

POLICY TITLE: **Acceptable Use Policy**

POLICY #: **ITS - 1**

DATE DRAFTED: **October 05, 2005**

APPROVED DATE: **December 05, 2005**

REVISION DATE:

1.0 INTRODUCTION

Trinity Valley Community College provides a wide variety of IT resources, including computers, networks, software, and access accounts, for use by students, administration, faculty and staff. These resources are administered by Information Technology Services & the Department of Administrative Computing and are intended for the legitimate business of the college.

Since the IT resources at TVCC are not unlimited, the college may give priority for resources to certain users or certain groups of users in support of its mission. Consistent with the College's anti-discrimination policy, the use of IT resources should not be denied or abridged because of race, sex, religion, national origin, age, disability, or marital status.

The College's general policies for academic freedom and for responsible, considerate, legal, and ethical behavior must extend to use of IT resources. Use of the TVCC network and the Internet is a privilege, not a right. To maintain this privilege, users of the College's IT resources are responsible for following both the letter and the spirit of this acceptable use policy.

The purpose of the Acceptable Use Policy is to establish procedures and guidelines concerning the acceptable use of Information Technology (IT) resources throughout all Trinity Valley Community College (TVCC) campuses.

2.0 Purpose

The acceptable use policy is to ensure that all IT resources are used in support of TVCC's mission statement.

3.0 Policies

3.1. GENERAL USE

The IT resources at Trinity Valley Community College are property of the college, and as such are subject to the policies outlined for general use of facilities, services and equipment. In addition, the following guidelines should be observed:

Each authorized user will be responsible for his/her use of the IT resources.

- Computer equipment shall not be relocated without notification and approval. Use Property Disposition forms to obtain necessary approval.
- Computer equipment shall not be left unattended while signed on to the LAN and/or mainframe. Each user must protect all resources by signing off the system or locking their equipment/office while unattended.
- Users with IT access accounts are responsible for all use of the accounts. All accounts (logins) are for the use of a single individual, the person for whom the account was approved. Sharing or loaning accounts is strictly prohibited. If users need to share

microcomputer resident data, they should utilize message-forwarding capabilities or shared directories on LAN servers.

- Employee's assigned logins shall not give their password to anyone. To prevent unauthorized parties from obtaining access to electronic communications, users must choose passwords that are difficult to guess (not a dictionary word, not a personal detail, and not a reflection of work activities). Numeric, alphabetic and "special" characters should be used in combination to increase the difficulty of intrusion.
- Users must not attempt to undermine the security or the integrity of computing systems or networks and must not attempt to gain unauthorized access. Users may not use any computer program or device to intercept or decode passwords or similar access control information. If security gaps are observed, they should be reported to IT Services immediately.
- The IT resources of the College may not be used to impersonate another person or misrepresent authorization to act on behalf of others or the College.
- The IT resources of the College may not be used to harass another person. Users should not transmit to others or display images, sounds, or messages that might be perceived by a reasonable person as, or have been identified as harassing. (See the College policies on sexual harassment and the student conduct codes.)
- IT resources may not be used to invade the privacy of others or make unauthorized use of their work. Users should not attempt to read or copy files belonging to others, or decrypt or translate encrypted material, unless the files have deliberately been made accessible by the owner(s) or authorization has been obtained to do so.
- Users should not intentionally damage or disable computer systems, networks, or software without authorization for any purpose. The College will take reasonable steps to ensure its IT resources are free of deliberately destructive software, such as viruses. Individuals must share responsibility for protecting college computers, and should ensure the integrity of any electronic media they introduce.
- Computer users must observe and comply with Federal, State, and local laws governing computer and information technology, and all college rules and regulations.
- The IT resources of the College may not be used for personal financial gain or commercial purposes.
- Occasional, incidental personal use of IT resources is permitted except when such use interferes with the performance of the user's job or results in significant cost or burden to the College. This does not preclude additional limits on personal use of equipment as may be determined by individual departments in accordance with normal supervisory procedures.
- The College reserves the right to approve all software prior to installation on any College computer and the right to remove any software determined to be detrimental to productivity.
- The College reserves the right to approve any personal IT equipment before connection to the TVCC network and to remove any equipment determined to be detrimental to the network.

3.2. Sharing of Accounts Prohibited

As a result of enrolling or being employed by the college, certain computing resources may be made available for your use. The college manages access to its limited computing resources by requiring that users identify their accounts with a unique personal user name and a secret password they obtained. Sharing a user account with others is prohibited; i.e., authorization to use college computing resources is not shareable or transferable.

Information Technology Services staff members are pleased to assist you in getting properly authorized to access the resources you need. We are also prepared to discuss alternative service providers with you if you are not eligible to access computing resources at the college.

Unauthorized use or misuse of TVCC computing resources may constitute theft of services, and may be criminally punishable. Violators may also be civilly liable for the value of the stolen resources.

3.3. Interference with Computer Use or Operations

Efforts to interfere with the use or operation of computing or networking resources are prohibited. These include:

- unauthorized use of any resources
- distribution of computer viruses, worms, trojan horse programs, email "bombs," chain letters, etc.
- actions that result in the denial of service to other users by triggering system security features, or intentionally misconfiguring equipment to render it unusable
- forged or counterfeited email messages
- posting USENET News articles to inappropriate newsgroups, posting to moderated newsgroups without the approval of the moderator, or cross-posting articles to many newsgroups simultaneously ("spamming")
- interference with the use of microcomputers, X terminals, or other workstations by the unauthorized display of output on such devices without the assent of the individual currently using the device

We ask that you cooperate with system administrators if you are advised of potential security problems associated with your account or system.

3.4. Recognition of Copyrights

Trinity Valley Community College respects copyright laws and insists that its students, administration, faculty, and staff do likewise. Copying proprietary software is theft, and will not be tolerated at TVCC. Illegally copied software subjects the college to risk of litigation, and denies software authors the compensation they deserve. Moreover, use of such software could result in your suspension or dismissal from the college, and either criminal prosecution or a civil suit for copyright infringement, or both.

Similarly, if you make materials available for others to retrieve or use (via a World Wide Web server, postings to a USENET newsgroup, etc.), be sure to respect their copyrights. In general, every document, image, or sound is copy written upon creation, and may only be used or redistributed with the permission of the copyright holder.