TOOELE TECHNICAL COLLEGE

Computer Resources Acceptable Use Policy

---

1. Purpose

1.1. The purpose of the Tooele Applied Technology College (TATC) Computer Resources Acceptable Use Policy is to ensure that all uses of TATC computer resources are ethical, legal and consistent with the stated purpose, goal, and mission of the TATC. Additionally, the policy seeks to protect TATC computer resources from damage and undue wear caused as a result of inappropriate use or harsh treatment.

1.2. Increasing global access and contact through computers and computer networks increases the availability of controversial material. Neither the UCAT Board of Trustees nor the TATC have control of the information on the Internet. Certain sites accessible via the Internet may contain material that is illegal, defamatory, inaccurate or potentially offensive to some people.

1.3. The TATC administration recognizes the importance of each individual's judgment regarding appropriate conduct in maintaining a quality resource system. While this policy does not attempt to articulate all required or proscribed behavior by its members, it does seek to assist in such judgment by providing the following guidelines:

2. Definitions

2.1. For the purposes of this policy:

2.1.1. User is defined as any TATC administrator, faculty member, staff employee, student and/or visitor.

2.1.2. Financial gain is defined as gain derived from any activity recognized under current U.S. Tax Code as qualifying as a business.

2.1.3. Illegal activities are defined as violations of local, state, and/or federal laws including, but not limited to, copyright violations, harassment, threats, libel, and disorderly conduct.

2.1.4. Disruptive activities are defined as activities including, but not limited to, those defined by Utah Code that interfere with the lawful operations of higher education institutions or that disrupt the activities of the school or its students.

2.1.5. Obscene is defined by reference to current applicable judicial and statutory provisions and is generally understood to mean objectionable or offensive by accepted standards of decency, i.e. whether the average person, applying contemporary community standards, would find that the material, taken as a whole, appeals to the prurient; whether the material depicts or describes, in a patently offensive way, sexual conduct specifically defined by the

applicable state law, and whether the material, taken as a whole, lacks serious literary, artistic, political, or scientific value (Miller v. California (413 U.S. 15,93 1973).

2.1.6. Inappropriate use is defined as a violation of the intended use, as outlined in this policy, of TATC computer resources.

2.1.7. Political lobbying is defined as activities on behalf of a particular party, candidate, or political issue such as constitutional amendments, referenda, etc.

2.1.8. P2P (Peer-to-Peer) is a networking term used when two or more potentially global computing devices are directly communicating with one another in an isolated fashion.

2.1.9. File sharing is a process using P2P technology to swap copyrighted files, which potentially violates copyright law.

2.1.10. Computer resources include all computer hardware, software, peripheral devices, the TATC wiring infrastructure, and the network and Internet environment accessed through these resources.

3. Policy

3.1. In addition to any other inappropriate and unacceptable use prohibited by this policy, and without limitation, the following are specifically prohibited:

3.1.1. Sharing of passwords and/or accounts

3.1.2. Attempts to gain access to any system or account without authorization from administration

3.1.3. Use of destructive or invasive software

3.1.4. Use of computer resources for personal financial gain

3.1.5. Use of computer resources for product advertisement or political lobbying

3.1.6. Use of computer resources for disruptive or illegal activities

3.1.7. Any file sharing or P2P file sharing allowing computing devices to upload/download information from any other computing device resulting in copyright violation/infringement

3.1.8. Use of computer resources to access or display images, sounds or messages which are obscene.

3.1.9. Use of computer resources, in a public location, which, while not necessarily obscene or otherwise illegal, nevertheless creates a hostile environment in violation of college policy, state, and or federal law.

3.2. **Authorized Network Use.** TATC hardware/software accounts shall be used only by the authorized owner of the account. Account owners are ultimately responsible for all activity under their account. Users are encouraged to change their passwords every 60 days.

3.3. **Network Access Time.** Excessive and open-ended use of the network in terms of access time cannot be accommodated due to cost and interference with legitimate needs of other users. Users are cautioned to exercise prudence in the shared use of this resource.

3.4. Privacy of Information. All communications and information accessible via TATC hardware/software should be assumed to be TATC property. Great care is taken by the TATC Network Administrator to ensure the right of privacy of users, however all files on TATC hardware are subject to review without notice.

3.5. Use of College-Owned Computer Equipment. Equipment accessing any network resource and installed software on the equipment is provided for purposes of the official work of the College, not for personal use or entertainment. Users are expected and required to use College-owned equipment primarily for official business in connection with their jobs. College policy does not prohibit incidental personal use of the equipment. However, users are required to exercise reasonable precautions in caring for any equipment authorized for use off-premises, and are personally responsible for any damage resulting from use of unauthorized persons.

3.5.1. All modifications to TATC hardware will be made at the direction and discretion of the Network Administrator upon approval of the Campus President.

