Oklahoma State University Policy and Procedures

APPROPRIATE USE POLICY	3-0601 ADMINISTRATION & FINANCE Information Technology May 2017

PURPOSE

1.01 As an institution of higher learning, Oklahoma State University encourages, supports, and protects freedom of expression, the free exchange of ideas, and an open environment that facilitates the pursuit of scholarly inquiry. The purpose of this policy is to outline, in general terms, the University's philosophy about acceptable use of information technology resources, with the overall objective of remaining consistent with other OSU A&M policies, and respecting the rights and obligations of academic freedom while protecting the rights of others.

1.02 As a public University, the resources of Oklahoma State University, discussed in this policy, are intended for use by users with no expectation of privacy. In this context, this policy addresses this intent and responsibility of the University to the public.

SCOPE

2.01 This policy applies to all University owned or controlled information technology resources whether individually controlled or shared, stand alone or networked.

2.02 This policy applies to the users of University information technology resources, whether such persons are students, staff, faculty, or authorized third-party users.

2.03 This policy applies to all information technology resource facilities owned, leased, operated, or contracted by the University

2.04 This Policy applies equally to all University-owned or University-leased information technology resources.

DEFINITIONS

3.01 A user is a person, whether authorized or not, who makes use of University information technology resources from any location.

3.02 Information technology resources – Technology and/or computer resources including, but not limited to, personal computers, workstations, mainframes, mobile devices (laptops, tablets, smart phones, etc.), printing equipment, and all associated peripherals and software, and electronic mail accounts, regardless of whether the resource is used for administration, research, teaching, or other purposes.

POLICY

4.01 User Responsibility and Expectations

Within the following sections, examples of acts or omissions, though not covering every situation, are included to specify some of the responsibilities that accompany computer use at Oklahoma State University, and to outline acts or omissions that are considered unethical and unacceptable, and which 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 discharge, dismissal, expulsion, and/or legal action, which may include referral for criminal investigation and/or prosecution.

4.02 Use Purposes

A. Appropriate use of OSU's computing and networking resources includes purposes such as instruction, independent study, authorized research, independent research, communications and official work of the offices, units, recognized student and campus organizations of Oklahoma State University. University computing facilities, systems, accounts and network resources are to be used for University-related activities for which they are assigned. At all times, use of the University's information technology resources must comply with federal and state law, and University policies.

B. University information technology resources are not intended to be used for generating or accessing obscene material as defined by Oklahoma or federal law and acceptable community standards or for creating a hostile work and/or educational environment.

C. Incidental personal use of University information technology resources is permitted, but must not interfere with a user's performance of official University business, result in direct costs to the University, expose the University to unnecessary risks, or violate applicable laws or other University or Board policy. Users shall have no expectation of privacy in any personal information stored by a user on a University information technology resource, including University electronic mail accounts. Storage of any electronic mail messages, voice messages, file, or documents created by incidental personal use by a user must be nominal.

4.03 Personal Devices and Systems

Users who connect to the University's information technology resources using privately owned personal computers, or other privately owned devices, consent to being scanned by the University's scanning programs for security purposes, such as malicious network traffic, while connected to those technology resources.

4.04 System Abuse and Disruptive Use

A. Users are expected to report suspected illegal activity or abuse, especially if related to any damage to or problems with their files, to abuse@okstate.edu or Ethics Point. Any defects discovered in the system accounting or system security are to be reported, as

well, so that steps can be taken to investigate and solve the problem. The cooperation of all users is needed to ensure prompt action. System administrators are required to report suspected unlawful or improper activities to the proper University authorities. Users have an affirmative duty to cooperate with system administrators in investigations of system abuse.

B. It is a violation of this policy to use the University's information technology resources for transmitting political campaigning, commercial or personal advertisements, solicitations, promotions, or programs, to libel, harass, threaten, or without authorization invade the privacy of other individuals. It is also a violation to use University information technology resources for the purpose of introducing a malicious program into the network, any server or any computer connected to the network. 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. This policy prohibits both the circumvention of mechanisms which protect private or restricted information, systems, or networks, as well as use of University resources for unauthorized access to private or restricted systems or networks and/or damage to software or hardware components of those systems or networks.

