Rogers State University
Computer Use Policy

Policy Statement

Freedom of expression and an open environment to pursue scholarly inquiry and for sharing of information are encouraged, supported, and protected at Rogers State University. These values lie at the core of our academic community. Censorship is not compatible with the tradition and goals of the University. While some computing resources may be dedicated to specific research, teaching, or administrative tasks that would limit their use, freedom of expression must, in general, be protected. The University does not limit access to information due to its content when it meets the standard of legality. The University's policy of freedom of expression applies to computing resources.

Concomitant with free expression are personal obligations of each member of the University community to use computing resources responsibly, ethically, and in a manner which accords both with the law and the rights of others. The campus depends first upon a spirit of mutual respect and cooperation to create and maintain an open community of responsible users.

Contents

Who Should Know This Policy

✓ President	✓Faculty
✓ Vice Presidents	✓ Other Accounting/Finance Personnel
✓ Deans	✓ Students
✓ Directors	✓Other Groups
✓ Department Chairs	✓ All employees

Responsibilities

Responsible for Policy	
University Officer Responsible:	
Brian Reeves	Director of Information Technology

Procedure

STATEMENT OF PURPOSE: This policy will establish the general guidelines for the use of RSU computing resources equipment, services, software, and computer accounts by students, faculty, staff and administration.

1.0 Definitions

1.1 Abuser is any user or other person who engages in misuse of computing resources as defined in Section 2.2 of this policy

1.2 Computing resources includes computers, computer equipment, computer assistance services, software, computer accounts provided by RSU, information resources, electronic communication facilities (including electronic mail, telephone mail, Internet access, network access), blogs, www browsing, storage media, mobile computing devices or systems with similar functions.

1.3 Computer account is the combination of a user number, username, or userid and a password that allows an individual access to a server or some other shared computer or network.

1.4 Information resources are data or information and the software and hardware that render data or information available to users.

1.5 Network is a group of computers and peripherals that share information electronically, typically connected to each other by either cable or satellite link.

1.6 Peripherals are special-purpose devices attached to a computer or computer network, such as printers, scanners, plotters, and similar equipment.

1.7 Server is a computer or computer program that manages access to a centralized resource or service in a network.

1.8 Software may be programs, data, or information stored on magnetic media (tapes, disks, diskettes, cassettes, etc.). Usually used to refer to computer programs.

1.9 System Administrator is a faculty, staff, or administrator employed by a central computing department such as Academic Computing Services whose responsibilities include system, site, or network administration *and* other faculty, staff or administrators whose duties include system, site, or network administration. System administrators perform functions including, but not limited to, installing hardware and software, managing a computer or network, and keeping a computer operational. System administrators include any persons responsible for a system which provides the capability to assign accounts to other users.

1.10 User is any individual who uses, logs in, attempts to use, or attempts to log in to a system, whether by direct connection or across one or more networks, or who attempts to connect to or traverse a network, whether via hardware, software or both. Each user is responsible for his or her use of the computer resources and for learning proper data management strategies.

2.0 User Responsibility

2.1 *Appropriate Use of Computing Resources:*

These guidelines set forth standards for responsible and acceptable use of University computing resources. They supplement existing University policies, OneNet Acceptable Use agreements (located at www.onenet.net) and state and federal laws and

regulations. Computing resources include, but are not limited to, host computer systems, University-sponsored computers and workstations, communications networks, software, and files.

Computing resources are provided to support the academic research, instructional, and administrative objectives of the University. These resources are extended for the sole use of University faculty, staff, students, and other authorized users ("users") to accomplish tasks related to the user's status at the University, and consistent with the University's mission. Users are responsible for safeguarding their identification (ID) codes and passwords, and for using them for their intended purposes only. Each user is responsible for all transactions made under the authorization of his or her ID. Users are solely responsible for their personal use of computing resources and are prohibited from representing or implying that the content constitutes the views or policies of the University.

Violation of these guidelines constitutes unacceptable use of computing resources, and may violate other University policies and/or state and federal law. Suspected or known violations must be reported to the appropriate University computing unit. Violations will be processed by the appropriate University authorities and/or law enforcement agencies. Violations may result in revocation of computing resource privileges; academic integrity proceedings, faculty, staff or student disciplinary action; or legal action.

2.2 *Prohibited Use of Computing Resources:*

RSU characterizes misuse of computing and information resources and privileges as unethical and unacceptable. Misuse constitutes cause for taking disciplinary action. Misuse of computing resources includes, but is not limited to, the following:

- Altering system software or hardware configurations without authorization, or disrupting or interfering with the delivery or administration of computer resources.
- Attempting to access or accessing another's computer, computer account, private files, or e-mail; or misrepresenting oneself as another individual or agent of the University in electronic
- Engaging in practices that threaten the network (e.g. loading files that may introduce a virus, using procedures and/or tools to gather information about RSU's computing resources, etc.).
- Installing, copying, distributing or using software in violation of copyright and/or software agreements, applicable state and federal laws;
- Using computing resources to engage in conduct which interferes with others' use of shared computer resources and/or the activities of other users, including studying, teaching, research, and University administration.
- Using computing resources for commercial or profit-making purposes without written authorization from the University.
- Failing to adhere to individual departmental or unit lab and system policies, procedures, and protocols.
- Allowing access to computer resources by unauthorized users.
- Using computer resources for illegal activities. Criminal and illegal use may include obscenity, child pornography, threats, harassment, copyright infringement, defamation, theft, and unauthorized access.

