Oklahoma City University
Computer Use Policy

(7/1/03)

Introduction

General

As an institution of higher education, Oklahoma City University will implement and maintain computer and electronic network systems to enhance, promote, and support the academic advancement and administrative services of the university. Students, faculty, staff, and guests may be granted access to and use of these systems as deemed appropriate by the university President or his or her authorized representatives. Authorized users of campus resources should use campus networks and computers wisely and consider the rights of others. The following policy provides guidelines and regulations for the proper use of computer and network resources on campus. The university will not tolerate the misuse of these resources.

Scope

This policy applies to all students, faculty, staff, and guests who use OCU networks, computer systems, and PC's. It covers all university-owned equipment and non-university-owned equipment residing on university property connected to university networks**.** It is applicable to all residence hall facilities, including the Cokesbury Court Apartments. All references in this policy to residence halls include Cokesbury Court apartments.

Use of any computer attached to a university network binds the user to this policy regardless of the ownership of said computer.

Section I: Computer Facility Guidelines

1. Introduction

Faculty, staff, and students are granted the *privilege* to use university computer facilities and data or voice communication networks. This policy provides guidance in the proper use of university computer, network, and communication systems.

For the purposes of this document, Campus Technology Services is a centrally managed group of support personnel responsible for the administration of university computer and network systems. Campus Technology Services is responsible for the administration, proper access and use, protection, and security of university systems and networks, and will take all actions necessary to protect and ensure proper use of these systems.

2. Authorized Users

Students: Students are authorized access to campus networks through campus labs and the residence halls. Access includes a login account to campus networks, an electronic mail account, and disk storage space on the student home server. Access to other systems or network services may be granted and revoked by university departments. Students may use their e-mail for personal communications; however, OCU administration cautions all students that they are responsible and accountable for their actions. Personal communications does not include personal or private business enterprises.

Residence Hall Students: Residence hall students are authorized to connect one Personal Computer (PC) or Laptop computer to campus networks. This policy applies in full to all residence hall students who bring computers to campus, except where noted. Equipment specifications are posted in the residence halls, labs, and CTS Help Desk. Students with computers in the residence halls should be extremely cautious with their network activities. Configuring a PC incorrectly could enable other users unwanted access to the PC. Under no circumstance can a residence hall student connect a server of any type, hub, switch, router, gateway, network-scanning device, sniffer, or probe to campus networks. Configuring a PC or laptop to work like a server constitutes a "server."

Residence hall students should not re-configure the network configuration of a PC or Laptop after CTS has set it. Doing so may render the computer unusable on campus networks or unprotected.

Providing shared resources from a computer in a residence hall is not recommended. All copyright laws and policies apply in full. Students who violate copyright laws on campus computer systems and networks will have their network privileges revoked**.**

Faculty and Staff: Full time faculty and staff are authorized access to campus networks, and provided an electronic mail account and disk storage space on the faculty and staff home server. The assigned department facilitates access authority for faculty and staff. Access to the administrative computing system, the web server, and other computer systems may be granted with approval from the system administrator and the assigned department.

The use of university network and computer resources are for university-sanctioned activity and business uses. Electronic mail can be used to communicate with colleagues and professional associates and should be limited to professional communiqué. Limited personal electronic mail and limited personal use of university computers is authorized; however, it should not interfere with official duties or violate university policies or local, state, or federal laws.

Adjunct faculty and part-time staff are authorized the same access as full-time faculty and staff; however, the assigned department is responsible for requesting and terminating access.

Guests: Departments may request access for a guest through Campus Technology Services. Access will be granted based on need for a specific period of time, and the department head or dean will be responsible for the guest's activities.

All Users: Students, faculty, staff, and guests are authorized to access computer systems and campus networks using only their assigned accounts.

The system administrators of departmental and individual computer resources are responsible for the security of information stored on those resources and for keeping those systems free from unauthorized access.

It is imperative that all university departments provide safeguards for confidential and business data. This includes, and is especially applicable to, any transmission of data with a Social Security number**.** Transmission of sensitive data in e-mails and desktop publishing software is not secure.

