TRUMAN STATE UNIVERSITY
INFORMATION TECHNOLOGY SERVICES

Computer Use Policy

Table of Contents

Preliminary Statement

Freedom of expression and an open environment to pursue scholarly inquiry and for sharing of information are encouraged, supported, and protected at Truman State University. These values lie at the core of our academic community. 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's policy of freedom of expression applies to computing resources. Concomitant with free expression are personal obligations of each member of our 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.

As an institution of higher education, the University encourages, supports, and protects First Amendment rights 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. As with any resource, it is possible to misuse computing resources and facilities and to abuse access to the Internet.

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 to accomplish tasks related to the user's status at the University, and consistent with the University's mission.

Use of University Resources

Use of University computing resources and facilities requires that individual users act in compliance with the University policies and procedures as detailed in *the Student Code of Conduct, the Staff Handbook,* and the *Faculty Handbook*. The University provides users with accounts that permit use of the computing resources and facilities within policies and procedures established by the University. Any person who uses University computing resources and facilities through University-owned equipment (such as public access computers at the libraries and computer labs) is also a user and is permitted to use the computing resources and facilities within policies and procedures established by the University. Users do not own accounts on University computers, but are granted the privilege of exclusive use. Users must respect the integrity of computing resources and facilities, respect the rights of other users, and comply with all relevant laws (local, state, federal and international), University policies and procedures, and contractual agreements. The University reserves the right to limit, restrict or deny computing resources and facilities for those who violate University policies, procedures, or local, state or federal laws.

Censorship

Censorship is not compatible with the goals of the University. The University shall not limit users' voluntary access to any information due to its content when it meets the standard of legality.

A. It has been the custom at Truman that supervisors and co-workers respect their colleagues' privacy in the workplace. The fact that a desk, office or computer is University property does not, by itself, entitle a supervisor or colleague to indiscriminately enter or access it.

B. Similarly, supervisors may legitimately define and inform employees of the ways in which the performance of their duties or the use of University resources will be monitored. For example, systems administrators may from time to time need to monitor system use in ways that make them privy to what users are doing. This need is legitimate when appropriately directed and confined, and users should be made aware that it will be done.

C. In normal cases, the individual's desire of privacy in his or her work space, and the University's need for information, have long been easily reconciled by a simple expedient: if a supervisor or colleague needs information, he or she asks for it. The advent of technology in the workplace does not alter this common courtesy. In the rare case where a request for information is unavailable – as when an employee is absent for a prolonged period and the information is not available elsewhere, or where the employee refuses to provide information to a person who is authorized to have it – a supervisor should consult with the President or his designee for guidance as to the proper ways of obtaining the information.

D. The University has long provided an internal mail delivery system that members of the community use for University business and incidental personal messages. E-mail is an electronic message-delivery system that supplements (and, increasingly, replaces) the delivery of paper. In either case, the message is intended for that person to whom it is addressed, and others should not read it without permission. A deliberate attempt to read another's mail, knowing it is not meant for the reader, is a serious breach of ethical conduct. At the same time, there is no right to use e-mail (any more than there is a right to use traditional mail) for objectives that are illegal or inimical to the University's purposes. Where sufficient evidence of such use exists, supervisors should consult the President or his designee.

E. Such principles also govern the use of other means of communication, such as telephone calls, voice mail and fax transmissions.

F. Systems administrators, information technology specialists, and others with expertise in, and specific responsibility for, computer systems do not thereby have special powers or authority to determine what expectations of privacy are reasonable, nor should they alone decide what uses of computing resources are permitted. Decisions in this respect should be made after due consultation with affected supervisors, deans and other senior University administrators, legal counsel, or others who are responsible for the proper use of University resources. The extent of consultation will vary with the nature of the decision to be made and the various actions under consideration.

Intellectual Property

All members of the University community should be aware that property laws apply to the electronic environment. Users must abide by all software licenses, University copyright and software policies and procedures, and applicable federal and state law. Users should assume that works communicated through a network are subject to copyright unless specifically stated otherwise. Unless permission of the author is obtained, utilization of any electronically transmitted information must comply with the "fair use" principle found in federal copyright law.

Criminal or Illegal Acts

Computing resources of the University, which include the hardware, software and network environment, shall not be used for illegal or criminal activities. Any illegal or criminal use of these resources will be dealt with by the appropriate University authorities and/or other legal and law enforcement agencies. Criminal and illegal use may involve, but is not limited to unauthorized access, intentional corruption or

misuse of computing resources, theft, defamation, obscenity, child pornography, and harassment based upon race, ethnicity, national origin, disability, age, religion or sex. Users must respect the rights of other users, respect the integrity of the systems and related physical resources, and observe all relevant laws, regulations, and contractual obligations.