2.3 User Responsibility. All users of RSU computing resources must act responsibly. Every user is responsible for the integrity of these resources. All users of RSU-owned resources must respect the rights of other computing users, respect the integrity of the physical facilities and controls, and respect all pertinent license and contractual agreements. It is the policy of RSU that all members of its community act in accordance with these responsibilities, relevant laws and contractual obligations, and the highest standard of ethics.

2.4 Password Protection. Each user is responsible for maintaining absolute security of any password or password right granted to the user. Passwords must not be "shared" with another user. Password security helps to protect the RSU system against unauthorized access.

2.5 Computing Resource Access. Access to RSU's computing resources is a privilege granted to RSU students, faculty, staff and administrators. RSU reserves the right to limit, restrict, or extend computing privileges and access to its information resources.

2.6 Freedom of Communication. It is the intention of RSU to maximize freedom of communication for purposes that further the goals of RSU. RSU places high value on open communication of ideas, including those new and controversial.

2.7 General Right of Privacy. A general right of privacy should be extended to the extent possible to the electronic environment. RSU and all electronic users should treat electronically stored information in individual files as confidential and private. Contents should be examined or disclosed only when authorized by the owner, approved by an appropriate institution official, or required by law. Privacy is mitigated by the following circumstances.

a. RSU is an agency of the State of Oklahoma and therefore subject to the Oklahoma Public Records Act. For RSU employees, electronic information created in the performance of their duties may be public records, just as are paper records. Such records may be subject to review and/or release under Oklahoma law. All computer files and e-mail communications, unless subject to a specific privilege, are subject to production under the Oklahoma Public Records Act and, when relevant, to discovery in civil litigation. In these cases, disclosure of personal e-mail or files not related to the specific issue discussed in any Public Records request or discovery will be avoided to the extent allowed by law.

b. Administrative files of RSU are generated as part of the process of managing the institution. Files that employees create or maintain can be reviewed by supervisors within this administrative context. Generally, faculty research files and files relating to scholarly endeavor will not be subject to such a review.

c. There is an acknowledged trade-off between the right of privacy of a user and the need of system administrators to gather necessary information to ensure the continued functioning of these resources. In the normal course of system administration, system administrators may monitor any computing activity or examine activities, files, electronic mail, and printer listings to gather sufficient information to diagnose and correct problems with system software or hardware. Sometimes system administrators may monitor computing activity or access files to determine if security violations have occurred or are occurring. In that event, the user should be notified as soon as practical. System administrators at all times have an obligation to maintain the privacy of a user's files, electronic mail, and activity logs.

d. Computer systems and stored data are subject to review by authorized personnel for audit purposes or when a violation of RSU policy or law is suspected.

2.8 Disclaimer – RSU makes no warranties of any kind, whether express or implied, regarding the electronic communications facilities or services it provides. RSU will not be responsible for any damages suffered by a user through the use of the RSU electronic communications facilities or services, including, but not limited to, loss of data resulting from delays, nondeliveries, misdeliveries, or service interruptions caused by its own negligence or by any error or omissions or any user. Use of any information obtained via the Internet will be at the user's risk. RSU specifically denies any responsibility for the accuracy or quality of information obtained through its electronic communications facilities and services.

3. Procedures

3.1 Computer accounts will be issued to authorized users only by Academic Computing Services

3.2 Prior to issuance of an account and password, all staff and faculty must execute such forms, including an acknowledgment and acceptance of the terms of this policy, as may be reasonably required by RSU.

3.3 User passwords must be kept private, and may not be disclosed to any other individual or entity. Passwords should be memorized; however, if a password is written down, it must be kept at all times in the user's wallet or purse. A password must NEVER be posted or placed where it can be discovered by someone other than the user.

3.4 Each user will be assigned a Userid in accordance with rules established by Academic Computing Services.

3.5 Personal passwords will be maintained by the individual user and must be changed at least every 90 days for faculty and staff and at least every 120 days for students, or at more frequent intervals as the user may elect. Passwords shall be selected in accordance with rules established by Academic Computing Services. In the event another person learns a user's password, the user must immediately change the password. Academic Computing Services will never ask a user for their password.

3.6 Any user who learns of an unauthorized use of his or her account must report the unauthorized use to Academic Computing Services immediately.

3.7 In the event it appears that a user has abused or is abusing his or her computing privileges, or engages in any misuse of computing resources, then RSU may pursue any or all of the following steps to protect the user community:

a. take action to protect the system(s), user jobs, and user files from damage;

b. begin an investigation, and notify the suspected abuser's project director, instructor, academic advisor, dean or administrative officer of the investigation;

c. refer the matter for processing through the appropriate RSU disciplinary system;

d. suspend or restrict the suspected abuser's computing privileges during the investigation and disciplinary processing. A user may appeal such a suspension or restriction and petition for reinstatement of computing privileges through the procedures existing at the time the user requests an appeal, which procedures will be provided to the appealing user in writing;

e. inspect the alleged abuser's files, diskettes, and/or tapes. System administrators must have reasonable cause to believe that the trail of evidence leads to the user's computing activities or computing files before inspecting any user's files;

f. In the event the misuse also constitutes a violation of any applicable federal, state or local law, RSU will refer the matter to appropriate law enforcement authorities.

Contacts

Policy Questions: Director of Information Technology, 918-343-7538

Policy History

Policy
Issue Date: 3-29-2000
Revised: 3/31/2015