C. Modifying or removing computer equipment, software, or peripherals without proper authorization is a violation of this policy. Users will use great care to ensure that they do not use programs or utilities which interfere with other users or which modify normally protected or restricted systems, networks or user accounts. It is inappropriate to encroach on others' use of the University's computers, via intended, unintended or negligent behaviors including but not limited to: sending of excessive electronic communications ('spam'), 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.

D. Interfering with the intended use of information resources or without authorization, destroying, altering, dismantling, disfiguring, preventing rightful access to or otherwise interfering with the integrity of electronic information and/or information systems are not all, but further examples of systems abuse.

4.05 User Accounts and Passwords

A. The integrity of most systems is maintained by password protection of accounts. Users are responsible for assisting in the protection of the systems they use. The integrity and secrecy of an individual's password is a key element of that responsibility. The security of your user account is your responsibility. Users are responsible for ensuring account passwords are strong according to best practices and by not using:
   1. passwords from other accounts such as social media, external email, or other web sites

2. dictionary words

3. personal names

4. computer system names

5. adjacent keyboard combinations such as ‘qwerty’, ‘asdzxc’ or ‘12345’

B. Users may use only their own computer accounts and are personally responsible for all use of their computer account(s). Users who have been authorized to use computing resources (by provision of a user account) may be subject to both criminal and civil liability, as well as University discipline, if the user discloses a password or otherwise makes those resources available to others without the permission of the system administrator.

C. Gaining, or attempting to gain access to the account of another user either by using programs or devices to intercept or decode passwords or similar access control information or by using any other means is prohibited. The negligence or naiveté 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. Intentionally allowing or assisting others to gain unauthorized access to information technology resources is prohibited, regardless of whether the computer, software, data, information, or network in question is owned by the University. Abuse of the networks to which the University belongs or the systems at other sites connected to those networks will be treated as an abuse of Oklahoma State University information technology resources privileges.

4.06 System Logging, Reviews, Privacy

A. Users of the University’s information technology resources are placed on notice that all computer systems maintain audit logs and/or file logs within the computer and that user information is backed up periodically. Information collected and stored may include, but is not limited to, user identification, date and time of the session, software used/accessed, files used/accessed, internet use and access, when requested and deemed necessary. 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. 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.

B. Users should be aware that information transmitted via the Internet may be intercepted by others. Accordingly, the privacy of electronic mail, voicemail and similar data should not be presumed. With regard to all information system data, users should also be aware that the University, as an agency of the State of Oklahoma, and as its officers

and employees, are subject to the provisions of the Oklahoma Open Records Act, 51 Okla. Stat. § 24A.1, et seq.

4.07 Additional Responsibilities

Some departments may have additional use restrictions and it is the user's responsibility to adhere to them. 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.

4.08 Email Use

A. General Purpose Use

1. As with other University resources, electronic mail (email) is made available to faculty, staff and students, to further the teaching, research, service, and Extension/outreach goals and mission of the University. Use of University email services, therefore, is intended to be in furtherance of such goals and mission. Incidental personal use of electronic mail is permitted, but must not interfere with a user's performance of official University business, result in direct costs to the University, expose the University to unnecessary risks, or violate applicable laws or other University or Board policy. Users shall have no expectation of privacy in any personal information sent, received, or stored by a user using University electronic mail accounts. Storage of any electronic mail messages created by incidental personal use by a user must be nominal.

2. Users shall respect the purpose and charters of electronic mailing lists (including local or network news groups and social media). 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.

3. Graduates and retirees are granted life-long use of their institutional email accounts with the understanding that they will adhere to the same policies and procedures which apply to students, faculty and staff. This privilege can be revoked by the University if use of the account results in a violation of policies or procedures, or if the account is needed for business continuity by the area which it served.

B. Reporting Offensive Email

The University provides email services to the University to support the academic and administrative activities, and email is used as an official form of communication. As members of the University's community, all users are expected to demonstrate good taste and sensitivity to others in their communications. However, the University cannot

protect individuals against the existence or receipt of material that may offend them, and users are warned that they may willingly or unwillingly come across, or be recipients of, material they find offensive. To report material received via email, send a complaint to abuse@okstate.edu or Ethics Point.

