The University of Tulsa Ethics Code and Policy for Computer Use

(adopted Oct4, 1993; revised July 26, 1995, revised July 23, 2004)

PURPOSE

To establish policy to ensure the provision of computer and telecommunication resources and services to the faculty, staff, and students, as well as outside clients of The University of Tulsa (TU). This policy applies to the use of all institutional data regardless of the office in which it resides or the format (paper, film, electronic, etc.) in which it is used.

The following policy, rules, and conditions apply to all users of TU computer and telecommunication resources and services. Violations of this policy are unethical and possibly unlawful. In accordance with established University practices, violations may result in disciplinary action that could result in expulsion from the University or dismissal from a position, and/or legal action.

POLICY

TU strives to provide all computer users with privacy and a fair share of technical resources. All computer users have the responsibility to use the TU computer resources in an efficient, effective, ethical, and lawful manner consistent with the Rules and Regulations of the University. The ethical and legal standards that all users should maintain are derived directly from standards of common sense and common decency that apply to the use of any public resource within the University and are documented in the local, state, and federal statutes and The University of Tulsa codes, rules, regulations, policies, and procedures.

The University of Tulsa seeks to protect computer-based information, recognized as a primary administrative, educational and research asset, from accidental or intentional unauthorized modification, misuse, destruction, disruption, or disclosure. In order to make every reasonable effort to protect the integrity of its computing systems, workstations, networks, lab facilities, etc., the University has the right to monitor its computing resources.

TU has an obligation to respect the privacy of a user's files, electronic mail, and printer listings to the best of its ability. With reasonable cause for suspicion, TU has the right to monitor any and all aspects of a system, including individual login sessions to determine if a user is acting in violation of the policies set forth in this document or as stated by law. The issuance of a password or other means of access is to assure appropriate confidentiality of university files and information and does not guarantee privacy for personal or improper use of university equipment or facilities.

1. USERS MUST ABIDE BY ALL SOFTWARE LICENSES, TU COPYRIGHT AND INTELLECTUAL PROPERTY POLICIES AND APPLICABLE FEDERAL AND STATE LAWS. (As an example, talking points for "SELECTED OKLAHOMA STATUTES AFFECTING USE OF TELECOMMUNICATIONS" are posted at http://www.is.utulsa.edu/policies/)

2. Users are responsible for safeguarding his or her user identification (ID) and password. Users should not print, store on-line, or give his or her password to others. The user is responsible to make authorized usage of the ID for its intended purpose only. Each user is responsible for all transactions made under the authorization of his or her ID.

3. Computer users shall not intentionally seek, provide, or modify information in or obtain copies of files, programs, keystrokes, or passwords belonging to other computer users without the permission of those other computer users. This includes all system files and accounts.

4. Files controlled by individual users are considered private, whether or not they are accessible by other users. A user must obtain written permission from the owner of a file to alter or copy a file that does not belong to him or her. The ability to read, alter or copy a file does not imply permission to read, alter or copy that file.

5. Each account owner and workstation user is solely responsible for the usage incurred through her/his account or workstation. Individuals who intentionally abuse accounts and privileges, degrade system performance, misappropriate computer resources or interfere with the operation of the computer and/or telecommunication facilities are subject to disciplinary action. The removal, modification, or reconfiguration of files on TU computer hardware or software is prohibited.

6. The electronic communication facilities are not to be used for the transmission of commercial or personal advertisements, solicitations, promotions, destructive programs, political material, or any other unauthorized or personal use.

7. The development and/or use of self-replicating code is allowed only under the direction of the academic faculty and Computing and Information Resources.

8. Computer users will use network links solely for the purpose permitted in the network guidelines (e.g., Internet1, Internet2, National Lambda Rail). Users are responsible for obtaining and adhering to all network acceptable use policies.

9. The ability to connect to other systems through the network does not imply the right to connect to these systems or to make use of these systems unless properly authorized by the owners of those systems.

10. Users share many resources, such as disk space, CPU cycles, printer queues, batch queues, login sessions, software licenses, etc. No user may monopolize these resources and should utilize these resources only to the extent necessary for purposes related to authorized use.

11. Computer users shall not intentionally develop or use programs or devices that harass other computer users or that infiltrate the system and/or damage the software or hardware components of the system. Users have the right not to be harassed whether it be by physical, verbal, electronic, or other form of abuse and may complain or bring formal grievance through appropriate channels where the abuse complained of is by a TU authorized user, whether on or off campus.

12. Although each user has the right to freedom of speech, harassing or defamatory material may not be sent via electronic mail or posted to electronic bulletin boards, news groups, etc.

13. Use of the electronic communication facilities (such as electronic mail, telephone mail, or systems with similar functions) to send fraudulent, harassing, obscene, indecent, profane, intimidating, or other unlawful messages is prohibited.

14. Users will not aid, abet, or act in conspiracy with another to violate any part of these policies, rules, and conditions.

15. Occasional proper personal use of computer equipment and software is permitted when personal use does not interfere with expected work performance or violate any applicable policy, rule, or law. An employee's performance appraisal may take into account personal use and a supervisor may require a change in personal use as a condition of employment where appropriate.