Network Definition and Usage Policies

The University network is defined to include any and all computer and electronic based communication facilities and/or equipment, which are owned or operated under the supervision of Truman State University. The University network is for use by authorized personnel affiliated with the University, consistent with, and in the course of, their official work, study, and/or research. Individual groups or projects within the University may adopt more restrictive network usage policies that apply to their subnetworks and personnel within their area. Acceptable and unacceptable uses of Truman computing resources including the campus network are outlined below. *Note: this list is not all inclusive*.

Acceptable uses:

- Any use that is necessary to complete research and/or coursework as assigned by or to any university employee or student.
- Communication for professional development or to collaborate in research and education.
- As a means for authorized users to have legitimate access to remote facilities such as email, network resources, and/or Internet access.
- The publication of information via the Internet's World Wide Web (WWW), File Transfer Protocol (FTP), or similar techniques.
- Other administrative and/or academic communications or activities in direct support of University projects and missions
- Limited personal use may be allowed when such use meets the following criteria; it does not interfere with University operations, it does not compromise the functioning of University network and computing resources, it does not interfere with the user's employment or other obligations to the University, and it does not violate any other University policy.

Unacceptable Uses:

- Any use deemed commercial or for-profit.
- Any use that is likely, intended, or by negligence causes unauthorized network disruption, system failure, or data corruption.
- Any use related to achieving, enabling, or hiding unauthorized access to network resources, Truman owned software, or other information belonging to Truman State University, either within or outside the Truman network.
- Any use related to sending/receiving electronic mail that includes, but not limited to, the following: solicitation or commercial use, forging any portion of an electronic mail message, spamming (bulk unsolicited email), or sending unwanted messages to unwilling recipients.
- Intentionally circumventing or building an unauthorized conduit through the University firewall with intentions of bypassing University network management and security devices.
- Use of another individual's identification; network, email or other university based account; and/or related passwords.
- Unauthorized transfer or entry into a file, to read, use, or change the contents; or for any other reason.
- Use of computing facilities or network resources to send obscene, harassing, abusive, or threatening messages or computer viruses or worms.
- Any use that violates Truman policies, procedures, and contractual agreements.
- Any use that violates local, state or federal laws.

User Responsibility and Account Ownership

Users may not allow other individuals to use their Truman assigned network, email, or other University based account. Employees and students are individually responsible for the proper use of their assigned accounts, and are accountable for any activity associated with the account. Users are also responsible for the security of their assigned accounts. Users should take proper

security measures to ensure the integrity of their accounts, and should also report any notice of unauthorized access.

Additional Policies

Truman State University is required by contract with MOREnet to abide by and therefore enforce their policies and procedures. The following section has been copied in whole from MOREnet. For more information about MOREnet's policies, procedures, and security measures, please visit the following website: http://www.more.net/security/.

MOREnet Acceptable Use Policy

Acceptable Use:

- All network use by MOREnet members, project participants and those connected via MOREnet members or project participants shall be for, or in support of, research; education; local, state or national government affairs; economic development or public service.

Unacceptable Uses:

- It is not acceptable to use MOREnet for purposes which violate federal or state law.
- It is not acceptable to use MOREnet for any purpose which violates copyright.
- It is not acceptable to use MOREnet in a manner that is harmful or harassing to others.
- It is not acceptable to use MOREnet in a manner that intentionally or negligently disrupts normal network use and service. Such disruption would include the intentional or negligent propagation of computer viruses, the violation of personal privacy, and the unauthorized access to protected and private network resources.
- It is not acceptable to use MOREnet for commercial activities that are not in support of education, research, public service, economic development or government purposes. Further, it is not acceptable to distribute unsolicited advertising. Additional information regarding unacceptable commercial uses of MOREnet is available.

Enforcement of Policy

Each MOREnet member or project participant must make reasonable efforts to publicize the policies of MOREnet and to ensure compliance of those connected through them.

Reported and perceived violations of the Acceptable Use Policy will be reviewed by the MOREnet Executive Director. Violations that are not promptly remedied by the member institution or project participant may result in action including the termination of MOREnet service or the forfeiture of MOREnet membership.

Questions

If you have questions about the MOREnet Acceptable Use Policy, its interpretation or enforcement, please send e-mail to security@more.net.
(Approved May 22, 2002)