3. Access to Computers, Computer Systems, and Campus Electronic Networks

There are many personal computers, computer systems, and network access points at OCU. Regardless of the method, location, and ownership, users are only authorized to access systems to which they are granted access by the university.

The university networks may provide access to computer systems, networks, and the Internet at other colleges, universities, businesses, or private organizations. The fact that a user can connect to a computer system or network, on- or off-campus, does not automatically give the user the authority to use it. A user must have proper approval to gain access to any system from or through the OCU networks.

The use of another user's ID or password is strictly forbidden on OCU networks and computer systems.

As a rule, a user should:

- access computer systems only through his or her authorized, assigned user id and password.
- not attempt to access any computer, computer system, or network without explicit authority to do so.
- not assume that, because he or she is able to connect to a computer, computer system, or network, he or she is authorized to use it.
- respect copyright laws. The Internet is not public domain. All material accessed through the Internet is protected by the same laws as if it were not on the Internet. All copyright, trademark, and patent laws apply to material accessed through OCU networks and the Internet. This includes-- but is not limited to--data, music, videos, documents, publications, research, and pictures.
- respect local, state, and federal laws that apply to all users of OCU campus networks and computer systems.

An authorized user should take reasonable care to prevent unauthorized access to the systems to which he or she is given authorized access. In particular, passwords should be carefully chosen and protected. When choosing a password, a user should:

- not use a name or a single word that can be found in a dictionary.
- not allow others to watch the entry of his or her password.
- not write passwords in an obvious place or write them down so they can easily be identified.
- change passwords regularly.

Anyone who thinks a password has been compromised should:

- Contact the system administrator immediately.
- Change the password immediately.

Any attempt to gain unauthorized access to a computer system will be regarded as a serious breach of university policy and may have administrative consequences.

As a rule, Campus Technology Services will not access user accounts and data files. However, to facilitate systems administration, security, or an investigation, CTS may access computer systems and personal accounts without notice.

4. Using, Copying, or Altering Data or Programs of Other People

Computer systems, networks, and the Internet provide access to a wide range of material, data, and information. Everyone is responsible for determining the status of the data and files he or she possesses on campus, accesses on OCU networks, accesses through computer systems, and accesses through the Internet. Under no circumstances should a user assume the material he or she accesses is free from copyright, confidentiality, trademark, and patent laws.

As a rule, a user should:

- not copy, use, redistribute, or alter any data, publications, files, or programs without express, written authority to do so.
- not assume that, because he or she knows another user has data, publications, files, or programs, anyone is allowed to use them.
- seek approval to redesign or reverse engineer any computer programs.
- not use backup copies of software for any reason other than to re-install it after a failure.
- not copy copyrighted material without written permission.

It is against federal law and university policy to create or possess, on university systems or property, files, programs, pictures, documents, and music in violation of copyright law.

The university reserves the right to monitor and access all computer and network systems, to include electronic messages, at any time and without notice to the user for the purpose of monitoring compliance with this policy and state or federal laws.

OCU, rich in tradition and excellence, opposes the overuse of network resources and breech of copyright infringements created by unprotected sharing of copyrighted music, video, and application programs. Web sites engaged in unethical or illegal practices may be blocked from campus access at the discretion of the university President and the President's Cabinet. Users of OCU computer systems, campus networks, and residence hall networks, who possess illegal files (e. g., unlicensed commercial programs, MP3) are subject to disciplinary action and may be turned over to state and federal authorities.

Some software licenses permit the user to keep a second copy for backup purposes. The user should not use this copy for any purpose other than to reinstate the software on the computer to which it is licensed.

Peer-to-Peer File Sharing Programs:

To ensure compliance with state and federal laws, OCU has adopted the position that it is against university policy to use Peer-to-Peer file sharing programs that have the capacity to breech the copyright of digital files; most specifically; music and video. The university will block the use of these programs on the OCU network and monitor network traffic to ensure policy compliance, and will work with state and federal agencies when appropriate.

5. University-Owned Personal Computers

Campus Technology Services will publish and maintain a list of approved software for use on university personal computers. Approved software will be installed as needed, when a valid license exists.

