Established 1909

OPSU POLICIES AND PROCEDURES

TITLE: Acceptable Computer Use Policy

APPROVED BY: Draft

DATE: 10-14-2005

A. Introduction
Oklahoma Panhandle State University (OPSU) attempts to create an environment where university information technologies meet the needs of university programs in research and instruction.

As an institution of higher learning, OPSU encourages, supports, and protects freedom of expression and an open environment to pursue scholarly inquiry and to share information. Access to networked computer information in general and to the Internet, in particular, supports the academic community by providing a link to electronic information in a variety of formats and covering all academic disciplines. Consistent with other University policies, this policy is intended to respect the rights and obligations of academic freedom, while protecting the rights of others. The computing and network facilities of the University are limited and should be used wisely and carefully with consideration for the needs of others. Usage of these facilities is a privilege rather than a right. As with any resource, it is possible to misuse computing resources and facilities and to abuse access to the Internet. The following statements address, in general terms, the University's philosophy about computing use.

B. Scope
This policy is applicable to all individuals using University owned or controlled computer and computer communication facilities or equipment. It is applicable to all University information resources whether individually controlled or shared, stand alone or networked. It applies to all computer and computer communication facilities owned, leased, operated, or contracted by the University. In addition, a user must be specifically authorized to use a particular computing or network resource by the campus unit responsible for operating the resource.

Individual units within the University may define "conditions of use" for information resources under their control. These statements must be consistent with this overall Policy but may provide additional detail, guidelines and/or restrictions. Such policies may not relax or subtract from, this policy. Where such "conditions of use" exist, enforcement mechanisms defined therein shall apply. Units must also publicize both the regulations they establish and their policies concerning the authorized and appropriate use of the equipment for which they are responsible. In such cases, the unit administrator shall provide the appropriate Vice President and the campus IT Director with a copy of such supplementary policies prior to implementation thereof. Where use of external networks is involved, policies governing such use also are applicable and must be adhered to.

C. Authorized Users
An authorized user is any person who has been granted the privilege by the University to access its computing and network systems and whose usage complies with university policy. Authority to use a particular University computing or network resource should come from the campus unit responsible for operating the resource.

D. Authorized Use
Use of University computers must comply with Federal and State laws and University policies. Facilities and accounts are to be used for the activities for which they are assigned.

Users are held responsible for their **own** computer accounts and the usage thereof.

Computing facilities, services, and networks may not be used in connection with compensated outside work for the

benefit of organizations unrelated to the University except in connection with scholarly pursuits (such as faculty publishing activities). State law generally prohibits the use of University computing and network facilities for personal gain or profit, and use of computing resources for unauthorized commercial purposes, unauthorized personal gain, or any illegal activities is prohibited.

E. Privacy
Following OPSU Policies and Procedures, Oklahoma laws and applicable federal laws, OPSU strives to protect personal privacy and the confidentiality of information. Information will be handled with the strictest of security and confidentiality standards.
(Buckley Amendment – Family Rights and Privacy Act, Open Records Act, Federal Electronic Communication and Privacy Act of 1986, Federal Computer Intrusion Laws)

F. User Responsibilities
Ethics and etiquette are required to successfully participate in the OPSU community and are extended to the computing environment. Individuals who share computing resources at OPSU and who also use those resources to access the worldwide network are responsible for knowing and following the Appropriate Computer Use Policy. It is the responsibility of the user to access and use data in accordance with the university's policy and applicable state and federal laws.

Access to the information resource infrastructure both within and beyond the University campus, sharing of information, and security of the intellectual products of the community all require that each and every user accept responsibility to protect the rights of the community. Access to the networks and to the information technology resources at OPSU is a privilege granted to University students, faculty, staff, and affiliates who have been granted special permission to use such facilities. Access to University information resources must take into account the following factors: relevant laws and contractual obligations, the requestor's need to know, the information's sensitivity, and the risk of damage to or loss by the University.

