intimidate, or otherwise annoy another person, for example, by broadcasting unsolicited messages or sending unwanted mail.

- Transmitting unsolicited information which contains profane language or panders to bigotry, sexism, or other forms of discrimination;
- Using University systems for partisan political purposes, such as using electronic mail to circulate advertising for political candidates.
- Creating, modifying, executing or retransmitting any computer program or instructions intended to gain unauthorized access to, or make unauthorized use of, a Computer Facility, Software or Licensed Software;
- Making unauthorized copies of copyrighted materials, such as licensed software, music, movies, etc.;
- Wasting computing resources, for example, by intentionally placing a program in an endless loop or by printing excessive amounts of paper.
- Using the University's systems for personal gain, for example, by selling access to your user ID or by performing work for profit in a manner not authorized by the University.
- Violating any laws or participating in the commission or furtherance of any crime or other unlawful or improper purpose;
- Using the Computer Facilities in a manner inconsistent with any published University policy.

Campus Electronic Access Policy:

USAO's policy is to allow students, faculty and staff access for educational and research purposes. Use for commercial purposes is expressly prohibited.

Mailing Lists:

Potential subscribers of an electronic mailing list are responsible for determining the purpose of the list before subscribing. Persons subscribing to an electronic mailing list will be viewed as having solicited materials delivered by the list as long as the material is consistent with the list's purpose. Persons sending materials to a mailing list, which are not consistent with the purpose of the mailing list, will be viewed as having sent unsolicited materials.

Exceptions:

The Chief Technology Officer, the Vice-Presidents of the University, or the President of the University may approve exceptions. Governing Law Federal and State Law also regulates unauthorized access to Computer Facilities, Software and Licensed Software. A brief summary of Federal Law relevant to this issue follows. Note that the laws of other states may apply depending on the actual location of the Computer Facility/ies in question.

Federal Law:

It is a violation of Federal Law intentionally (1) to access a computer without authorization and thereby to obtain classified information; (2) to access a computer without authorization and

thereby to obtain financial records of a financial institution; (3) to access any U. S. Government computer without authorization if such conduct affects the use of the Government's operation of the computer; (4) to access a Federal computer without authorization with the intent to defraud; (5) to access a financial institution or U. S. Government computer without authorization and thereby alter, damage, or destroy information which causes losses to others of a value exceeding $1,000 or more during any one year or which modifies or impairs medical diagnosis, treatment, or care; or (6) with intent to defraud to traffic in passwords or similar information through which a computer may be accessed if the trafficking affects interstate commerce or the computer is used by the U. S. Government. The penalty can be a fine or as much as 20 years in the Federal penitentiary for certain of these violations. (18 USCA sec. 1030) Copyright is a constitutionally conceived property right which is designed to promote progress of science and the useful arts by securing for an author the benefits of his/her original work for a limited time (US Constitution Art. I, Sec.8). Congress has passed the Copyright statute (17 USCA sec. 101 et seq) to implement this policy by balancing the author's interest against the public interest in the dissemination of information affecting areas of universal interest.

Enforcement:

The University considers any violation of appropriate use principles or guidelines to be a serious offense and reserves the right to copy and examine any files or information residing on any computer or system within the University network allegedly related to inappropriate use. Violators are subject to disciplinary action as prescribed in the honor codes and the student, faculty, and staff handbooks. Offenders also may be prosecuted under laws including (but not limited to) the Privacy Protection Act of 1974, The Computer Fraud and Abuse Act of 1986, The Computer Virus Eradication Act of 1989, Interstate Transportation of Stolen Property, and the Electronic Communications Privacy Act.

Questions:

If you have questions about the contents of these policies contact Information and Technology Services (Austin Hall, room 113, or 405-574-1234, or ithelpdesk@usao.edu). If necessary, the technicians will help direct your query to the proper authorities