TECHNOLOGY & NETWORK USAGE POLICY

Application: This policy applies to all computer systems and networks operated and managed by UCO colleges, academic, and administrative departments.

INTRODUCTION

The University of Central Oklahoma has the responsibility for securing its computing and networking systems (both academic and administrative) against unauthorized access, while making the systems accessible for legitimate academic and administrative uses. This responsibility includes informing persons who use the UCO computer and network systems of expected standards of conduct and encouraging their application. It is important for the user to practice ethical behavior in computing activities because the user has access to many valuable and sensitive resources and the user's computing practices can adversely affect the work of other people. Improper use and abuse of the computers and networks will not be permitted.

PURPOSE

This policy provides direction to be used in managing computer resources and in allowing or denying access to UCO computer or network resources.

Unauthorized Use of UCO Computing Equipment

Allowing others to use one's User ID and password.

Inappropriately using the computing facilities at other sites through network connections from UCO (e.g. illegal or unauthorized access; modifications to programs or information, etc.).

Using abusive or harassing language.

Viewing pictures of an erotic or sexual nature when such images are able to be viewed by others who are offended by them; and, mailing, printing, or copying obscene materials.

THEFTS OF SERVICES

Thefts of services can be a crime under state and federal law. Violators may be referred to the appropriate authority for disciplinary action. Accounts may be subject to immediate deactivation.

COMPUTER ACCOUNTS

Student accounts will be considered inactive if students do not maintain continuous enrollment in successive fall and spring semesters. Enrollment in the summer session is not required to maintain continuous enrollment from the spring to the fall semester in the same calendar year.

MAILBOX SIZE

If a user's mailbox reaches 70% utilization, a notice will be sent requesting that the user delete some messages; if the mailbox reaches 100% capacity new mail will not be received. Notes

STATEMENT OF USE

This policy of computing practice applies to all persons using the UCO computing and networking systems. Disciplinary action for violating the policy shall be governed by, but may not be limited to, the applicable provisions of student handbooks, faculty and staff handbook, policies of the University of Central Oklahoma, Board of Regents of Oklahoma Colleges, Oklahoma State Regents for Higher Education, Statutes of the State of Oklahoma and federal law. Persons who violate this policy may also have their access privileges to UCO computing and networking systems revoked.

1. Computer and network system users are responsible for following the published procedures to access UCO and other University of Central Oklahoma computing systems and networks.
2. A user must use only the computer accounts which have been authorized for his/her use.
3. Users are responsible for the use of their computer accounts. Users should make appropriate use of system-provided protection features such as passwords and file protections, and should take precautions against others obtaining access to their computer resources. Users should not make an account available to others for any purpose. If assistance is needed in using an account, contact Information and Technical Support (helpdesk) at extension 2255 or support@uco.edu.
4. Computer accounts and access to networks interred, UCO Department networks, etc., must be used only for the purposes for which they are authorized. For example, student faculty and staff accounts, issued for legitimate classroom or office work, cannot be used for non-UCO related private consulting, commercial enterprise and/or personal financial gain.
5. The computer will not be used as an instrument to intimidate or offend persons. Using the computer as a means of communication to terrify, intimidate, threaten, harass, annoy or offend another person constitutes grounds for cancellation of access to UCO computers/networks and may result in disciplinary and/or legal actions. Use of a computer as a means of: a) communicating indecent, lewd or obscene language to another person, or b.) communicating a threat or lewd suggestion to another person, shall be prima face evidence of an intent to terrify, intimidate, threaten, harass, annoy or offend.
6. Playing computer games other than for educational purposes on UCO computers is not allowed and may result in the loss of access to UCO computers and networks.
7. Users shall not access, copy, or transport privileged programs, files, or data without prior authorization. User software may be used on computers only if it has been legally obtained and

if its use does not violate license or copyright restriction. Users may not inspect, modify, distribute or copy privileged data or software.