Anyone who accesses, uses, destroys, alters, or damages University information resources, properties or facilities without authorization, may be guilty of violating state or federal law, infringing upon the privacy of others, injuring or misappropriating the work produced and records maintained by others, and/or threatening the integrity of information kept within these systems. Such conduct is unethical and unacceptable and will subject violators of this Policy to disciplinary action by the University, including possible termination from employment, expulsion as a student, and/or loss of computing systems privileges.

Individual users certify understanding and agreement to adhere to OPSU's policies by signing on to OPSU systems. Specifically, a user acknowledges an understanding of and agreement to adhere to the following:

- Users are personally responsible for all activities on their User ID or computer system and may be subjected to disciplinary action and/or loss of privileges for misuse of computers or computing systems under their control, even if not personally engaged in by the person controlling the computer or system.
- Updates to the system and changes in system data are to be made in a manner that is consistent with the University policies and procedures that govern the particular action to be changed.
- Computing resources are to be used only for legitimate University business.
- It is against the University's policy to use the University's records including, but not limited to, confidential information for personal interest or advantage.
- Proper password security is to be maintained by not revealing passwords to others.
- Security is to be maintained by **not** providing unauthorized users access to or use of the University's information systems.
- Proper physical security is to be maintained by not leaving a workstation/terminal unattended while logged in to the University's systems.
- The privacy and confidentiality of all accessible data is to be maintained and it is understood that unauthorized disclosure of personal /confidential information is an invasion of privacy and may result in disciplinary, civil and/or criminal actions against an individual.
- Suspected security violations will be reported to the campus IT Director.
- Under existing law, any person who maliciously accesses, alters, deletes, damages or destroys any computer system, network, computer program or data may be charged with a felony.
  The University also requires that members of its community act in accordance with these responsibilities,
- **Act in accordance with the Family Educational and Privacy Rights Act (Buckley Amendment),**
- respect copyrights and licenses,
- respect the integrity of computer-based information resources,

- refrain from seeking to gain unauthorized access,
- respect the privacy of other computer users, and comply with this Policy, the University's Student or Faculty Handbook, as appropriate, OPSU Policies and Procedures, relevant laws and contractual obligations, and the highest standard of ethics. OPSU accommodates and does not interfere with standard technical measures used by copyright holders to identify and protect their rights (for further information see the U.S. Copyright Office at www.loc.gov/copyright).

Network User Responsibilities

The owners or primary users of computers connected to the OPSU network are responsible for the following:

1. Abiding by OPSU's Appropriate Computer Use Policy
Users should efficiently use network resources and follow OPSU's Appropriate Computer Use Policy and OPSU's Network Security Policy. Users are personally responsible for all activities on their User ID or computer system and may be subjected to disciplinary action and/or loss of privileges for misuse of computers or computing systems under their control, even if not personally engaged in by the person controlling the computer or system.
2. Reporting Problems
Users should promptly report network problems to either the local network administrator or to the campus IT Director, and cooperate with support staff in correcting malfunctions.
3. Taking Proper Security Precautions
Users should select secure passwords and change them regularly. Security-minded network access techniques should be used whenever practical.
4. Keeping the Operating System Secure
Users should make sure their computer's operating system is kept up-to-date with current security patches. This may be accomplished by the owner, local support staff, or central staff.

- **Network Use Special Notifications**

  The University's computing and network systems are a university owned resource and business tool only to be used by authorized individuals for business and academic purposes. Users should never distribute mailing lists owned by the University. The University owns everything stored in its systems unless it has agreed otherwise. The University has the right of access to the contents of stored computing information at any time for any purpose for which it has a legitimate "need to know." The University will make reasonable efforts to maintain the confidentiality of computing information storage contents and to safeguard the contents from loss, but is not liable for the inadvertent or unavoidable loss or disclosure of the contents.

  Devices not approved for use on OPSU's Data Communication Network may be disabled to ensure the stability and availability of the network.

The University reserves the right to limit, restrict, or extend computing privileges and access to its information resources. Usage is a privilege, not a right.

Users are held responsible for their own computer accounts and the usage thereof. Users will be subject to disciplinary action, including termination and/or loss of privileges for misuse of computers or computing systems under their control.