Additional software may be installed on university PCs with the permission of the department head or Campus Technology Services. The department must maintain a copy of the license for the full duration of use.

Any additional software installed on a PC that prevents it from working properly will be removed and prohibited from future installation.

All faculty and staff considering the installation of additional software should consult Campus Technology Service prior to its purchase and installation. Software games, screen savers, and personal utilities will not be supported and should not be installed on university-owned PC's.

6. Administrative Data

During the course of employment or studies at OCU, a user may be provided access to university business or confidential data. All data accessed on university computer systems and networks is for university business only. Under no conditions should students, faculty, or staff breech the confidentiality of university constituents.

Any attempt to gain unauthorized access to administrative data will be regarded as a serious breach of university policy. Anyone needing detailed advice concerning the status of data to which he or she has access should consult the department head or supervisor.

7. Offensive and Unsolicited Material

Material that is likely to be offensive must not be sent or requested to be received over OCU networks or stored in university computer systems. This includes, but is not limited to, pornography, jokes, videos, and cartoons. In addition, one should not send material that is likely to cause a nuisance to other computer users, either within or outside the university. Causing the transmission of offensive, harassing, or nuisance material over university networks is considered a serious breach of policy. “Chain letters” and “mail bombs” are prohibited. If a user asks for material to be sent which he or she finds offensive , there is little retaliation the university can take.

Campus Technology Services does not regularly monitor or control the content of material available over OCU networks. Users must take personal responsibility for the material they access on campus networks and computer systems. The fact that material is available from a source does not mean the material is necessarily suitable for redistribution or free from copyright restrictions. If a campus user passes on inappropriate material sent by another user, the fact that it originally came from another source is not a defense. All users are responsible for the content in any data or e-mail transmission.

8. Disruption of Services

Computer and network users must take all reasonable care to avoid disrupting services for other users. Activities that are likely to place a heavy demand on a system or network should be performed at off-peak times. The responsible computer department reserves the right to suspend or terminate any activity that threatens the integrity of a system or the disruption of service. Deliberate disruption of services is viewed as a negligent act and is subject to disciplinary action.

9. Viruses

Computer viruses are programs that perform deliberate destruction and disruption of computer systems and networks. Computer viruses come from many places and sources. All campus computer users should take care to avoid downloading and installing programs from unreliable sources. Many viruses are transmitted through electronic mail. Users should be skeptical of all e-mail and attachments received.

Anti-virus software is an excellent line of defense. However, it should be properly installed and updated frequently.

10. Internet Programs, Utilities, Services, and Games

There are many services and programs offered over the Internet, some free and some subscribed. These include interactive gaming sites, long distance telephone calling, and video on demand. Generally, these services utilize many network resources. OCU will not provide access to these services unless they are determined to be required for the academic mission of the university. Users may request access to these services from Campus Technology Services.

11. Reporting and Investigating Misuse of Centrally Managed Services

It is in the general interest of all members of the university to prevent the misuse of computer systems, data networks, and voice networks. Users with knowledge of misuse, abuse, or neglect should report the incident to Campus Security or Campus Technology Services. Complaints or reports should be directed to the Help Desk during operating hours or by e-mail to the Help Desk. Please provide as much information as possible about any incident. Campus Technology Services will not invade someone's privacy on anonymous report.

Campus Technology Services continually monitors the performance and load on systems. Any unexpected variations are always investigated immediately. Investigative actions will be taken when valid reports of misuse and abuse are made. Unsubstantiated reports will not be pursued.

Campus Technology Services will occasionally scan network and computer resources. However, electronic mail will not be accessed unless there is evidence of abuse or misuse. Campus Technology Services will access electronic mail accounts only with the permission of the university President, Vice President of Student Services, Vice President of Academic Affairs, or Director of Human Resources. A user can approve the access of his or her own account by Campus Technology Services. Users should not allow other users access to their e-mail account.

Section II: Computer Network Procedures

1. Computer Accounts

Accounts to computer and network services will be provided under the following procedures:

Students: Students will receive network and electronic mail accounts upon enrollment in a class at Oklahoma City University. A registered student can obtain a user id and a password from one of the three open-access computer labs on campus. A student's accounts will be disabled when the student does not enroll in the next academic semester. Accounts can also be disabled or terminated at the request of the Vice President of Student Services.