8. Users shall not attempt to encroach on others' use of the facilities or deprive them of resources.
9. Users shall not attempt to modify system facilities. Users should not damage or obstruct the operation of the computer systems or networks.
10. Users should avoid or schedule for non-peak hours intense computing and/or transmission activities which would degrade system performance.
11. Users shall not supply, or attempt to supply, false or misleading information or identification in order to access computer systems or networks.
12. Users shall not attempt to subvert the restrictions associated with any computer accounts.
13. Users shall not examine, change, or use another person's (or institutional) username, password, files or e-mail.
14. Users shall always identify themselves appropriately and undertake no activities anonymously.
15. Electronic data on all UCO systems is private and confidential.
16. Use of OneNet , SREB, and other systems to which UCO connects and /or is associated with, shall be governed by the policies and guidelines of said service.

COMPUTER/DATA COMMUNICATION RESOURCE MANAGEMENT

The University will not guarantee the privacy or integrity of user's files, including e-mail, but will use its best efforts to protect the integrity of individual user accounts and files from access and use by unauthorized persons. The University does not routinely review user's files including e-mail, however, in cases of system failure and subsequent repair or where there is reason to believe there has been unauthorized use or misuse of computer resources, Office of Information Technology computing personnel, UCO Department of Public Safety personnel and administrative personnel of the university shall have the authority and right to monitor, review and audit individual user files, including email. Individual user files may also be reviewed , audited or searched when subject to court order, subpoena or other process of law.

1. All files stored on the computer mainframe and UCO file servers may be routinely copied to a tape or disk. Information can be recovered by systems administration personnel.
2. All files created, stored, uploaded or received through electronic mail are subject to audit and / or review by specifically designated computer administrators/managers. A review/audit may include files stored in a user's active account or archived on tape or disk. Such reviews/audits will be in compliance with federal and state law, as well as appropriate university policies and procedures.
3. Acceptance of a UCO computer account and /or use of UCO computing equipment constitutes consent to appropriate monitoring.
4. Questions about the use, material or links not covered in these policies and guidelines should be brought to the attention of the Office of Information Technology before the user conducts the activity in question.
5. All new purchase of desktop systems shall:

a. Conform to the Desktop Management Interface protocol and
b. Be purchased with a minimum three years parts and labor warranty from the manufacturer.

OBSCENITY LAW AND THE INTERNET

Oklahoma has adopted the Miller test (Miller vs. California, 1973) and has attached criminal penalties to obscene expression. The Miller test provides the following definitions of obscenity:

1. Whether the average person, applying contemporary community standards would find that the work, taken as a whole, appeals to the prurient interest:
2. Whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law: and
3. Whether the work, taken as a whole, lacks serious literary, artistic political or scientific value

Federal law prohibits conduct similar to that at the state level. The general federal restriction on obscenity is codified at 18 U. S. C. S. 1461-1465.

WORLD WIDE WEB (WEB) HOMEPAGE CONSTRUCTION

UCO recognizes the benefit to the public and to members of the university community of electronic publishing on the Internet. Subject to resources available,

The university provides access distribution, storage capacity maintenance and other creative and technical support of academic and administrative units, for educational use and other purposes consistent with official university business.

Websites are to be developed and maintained responsibly in compliance with university policy, and applicable state and federal laws. The Office of Information Technology and the Office of University Relations will review and monitor departmental and college websites to ensure technical integrity and protection of the University's image. Please refer to the UCO Principles and Guidelines for Use of the World Wide Web.

DISTRIBUTION

This policy shall be distributed to all managers of UCO systems and file servers, users of the UCO computing and network facilities, Information Technology personnel, and Department of Public Safety personnel. This document is accessible on the UCO Website

EFFECTIVE DATE

Created: May 1, 1998
Revised: 2/25/03
Title Revision: 5/2/06

OFFICE OF
Information Technology
UNIVERSITY OF CENTRAL OKLAHOMA

For additional help or assistance, contact the UCO Service Desk at 405.974.2255 or support@uco.edu.