OKLAHOMA STATE UNIVERSITY INSTITUTE OF TECHNOLOGY
POLICY & PROCEDURES LETTER

Appropriate Computer Use	**6-001** **INFORMATION TECHNOLOGIES** **July 2009**

POLICY

Scope and Applicability

1.01 As an institution of higher learning, Oklahoma State University System 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. 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.

1.02 This policy is applicable to all individuals using University owned or controlled computer and computer communication facilities or equipment, whether such persons are students, staff, faculty, or authorized third-party users of University computing information resources. 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. This includes, but is not limited to, word processing equipment, personal computers, workstations, mainframes, minicomputers, and associated peripherals and software, and electronic mail accounts, regardless of whether used for administration, research, teaching, or other purposes. A user must be specifically authorized to use a particular computing or network resource by the campus unit responsible for operating the resource.

1.03 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. These individual units are responsible for publicizing 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 Executive Vice President 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.

User Responsibilities and Expectations

2.01 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 Oklahoma State University Institute of Technology is a privilege granted to University students, faculty, staff, and third parties 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.

2.02. 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 separation from employment, suspension as a student, and/or loss of computing systems privileges.

2.03 The University requires members of its community act in accordance with these responsibilities, this Policy, the University's Student or Employee Handbook, as appropriate, OSU System Policies and Procedures, relevant laws and contractual obligations, and the highest standard of ethics. The policies as stated in this Policy are intended to ensure that users of University information resources shall:

- respect software 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.

2.04 The University reserves the rights to limit, restrict, or extend computing privileges and access to its information resources. Data owners—whether departments, units, faculty, students, or staff—may allow individuals other than University faculty, staff, and students access to information for which they are responsible, so long as such access does not violate any license or contractual agreement, University policy, or any federal, state, county, or local law or ordinance. However, 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.

2.05 Units and individuals may, with the permission of the appropriate University officials 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.

Authorized User Purposes

3.01 Use of University computers must comply with Federal and State law and University policies. University computing facilities and accounts are to be used for the University-related activities for which they are assigned. When users cease to be members of the academic community (such as by graduating or ceasing employment) or when persons are assigned to a new position and/or responsibilities within the University, the access authorization of such person will be reviewed and may be altered. Users whose relationships with the University change may not use computers and computing resources, facilities, accounts, access codes, privileges, or information for which they are not authorized in their new relation to the University.

3.02 Users may use only their own computer accounts. The negligence or naivete of another user in revealing an account name or password is not considered authorized use. Convenience of file or printer sharing is not sufficient reason for sharing a computer account. Users are personally responsible for all use of their computer account(s).

3.03 Appropriate use of computing and networking resources includes instruction, independent study, authorized research, independent research, communications, and official work of the offices, units, recognized student and campus organizations, and agencies of the University. 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), or in a purely incidental way. 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.

Special User Notifications

4.01 The University makes available both internal and external computing facilities consisting of hardware and software. The University accepts no responsibility for any damage to or loss of data arising directly or indirectly from the use of these facilities or for any consequential loss or damage. The University makes no warranty, express or implied, regarding the computing services offered, or their fitness for any particular purpose.

4.02 Liability for any loss or damage shall be limited to a credit for fees and charges paid to the University for use of the computing facilities which resulted in the loss or damage.

4.03 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 themselves 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.

4.04 An individual using University computing resources or facilities must do so in the knowledge that he/she is using University resources in support of his/her work. The University owns everything stored in its facilities 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.

4.05 Any individual using University computing resources and facilities must realize that all mainframe computer systems maintain audit trail logs or file logs within the mainframe computer. Such information as the user identification, date and time of the session, the software used, the files used, the computer time, and storage used, the user account, and other run-related information is normally available for diagnostic, accounting, and load analysis purposes. Under certain circumstances, this information is reviewed by system administrators, either at the request of an institutional unit, or in situations where it is necessary to determine what has occurred to cause a particular system problem at a particular time. For example, analysis of audit files may indicate why a particular data file is being erased, when it was erased, and what user identification has erased it.

4.06 CIS employees and system administrators do not routinely look at individual data files. However, the University reserves the right to view or scan any file or software stored on the computer or passing through the network, and will do so periodically to verify that software and hardware are working correctly, to look for particular kinds of data or software (such as computer viruses), or to audit the use of University resources. Violation of policy that comes to the attention of University officials during these and other activities will be acted upon. User data on the mainframe will be periodically copied to backup tapes. The University cannot guarantee confidentiality of stored data. Users should be aware that use of one of the data networks, such as the Internet, and electronic mail and messages, will not necessarily remain confidential from third parties outside the University in transit or on the destination computer system, as those data networks are configured to permit fairly easy access to transmissions.

