



United Tribes Technical College

Acceptable Use Policies for United Tribes Computer System

1.0 Policy

The purpose of this policy is to outline the acceptable use of computer equipment at United Tribes Technical College. Inappropriate computer use exposes everyone to risks including virus attacks, compromise of network systems and services, and possible litigation. College computing systems are for business purposes in serving the administrative, academic and research activities of the College, faculty, staff and students.

This policy establishes rules and prohibitions that define acceptable use of College systems and technology. While acceptable use is encouraged, unacceptable use may be grounds for loss of computing privileges, disciplinary action, and legal sanctions under federal, state and local laws.

Effective security is a team effort involving the participation and support of every College employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines and conduct their activities accordingly.

2.0 Scope

This policy applies to faculty, staff, students, contractors, consultants, temporaries, and other workers in the College (hereafter referred to as “Users”), including all personnel affiliated with third parties. This policy applies to all equipment and or systems that are connected to the UTTC network, including, but not limited to, facsimiles, telephones, computers, the UTTC e-mail system, and the Internet.

3.1 General Use and Ownership

1. For security and network maintenance purposes, authorized individuals within UTTC may monitor equipment, systems and network traffic at any time.
2. UTTC reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy and College policies. This may include, but may not be limited to, monitoring Internet usage of any kind, monitoring email messages, and listening to stored voice-mail messages.
3. All electronic and telephonic communication systems and all communications and information transmitted by, received, or stored in these systems are the property of UTTC and as such are to be used, to the maximum extent possible, for job-related purposes.

3.2 Security and Proprietary Information

1. Examples of confidential information include but are not limited to: UTTC private, UTTC strategies, competitor sensitive, trade secrets, specifications, student lists, and research data. Users should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
3. All PCs, laptops and workstations should be secured with passwords for all local accounts in compliance with the UTTC's Password Policy. Use additional settings as deemed necessary to prevent unauthorized access to resources and data that resides either locally or remotely.
4. Because information contained on portable computers is especially vulnerable, special care should be exercised.
5. While it is currently not required, postings by Users from a UTTC email address to newsgroups, bulletin boards, blogs, etc. should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of UTTC, unless posting is in the course of business duties.
6. All computers used by the employee or student that are connected to the UTTC Internet/Intranet/Extranet, whether owned by the employee/student or the College, should be continually executing approved virus-scanning software with a current virus database.
7. Employees and students must use extreme caution when opening unsolicited e-mail attachments, which may contain viruses, e-mail bombs, or Trojan horse code. If uncertain about an attachment, employees may contact the UTTC IT Department, and students may contact email support at "student.email.support@uttc.edu".

3.3. Acceptable Use

In general, the same ethical conduct that applies to the use of all College resources and facilities applies to the use of UTTC's systems and technology. In making acceptable use of the College's systems and technology you must:

1. Use College systems and technology is intended for authorized purposes. Personal use should be limited to what is necessary and reasonable and should not interfere with College operations.
2. Protect your user-id and system from unauthorized use. You are responsible for all activities on your user-id or that originate from a system.
3. Access only information that is your own, that is publicly available, or to which you have been given authorized access.
4. Use only legal versions of copyrighted software in compliance with vendor license requirements.
5. Be considerate in your use of shared resources. Refrain from monopolizing systems, overloading networks with excessive data, degrading services, or wasting computer time,

connect time, disk space, printer paper, manuals, or other resources. **NOTE:** The UTTC IT Department provides network bandwidth as needed to the various departments/areas on campus. The IT Department maintains the right as needed to allocate or restrict access when appropriate in order to maintain network stability and ensure the proper functioning of core college applications and systems.

3.4. Unacceptable Use

The following activities are prohibited. Users may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an employee or student of UTTC authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing UTTC -owned resources

The lists of prohibited activities presented below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities:

The following activities are strictly prohibited, with no exceptions

1. Violations of the rights of any person or entity protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the College.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, copyrighted videos and/or movies, and the installation of any copyrighted software for which the College or the end user does not have an active license is strictly prohibited.
3. Using any peer-to-peer (P2P) file-sharing program, such as Kazaa, BearShare, LimeWire, etc.
4. It is illegal to export software, technical information, encryption software or technology, in violation of international or regional export control laws. The appropriate College IT Department member should be consulted prior to export of any material that is in question.
5. Downloading or installing application software from the Internet on UTTC computers, except as necessary to access information needed to conduct UTTC business or to protect information on the user's computer. Any such software must be approved in advance by the UTTC IT Department.
6. Violations of copyright law. Many of the materials on the Internet are protected by copyright. Even though they may seem to be freely accessible, copyright laws that apply to print media also apply to software and material published or made available on the Internet. Employees are permitted to print out Web pages and to download material from the Internet for informational purposes as long as the purpose for such copying falls into the category of "fair use". Please do not copy or disseminate material that is copyrighted.

Employees having any questions regarding such materials should contact their supervisor.

7. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
8. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
9. Using a College computing asset to engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
10. Making fraudulent offers of products, items, or services originating from any UTTC account. Or, offers of products, items, or services for personal profit from any UTTC account.
11. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
12. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access. The only exception to this is when access is part of a security analysis performed by an authorized individual within the College. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information.
13. Port scanning or security scanning is expressly prohibited unless prior approval is obtained from the UTTC IT Department.
14. Executing any form of network monitoring which intercepts data not intended for the user's host, unless this activity is a part of the user's normal job/duty.
15. Circumventing user authentication or security of any host, network or account.
16. Interfering with or unsanctioned denying of service to any user other than the user's host (for example, denial of service attack).
17. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
18. Intentionally causing physical damage to UTTC equipment, including but not limited to telephones, fax machines, printers, scanners, computers, monitors, and so on.
19. Providing information about, or lists of, UTTC employees or students to parties outside the College.

Email and Communications Activities:

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2. Any form of harassment via email, telephone or paging, whether through content, language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters" or "pyramid" schemes of any type.
6. Use of unsolicited email originating from within UTTC 's networks or other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by UTTC or connected via UTTC 's network.
7. Posting identical or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam)

4.0 Enforcement

Any employee or student found to have violated this policy may be subject to disciplinary action by their Administrative unit or the College and have email, network usage discontinued.

5.0 Definitions

Term	Definition
Blog	Blog is short for weblog. A weblog is a journal (or newsletter) that is frequently updated and intended for general public consumption. Blogs generally represent the personality of the author or the Web site.
Extranet	A private network that uses the Internet protocol and the public telecommunication system to securely share part of a business's information or operations with suppliers, vendors, partners, customers, or other businesses.
Internet	A worldwide system of computer networks.
Intranet	A private network that is contained within an enterprise.
Newsgroup	An area on a computer network, especially the Internet, devoted to the discussion of a specified topic.
Spam	Unauthorized and/or unsolicited electronic mass mailings.