Units and individuals may, with the permission of the appropriate Vice President and in consonance with applicable University policies and guidelines, configure computing systems to provide information retrieval services to the public at large. However, in so doing, particular attention must be paid to University policies regarding authorized use (must be consistent with the mission of the University), ownership of intellectual works, responsible use of resources, use of copyrighted information and materials, use of licensed software, and individual and unit responsibilities. Contact information for the system administrators of these systems must be reported to the campus IT Director.

G. Special Notifications
The University cannot protect individuals against the existence or receipt of material that may be offensive to them. As such, those who make use of electronic communications are warned that they may come across or be the recipients of materials they find offensive. Those who use e-mail and/or make information about them available on the Internet should be forewarned that the University cannot protect them from invasions of privacy and other possible dangers that could result from the individual's distribution of personal information. Personal use of any University information

system to deliberately access, download, print, store, forward, transmit or distribute obscene material is prohibited.

The University's computing and network systems are a university owned resource and business tool only to be used by authorized individuals for business and academic purposes. Users should never distribute mailing lists owned by the University. The University owns everything stored in its systems unless it has agreed otherwise. The University has the right of access to the contents of stored computing information at any time for any purpose for which it has a legitimate "need to know." The University will make reasonable efforts to maintain the confidentiality of computing information storage contents and to safeguard the contents from loss, but is not liable for the inadvertent or unavoidable loss or disclosure of the contents.

The OPSU Data Communications Network is a mission critical strategic University resource. In order to protect the Data Communications Network, devices that are considered end nodes, other than computers, servers, printers, and workstations must not be plugged into any network port, unless special arrangements are made with the campus IT Director. This includes but is not limited to hubs, switches, repeaters, routers, network modems and wireless access points whose installation has not been coordinated and registered with campus IT Director. These devices may be incorrectly configured or incompatible with the OPSU Network causing outages and reliability problems to all or part of the network. Devices not approved for use on OPSU's Data Communication Network may be disabled to ensure the stability and availability of the network.

OPSU strives to provide high availability and stable network resources relevant to the OPSU community's needs. Colleges or Departments needing additional network resources should contact the campus IT Director.

H. Access
Unauthorized access to information systems is prohibited. No one should use the ID or password of another; nor should anyone provide his or her ID or password to another. A password should never be shared, not even with computer support personnel. Users are personally responsible for all activities on their User ID or computer system, including security of their own passwords and may be subjected to disciplinary action and/or loss of privileges for misuse of computers or computing systems under their control, even if not personally engaged in by the person controlling the computer or system.

I. Ownership and Rights of Access to Software and Data
OPSU has software and data that have been acquired through a variety of sources. Some software and data, though available for use by all users of OPSU's systems, remain the property of the supplier and the dissemination of the software or data (in any form) is strictly prohibited. This also applies to software made available by non-IT University personnel. This software is not to be distributed, unless authorized by the person or department that initially secured the software or data. No software or data should be distributed, reproduced or used without ensuring that proper licensing and/or authorization has been obtained.

J. Conduct Expectations and Prohibited Actions
OPSU provides computing resources and worldwide network access to members of the OPSU community for legitimate academic and administrative pursuits to communicate, access knowledge, and retrieve and disseminate information. All members of the OPSU community (faculty, staff, students, and authorized guests) sharing these resources also share the rights and responsibilities for their use.

Examples of misuse include, but are not limited to:

- Knowingly running or installing on any computer system or network, or giving to another user, a program intended solely for the purpose of damaging or placing excessive load on a computer system or network. This includes, but is not limited to, computer viruses, Trojan horses, worms, bots, flash programs or password cracking programs.
- Attempting to circumvent data protection schemes or uncover security loopholes without prior written consent of the system administrator. This includes creating and/or running programs that are designed to identify security loopholes and/or intentionally decrypt secure data.
- Using computers or electronic mail to act abusively toward others or to create a hostile environment, violent reaction, such as stalking, threats of violence, or other hostile or intimidating "fighting words."
- Posting on electronic bulletin boards or web pages materials that violate the University's codes of conduct (faculty, student). This includes posting information that is slanderous or defamatory in nature or displaying graphically disturbing or sexually harassing images or text in a public computer facility or location that are in view of other individuals.
- Attempting to monitor or tamper with another user's electronic communications or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner.