Conduct Expectations and Prohibited Actions

5.01 The well being of all computer users depends on the availability and integrity of the system. Any defects discovered in the system accounting or system security are to be reported to the appropriate system administrators so that steps can be taken to investigate and solve the problem. The cooperation of all users is needed to ensure prompt action. The integrity of most systems is maintained by password protection of accounts. A computer user who has been authorized to use such a protected account may be subject to both criminal and civil liability, as well as University discipline, if the user discloses a password or otherwise makes the account available to others without the permission of the system administrator.

5.02 Restrictions on computer security and self-replicating code are to be interpreted in a manner that protects university and individual computing environments, but does not unduly restrict or limit legitimate academic pursuits.

5.03 The following examples of acts or omissions, though not covering every situation, specify some of the responsibilities that accompany computer use at Oklahoma State University, and outline acts or omissions that are considered unethical and unacceptable, and may result in immediate revocation of privileges to use the University's computing resources and/or just cause for taking disciplinary action up to and including separation, suspension, and/or legal action:

A. Violating any software license agreement or copyright, including copying or redistributing copyrighted computer software, data, or reports without proper, recorded authorization. Software protected by copyright shall not be copied except as specifically stipulated by the owner of the copyright. Protected software is not to be copied into, from, or by any University facility or system, except by license. The number and distribution of copies must be handled in such a way that the number of simultaneous users in a unit does not exceed the number of original copies purchased by that unit, unless otherwise stipulated in the purchase contract.

B. Interfering with the intended use of the information resources or without authorization, destroying, altering, dismantling, disfiguring, preventing rightful access to or otherwise interfering with the integrity of computer-based information and/or information resources.

C. Modifying or removing computer equipment, software, or peripherals without proper authorization.

D. Encroaching on others' use of the University's computers. This includes but is not limited to: the sending of chain-letters or excessive messages, either locally or off-campus; printing excess copies of documents, files, data, or programs; running grossly inefficient programs when efficient alternatives are known to be available; unauthorized modification of system facilities, operating systems, or disk partitions; attempting to crash or tie up a University computer; damaging or vandalizing University computing facilities, equipment, software, or computer files.

E. Developing or using programs which harass other computer users or which access private or restricted portions of the system and/or damage the software or hardware components of the system. Computer users shall use great care to ensure that they do not use programs or utilities which interfere with other computer users or which modify normally protected or restricted portions of the system or user accounts. Computer users shall not use network links for any use other than permitted in network guidelines (e.g., ONENET, Internet, NSFNet, BITNET). The use of any unauthorized or destructive program may result in legal civil action for damages or other punitive action by any injured party, including the university, as well as criminal action.

F. Using University computing resources for commercial purposes or non-University-related activities without written authorization from the University. In these cases, the University will require restitution payment of appropriate fees. This Policy applies equally to all University-owned or University-leased computers.

G. Using University computing resources to generate or access obscene material as defined by Oklahoma or federal law and acceptable community standards or creating a hostile work and/or educational environment.

H. Seeking to gain or gaining unauthorized access to information resources or enabling unauthorized access.

I. Accessing computers, computer software, computer data or information, or networks without proper authorization, or intentionally allowing others to do so, regardless of whether the computer, software, data, information, or network in question is owned by the University. For example, abuse of the networks to which the University belongs or the computers at other sites connected to those networks will be treated as an abuse of Oklahoma State University computing privileges.

J. Without authorization invading the privacy of individuals or entities that are creators, authors, users, or subjects of the information resources.

K. Using University electronic communication facilities to send fraudulent, harassing, obscene, threatening, or other unlawful messages is prohibited. Users shall respect the purpose and charters of computer mailing lists (including local or network news groups and bulletin-boards). It is the responsibility of any user of an electronic mailing list to determine the purpose of the list before sending messages to the list or receiving messages from the list. Persons subscribing to an electronic mailing list will be viewed as having solicited any material delivered by the list as long as that material is consistent with the purpose of the list. Persons sending to a mailing list any materials which are not consistent with the purpose of the mailing list will be viewed as having sent unsolicited material to the mailing list.

L. Transmitting commercial or personal advertisements, solicitations, promotions, or programs intended to harass other computer users or access private or restricted computer or network resources. Some public bulletin boards may be designated for selling items, etc., and must be used appropriately, according to the stated purpose of the list(s). Vendors may send product information and technical material to specific mailing lists, with the permission of the manager of the mailing list.

M. Seeking to provide information on, obtain copies of, or modify data files, programs, or passwords belonging to other users without the permission of those other users; Using programs or devices to intercept or decode passwords or similar access control information.

N. Attempting to circumvent mechanisms intended to protect private information from unauthorized examination by others in order to gain unauthorized access to the system or to private information; Configuring or running software so as to allow unauthorized use.

O. Using University computers or computing systems in any manner which violates Federal, state, or local laws, or University policies.

P. Using University computing facilities or accounts for other than the University-related activities for which they were assigned and intended.