3.5.2. Any off-site use of TATC hardware must be approved by the user's immediate supervisor. Equipment taken off-site for instructional purposes must be signed in and out following approved TATC procedures.

3.5.3. While this policy recognizes that a reasonable amount of wear due to use is to be expected, any damage which is deemed to be the result of intentional misuse, abuse, or gross negligence will be the financial responsibility of the assigned user. Additionally, users will be held accountable for any wear or damage caused by use of the equipment for non-approved or inappropriate purposes.

3.6. Authorization and Installation of Software. Software installed on College computer equipment must be installed by TATC Information Technology employees. Installation of personal copies of software or installation of software (including but not limited to computer games) by other College employees may only be done with the approval of the employee's immediate supervisor and with the consent of the Information Technology Department. This policy is intended to ensure compliance with software licensing obligations and also to safeguard against avoidable introduction of computer viruses, as well as avoiding unnecessary potential overloading of memory and hard disc storage capacity of College-owned equipment. Need for the installation of specific specialized software packages (apart from College-wide standard software modules) may be verified in writing by the cognizant administrator and installed by the specific end- user with authorization of the Information Technology Department.

3.7. Prohibition on Copying College-Owned Software. Under no circumstance may unauthorized users copy College- owned software for installation on personal, or any other, computer equipment. In some cases, users wishing to work at home on College business, either on their own time or on an approved telecommuting basis, may wish to utilize personally-owned computer equipment. With specific approval by the cognizant administrator, related College-owned software may be installed on the user's personal computer equipment, but only by TATC Information Technology employees. An inventory of College-owned software installed on a user's personal PC

will be maintained, and the software will be deleted and the deletions verified when the user terminates employment with the TATC.

3.8. Internet Access and Use. On a need-to-have basis, the Information Technology Department will activate access to the Internet. Users are expected to exercise sound judgment in the use of this resource, and to limit their use primarily to official College business and to incidental and off-duty personal uses that are appropriate to standards of ethical behavior. Users with off-premises access to the Internet are required to safeguard against its use by unauthorized persons.

3.9. Policy Consent and Infractions. All users must sign an agreement to comply with this policy before being assigned any equipment or given any access to College computer resources. All non-employee users must be given ample opportunity to review this policy and are to understand that use of College computer resources constitutes an agreement to be bound by this policy.

3.9.1. Use of College computer resources should be appropriate, professional, and consistent with the mission of the institution. As necessary, the College Administration will determine whether specific uses of College computer resources are consistent with this policy.

3.9.2. In the event that the Information Technology Department suspects or detects an infraction of this policy, they will report their suspicions to the Campus President for further investigation and/or appropriate action.

3.9.3. Violations of the provisions stated in this policy may result in suspension or revocation of any or all computer privileges and or disciplinary actions.

3.10. Password Requirements. A strong and secure password is one of the most effective ways to secure TATC's electronic information. The following are the minimum acceptable standards for any password created on a computer system at TATC:

3.10.1. Must be 8 characters and contain at least one special character

3.10.2. Must not be the same passwords used for personal accounts

3.10.3. Must not be shared with anyone

3.11. Data backups. Electronic data is only backed up for specific locations. Employees are strongly encouraged to save any data important to the College in a location that is being backed up.

3.11.1. Daily backups are performed on staff user data contained in the following locations:

3.11.1.1. Windows computers folders: Documents, Desktop, and the Shared Drive

3.11.1.2. Google Apps data: Email, Drive, Calendar, Sites, Contacts, and Groups

3.11.2. The following data locations are NOT being backed up by the TATC IT department:

3.11.2.1. Pictures, Music, Videos, Downloads, Favorites, and **any student data**

3.11.2.2. Any other data stored in the cloud or elsewhere on the Internet

3.11.2.2.1. Examples of cloud storage include: Dropbox, Evernote, or any other computer system not physically located at TATC.

3.11.2.2.2. Although the Learning Management System is in the cloud, it is backed up twice annually.

4. Internet Safety

4.1. The Following uses of the Internet & computer equipment are prohibited:

4.1.1. Any access by computer users to inappropriate matter on the Internet;
4.1.2. Unauthorized access including "hacking" and other unlawful activities by students online;
4.1.3. Unauthorized disclosure, use, and dissemination of personal information regarding students;

4.2. Monitoring

4.2.1. TATC reserves the right to monitor and review any material on any machine at any time in order for the

4.3. Filtering

4.3.1. In order to ensure the safety and security of the school's users, a technology protection measure is in place in order to block or filter inappropriate sites on the internet. This filtering mechanism protects against access by adults and minors to visual depictions that are obscene, child pornography, or – with respect to use of computers with internet access by minors – harmful to minors.