C. University Access to User Email

1. Users should be aware that the University, as an agency of the State of Oklahoma, as well as its officers and employees, are subject to the provisions of the Oklahoma Open Records Act. There is no privacy associated with use of University email resources. The University owns, and has right of access to, for any purpose, the contents of all computing information transmitted through or stored on its systems. The University may access and disclose any, or all, of the following:
   a. Data transmitted through or stored on its electronic mail and Internet access systems, regardless of the content of the data,

   b. Information related to the use of electronic communication.

2. If an occasion arises when a University officer or supervisor believes that access to an individual's email account is required for the conduct of University business, the University individual is not available (i.e., death, disability, illness or separation from the University), and a system administrator is required to access the individual's email account, the following procedure shall be followed:
   a. The University official or supervisor shall secure permission to access the email account from the Provost and Senior Vice President (Provost) or the designee of such officer.

   b. If the Provost approves the request, he/she will provide written authorization to the Information Security Officer (ISO), who will direct the system administrator to access the email account.

   c. When email communications from a specific individual's University email account are requested by a third party pursuant to the Oklahoma Open Records Act, as part of an internal University investigation, or pursuant to court order or other legal proceeding, the University may, when reasonable and allowed by law, make a reasonable and timely effort to notify the individual whose email account is accessed. However, the University is not required to make such notification.

D. Email Content Classification

It is the responsibility of email users to follow the OSU Data Classifications Policy regarding email content classification and restrictions, protections, or other applicable limitations on email distribution and storage.

4.09 Digital Media Communications / Social Media Use

A. Digital Media Defined

This section applies to any faculty, employee or associate involved in creating, contributing to or distributing University-related information via digital media communication channels often times referred to as Social Media platforms. The term digital media refers to any communications facilitated by technology. This can include online channels, phone/app-based communications and more.

B. Professional and Personal Use

1. The University utilizes social media technologies to enhance more direct communications with its faculty, staff, students, alumni, and prospective students.

2. University employees that use social media should use caution when using their personal social media accounts for business purposes. Specifically:

   a. Individuals should not use their personal account to act or be perceived as acting as representatives of a University, their college, school division, etc. unless given the expressed authority to do so by University Communications. This will help prevent the perception that published personal content is an expression of an official University position. See OSU Policy 1-0103, Use of University Name, for more information.

   b. Individuals should never share proprietary or confidential information or comment on anything related to legal matters without the appropriate approval.

   c. Content shared via social media platforms must also adhere to OSU and OSU A&M policies and procedures as well as state and federal regulations, including though not limited to, FERPA, HIPAA, PCI DSS and NCAA limitations

C. Registering Digital Media Accounts

1. Any person that would like to register a digital media account on behalf of an OSU A&M organization, department or college must request access to the official registration form and work with the Office of Communications to ensure accounts are set up properly. All registered digital media accounts also must adhere to the Digital Media Policy above and University Social Media Guidelines.

2. For questions concerning the use of OSU trademarks, including the OSU logo, please visit, https://trademarks.okstate.edu/.

4.10 Network Usage

Excessive or inappropriate use of the network and network resources may result in network access restriction, revocation of access privileges entirely, or further sanctions covered in Section 4.12 regarding Non-Compliance.

A. Prohibited Devices on Network

1. Users of University information technology resources, specifically those using the University's network are authorized to use only network devices authorized by the campus Information Technology department. Specifically, prohibited devices include, but are not limited to, hubs, switches, repeaters, routers, network modems and wireless access points. These devices may be incorrectly configured or incompatible with the University network causing outages and reliability problems to all or part of the network. Devices not approved for use on the network will be disabled to ensure the stability and availability of the network.

2. For more information on network use, reference the OSU Network Policy at it.okstate.edu/policies.

4.11 Software Licenses and Copyrights

A. Software Licenses

Violating any software license agreement or copyright, including copying or redistributing copyrighted computer software, data, or reports without proper, recorded authorization is prohibited. 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 department does not exceed the number of original copies purchased by that department, unless otherwise stipulated in the purchase contract.

B. General Use of Copyright Material

1. All users of University technology resources are required to abide by and comply with all state and federal laws governing software license, leasing, or copyright agreements.

2. More information on copyright compliance can be found through the United States copyright Office, the Copyright Clearance Center, or the OSU A&M Libraries Copyright pages.

4.12 Non-Compliance

Violations of this policy 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 discharge, dismissal, expulsion, and/or legal action, which may include referral for criminal investigation and/or prosecution.

Approved:
E-Team, June 2017
Board of Regents, June 2017