Q. Using computers or the University computing resources to engage in political campaigning or commercial advertisement.

System Administrator Responsibilities

6.01 The Board of Regents for Oklahoma State University and the Agricultural and Mechanical Colleges are the legal owners of all University "owned" or controlled computers and networks. The contents of all storage media owned or stored on University computing facilities are the property of Oklahoma State University Institute of Technology unless a written contract signed by the suitable contracting authority exists to the contrary. Day-to-day control of any particular system resides with the head of a specific subdivision of the University structure, such as a Dean, Director, unit leader, or principal investigator.

6.02 Management of the data which is contained within the various data systems of the University must be administered in a fashion consistent with the mission and efficient operations of the University, applicable state or federal laws, and potentially applicable privacy considerations.

6.03 The University official in charge of a particular unit or system may designate another person or persons to manage the system. This person (or persons), or the owner in the absence of such a designation, is the "system administrator". The system administrator's use of the University's computing resources is governed by the same guidelines that apply to any other user. However, the system administrator has additional responsibilities and authorities with respect to the system under his/her control and its users.

6.04 The system administrator has certain responsibilities to the University as a whole for the system(s) under his/her control, regardless of the policies of his/her unit, and the owner has the ultimate responsibility to see that these are carried out by the system administrator. These responsibilities are:

A. To take reasonable precautions against theft of, or damage to, the system components.

B. To faithfully execute all hardware and software licensing agreements applicable to the system.

C. To treat information about, and information stored by, the system's users as confidential (as conditioned in this policy) and to take reasonable precautions to ensure the security of a system or network and the information contained therein.

D. To share information about specific policies and procedures that govern access to and use of the system and services provided to the users or explicitly not provided. This information should describe the data backup services, if any, offered to the users. A written document given to users or messages posted on the computer system itself shall be considered adequate notice.

E. To cooperate with the system administrators of other computer systems or networks, whether within or without Oklahoma State University Institute of Technology, to find and correct problems caused on another system by the use of the system under his/her control.

6.05 The system administrator is authorized to take all reasonable steps and actions to implement and enforce the usage and service policies of the system and to provide for security of the system. System administrators operating computers and networks may routinely monitor and log usage data, such as network session connection times and end-points, CPU and disk utilization for each user, security audit trails, network loading, etc. These units may review this data for evidence of violation of law or policy and for other lawful purposes. System administrators may access computer user' files at any time for maintenance purposes. System administrators may access other files for the maintenance of networks and computer and storage systems, such as to create backup copies of media.

6.06 When system response, integrity, or security is threatened, a system administrator is authorized to access all files and information necessary to find and correct the problem or otherwise resolve the situation.

6.07 If an occasion arises when a University officer or supervisor believes that access to an individual's data is required for the conduct of University business (unrelated to the need to investigate possible wrongdoing), the individual is not available, and a system administrator is required to access the individual's account, the following procedure shall be followed:

A. The University official or supervisor shall secure permission to access the data from the Executive Vice President or designee of such officer.

B. An appropriate form with the signature of the Executive Vice President shall be presented to the system administrator allowing the system administrator to proceed to access the data.

C. The individual whose e-mail account has been accessed will be notified as soon as possible by copy of the above referenced form. Where necessary to ensure the integrity of an investigation into the use of University computing resources, such notice, with the approval of the Executive Vice President, may be delayed until such time as such investigation would no longer be compromised.

6.08 System administrators are required to report suspected unlawful or improper activities to the proper University authorities. Computer users, when requested, have an affirmative duty to cooperate with system administrators in investigations of system abuse. Users are encouraged to report suspected illegal activity or abuse, especially if related to any damage to or problems with their files.

6.09 If an occasion arises when a University officer or supervisor believes that a user is violating state or federal law, or University policy, and that access to an individual's data is required in order to conduct an internal investigation into such possibility, system administrators may monitor all the activities of and inspect the files of such specific user(s) on their computers and networks. In such cases, and a system administrator is required to access the individual's data, steps (1) and (2) set forth above in Section 3.01(F) shall be followed and the Office of Legal Counsel shall be contacted and informed of the matter.

Consequences of Misuse of Computing Privileges

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

7.02 Abuse of computing privileges is subject to disciplinary action. 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:

A. Notify the user's unit leader or supervisor of the investigation.

B. Suspend or restrict the user's computing privileges during the investigation.

C. Inspect the user's files, diskettes, tapes, and/or other computer-accessible storage media. System administrators must be certain that the trail of evidence clearly leads to the user's computing activities or computing files before inspecting the user's files.

D. Refer the matter for possible disciplinary action to the appropriate University unit

7.03 Individuals whose privileges to access University computing resources have been suspended may request that the Executive Vice President, or his/her designee, review the suspension. The Executive Vice President, 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. There is no right to a hearing or appearance regarding such issues and the decision made by the Executive Vice President or designee is final.

Approved: October 2004
Revised: July 2009