Staff: Staff will be assigned network and electronic mail accounts by submission of a Systems Update Information Form from Human Resources. This is normally an automatic process. Staff can obtain user ids and passwords from Campus Technology Services. Staff accounts are terminated upon resignation of employment or request of a supervisor or vice president.

Faculty: Faculty will be assigned network and electronic mail accounts by request of their respective deans. Full-time and adjunct faculty are authorized network and e-mail accounts on approval of their respective deans. Accounts are terminated upon resignation of position or request of a dean.

Guests: Vice presidents and deans can request accounts for guests. The vice president or dean is fully responsible for the actions of the guests and is required to notify Campus

Technology when the guest account is no longer needed. Guests are required to follow all the policies and procedures of the campus and are fully responsible for their actions.

Accounts will not be disabled or terminated when an employee changes employment status within the campus. Human Resources will be consulted to validate changes in employment.

Access to a computer account may be revoked for a violation of security provisions, unlawful activity, or violation of university policy.

2. Computer Laboratories

There are many computer labs on campus. Only the three "open access" computer labs located in the Noble Business School, Student Faculty Center, and Dulaney Browne Library basement are open to all students, staff, and faculty. Students must request usage of the other labs on campus from the applicable department.

The PCs located in the residence halls are for residence hall students only.

If the "open access" labs become over-crowded, students performing class work will have priority over users performing personal work, e.g., e-mail, Internet use, personal correspondence.

All persons must accept the marked priority of designated equipment in the computer labs. Examples include, but are not limited to, computers reserved for disabled persons and general reservations.

When the university is officially closed, computer labs will close.

Lab policies and procedures are posted in the labs. Patrons should review the policies before use.

Computer Labs will close at their scheduled time.

All persons must comply with the instructions given by the lab monitor on duty.

3. Electronic Mail

Electronic mail is provided to most university constituents. It has become a common communication utility, with substantial operating expense, and easily can be misused. All constituents are reminded that university e-mail is primarily for university use. Electronic mail can be used to communicate with colleagues and professional associates. Limited personal electronic mail is authorized; however, it should not interfere with official duties or violate university policies or local, state, and federal laws**.**

Faculty and staff will generally access e-mail with the MS Outlook client while on campus. Otherwise, all other users will utilize the Internet web client accessible at <email.okcu.edu>.

E-mail accounts will be created using the procedures outlined above.

Users should periodically delete or move unwanted messages from their Inbox, Sent Items, and Deleted Items folders. Campus Technology Service may, after proper notification, delete electronic mail located in mail holding areas after a fixed period of time in order to conserve computer storage space.

Student e-mail will be deleted 2 weeks after the end of the spring semester. Authorized student accounts will remain active after the deletion of the electronic mail. Students should make plans to back up e-mail they want to save.

4. Data Backup

Campus Technology Services highly encourages all computer users to back up working data files on PCs, laptops, and servers. Backing up this data is the responsibility of the user.

Campus Technology Services are only responsible for backing up data on the main computer systems and servers. Backups of network servers and the e-mail system will be maintained for a period of three months.

5. General

University departments may request exceptions to these policies. The university President or his or her designee must authorize these exceptions.

University harassment policies apply equally to electronic media such as telephone, computer system, and computer network communications.

All persons who have any questions or doubts about using a computer account, computer system, or computer network should contact Campus Technology Service prior to using the account.

Federal, state, and local laws apply to computer system and computer network use. Particular attention is called to federal export regulations when using computer networks. For example, there are regulations that make it illegal to export data encryption software.

Section III: Guidelines on Internet Use and Web Site Hosting

1. Internet Usage

OCU provides all campus constituents access to the Internet. It provides a wide array of access to information, news, education, shopping, and sports to name a few. It also provides access to illegal activities such as copyright infringement, pornography, and gambling. Users of the OCU networks and the Internet should familiarize themselves with local, state, and federal laws regarding legal and illegal Internet activity.