- Using campus networks to gain, or attempt to gain, unauthorized access to any computer system.
- Using a computer account or obtaining a password without appropriate authorization.
- Masking the identity of an account or machine. This includes sending email that appears to come from someone else.
- Performing an act without authorization that will interfere with the normal operation of computers, terminals, peripherals, networks, or will interfere with others' ability to make use of the resources.
- Using an account for any activity that is not approved through policy and procedure, such as, such as consulting services, typing services, developing software for sale, advertising products, and/or other commercial enterprises for personal financial gain.

K. Systems Security Officer
The university's campus IT Director or the person designated by the President of OPSU, shall be the primary contact to work in conjunction with appropriate university officials for the interpretation, enforcement and monitoring of this policy and the resolution of problems concerning it. Any issues concerning law shall be referred to OPSU Legal Counsel for advice and action as applicable.

In situations that are an immediate threat to the security or operation of a computer or network, the campus IT Director may require immediate intervention of access privileges and affected user files or messages. In such an emergency, the campus IT Director will notify, as soon as possible, the appropriate university administrators and users affected by the situation.

L. Consequences of Misuse
Misuse of computing, networking, or information is unacceptable, and users will be held accountable for their conduct. Serious infractions can result in temporary or permanent loss of computing and/or network privileges and/or Federal or State legal prosecution. Appropriate corrective action or discipline may be taken in conformance with applicable personnel policies and student policies. Some computer abuses are a crime, (such as illegal reproduction of software protected by U. S. copyright law) and penalties can include a fine and/or imprisonment.

Abuse of computing privileges is subject to disciplinary action, including termination of employment. If system administrators have strong evidence of misuse of computing resources, and if that evidence points to the computing activities or the computer files of an individual, they have the obligation to pursue any or all of the following steps to protect the user community:

- Notify the campus IT Director.
- Notify appropriate departmental administrators
- Will notify the user's instructor, department or division chair, or supervisor of the investigation, when appropriate.
- May suspend or restrict the user's computing privileges during the investigation.
- May inspect the user's files, diskettes, tapes, and/or other computer-accessible storage media.
- Will refer issues, when appropriate, to the appropriate University department for possible disciplinary action, i.e., this may include but not be limited to the Office of the Vice President of Academic Affairs, the Office of the Vice President for Fiscal Affairs, the unit administrator for staff, and the Dean of the School for faculty.

Users, when requested, are expected to fully cooperate with system administrators or the campus IT Director in any investigations of system abuse. Failure to cooperate may be grounds for cancellation of access privileges or disciplinary action, including dismissal.

When individual privileges to access University computing resources have been suspended, a user may request that the Vice President of Academic Affairs, or his/her designee, review the suspension. The Vice President of Academic Affairs, or designee, in his/her discretion, may reinstate privileges, alter any restrictions that have been imposed, or refuse to interfere with the administrative action taken to that time. Further appeals may be filed with the Office of Student Conduct, the University Personnel Office, or the Chair of the Faculty Senate, as appropriate.

Failure to comply with these policies, rules and regulations may result in disciplinary action, up to and including dismissal. Any violation of local, state or federal laws may carry the additional consequence of prosecution under the law, where judicial action may result in specific fines or imprisonment, or both; plus the costs of litigation or the payment of damages or both; or all.

M. Notification
References to this policy may be in the OPSU Catalog, the Student Handbook, the OPSU Staff Handbook, the OPSU web site and the OPSU Faculty Handbook.

N. Application and Enforcement Each University department shall be responsible for enforcing this Policy in a manner best suited to its own organization. It is expected that enforcement will require cooperation between such departments as computer systems administration, personnel, affirmative action, academic affairs and student affairs.

References

OPSU Administrative Policies & Procedures
-Buckley Amendment – Family Rights and Privacy Act
-Digital Millennium Copyright Act
-Federal Computer Intrusion Laws
-Federal Electronic Communication and Privacy Act of 1986