There will be no protection from the university for illegal Internet activity. The university will work with all authorities to ensure safe and lawful Internet usage. University administrators will act upon any misuse by policy or by law. Substantiated misuse may constitute administrative action.

2. Web Sites

OCU maintains a Web Site Policy that should be read by all constituents developing web pages on university official and student web servers.

Students and faculty are provided 3 Megabytes of disk space for a personal web page on the OCU Student web server. Access to this service can be obtained in the computer labs. Students are authorized to create a personal web page on the student web server. The Microsoft Front Page software is loaded on the "open access" lab PCs and is available for checkout in the libraries. Students can only write to the Student Web Server from on campus.

Although the Student Web Server is a "personal" web page server, students are advised that this is a university resource. All university policies and procedures, and state and federal laws apply. Web sites should be tasteful and free from conflict with university policies regarding copyright, pornography, harassment, sexist or racist material, offensive language, and defamatory material.

Students posting personal web pages should familiarize themselves with the relevant regulations and our guidelines for legal and ethical use.

All web developers should be very careful making links to other sites. Do not assume that all material on the Internet is acceptable for use at OCU. Anyone having doubts as to the suitability of a link can e-mail the web master at <webmaster@okcu.edu>.

Do not include in personal web pages instructions, policies, or procedures that might contribute to the improper use of OCU facilities.

Personal pages must not give the impression that the university sanctions the content.
Student must include this statement on each page of a Personal Web Site:

The views and opinions expressed on this web site are those of [student name] and not necessarily those of Oklahoma City University.

Always provide in the html the name and contact details of the person responsible for a page.

Always provide the date on which the page was last updated.

Section IV: Prohibited Conduct

The following is prohibited conduct for any individual using OCU managed computers or networks:

1. Using any computer system or computer network for illegal purposes.

2. Using a computer system or computer network in violation of university standards of academic ethics.

3. Disrupting university activities, which encompasses obstruction or disruption of teaching, research, administration, disciplinary procedures, sports, and public service functions.

4. Removing university computer and network equipment without the authorization of the President or a vice president, dean or department head. All equipment should be signed out with an explanation of destination and estimated time of return.

5. Possessing, storing, or transmitting computer software or data without authorization.

6. Gaining access to, attempting to gain access to, or causing access to be gained to any PC, computer system, or network without authorization.

7. Altering, deleting, or destroying data, information, or programmatic instructions contained on or in a computer or network system without authorization of the owner.

8. Publishing user account ids and passwords for computer and network systems.

9. Publishing university telephone numbers and e-mail addresses without authorization of the President or his or her designee.

10. Using university computers or telecommunications device to commit any form of harassment.

11. Attempting to circumvent university computer system or computer network security systems, or using university computer systems or computer networks in attempting to circumvent security systems elsewhere.

12. Failing to follow state and federal laws when reaching international locations by way of university computer networks.

13. Failing to respect all copyrights or proprietary rights.

14. Connecting, disconnecting, tampering with, or making changes to physical components of computer and network systems without authorization.

15. Attempting to access administrative data on any university computer system or computer network without authorization.

16. Using a computer system or computer network to eavesdrop or to collect passwords or authentication information.

17. Forging electronic mail or other messages. No person may send a message in such a way that makes it appear to be sent by another person.

18. Using a university computer account owned by someone else. A user is not authorized to give permission to someone else to use his or her account.

Section V: Consequences of Misuse of Computing Privileges

All users of university computer systems and networks should respect the rights of others and are obligated to safeguard university resources. Abuse and illegal activity should be reported to Campus Security or Campus Technology Services.

Campus Technology Services or Campus Security will investigate all reports of abuse and illegal activity. All university constituents are obligated to cooperate with investigations of computer and network abuse and illegal activity.

Intentional abuse, breeches of security, or illegal activity may result in loss of computer and network privileges and may be in violation of OCU employment policies. OCU may consult and report illegal activity to local and federal officials.

Violations of this policy may also subject the user to appropriate disciplinary action in accordance with applicable OCU employment, faculty/staff and student policies. Such action may include the termination of employment, or a student’s expulsion from the university.