Davis Technical College
Network Resources Acceptable Use Policy

Effective Date: 27 June 2019
Board Approval: 22 February 2007
Revised Board Approval: 28 March 2013
Revised President's Council Approval: 23 April 2018
Revised Board Approval: 28 June 2018
Revised: 6 June 2019
Revised President's Council Approval: 17 June 2019
Revised Board Approval: 27 June 2019

1. Purpose

The Davis Technical College (College) establishes this Network Resources Acceptable Use Policy to ensure that all employees consistently support the purpose, goal, and mission of the College through their appropriate use of College network resources. Additionally, the policy seeks to protect the College network resources from damage and undue wear caused by inappropriate use or harsh treatment. The College encourages, in both implementation and spirit, the pursuit of improved training utilizing network resources in its open network structure.

However, it is important to recognize that with increased access to computerized information, access to controversial material may increase, which may contradict the educational purpose of the College. While some internet sites information accessed via College network resources may contain material that is illegal, defamatory, offensive or inaccurate, neither the Utah System of Technical Colleges nor the College have control of such information.

Further, the College Administration recognizes the importance of each individual's judgment regarding appropriate conduct in maintaining a quality resource system. In addition, 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 definitions and guidelines:

2. Definitions

2.1. Authorized personal use is defined as use by a College employee who is authorized to use College property as part of fulfilling the employee's regular job duties on a personal basis.

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

2.3. Inappropriate use is defined as a violation of the intended use of College network resources.

2.4. Political lobbying is defined as activities on behalf of a particular party or candidate.

2.5. Network resource is any computing device connected or has the potential to connect to College wiring or wireless infrastructure.

2.6. Malware or Malicious Software is software designed to infiltrate or damage a computer system without the owner's informed consent.

2.7. Social Media is a category of internet-based resources that enable the user to generate content and encourage other user participation. This includes all means of communicating or posting information or content of any sort on the internet. Common social media networking sites includes, but not limited to, Facebook, Myspace, LinkedIn, Twitter, YouTube, Wikipedia, Pinterest, blogs, chat rooms, virtual worlds, and other such sites.

2.8. Trojan Horse is a computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

2.9. A worm is a computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively.

2.10. A port scan is a series of messages sent by someone attempting to break into a computer to learn which computer network services, each associated with a "well-known" port number, the computer provides. Port scanning, a favorite approach of computer cracker, gives the assailant an idea where to probe for weaknesses. Essentially, a port scan consists of sending a message to each port, one at a time. The kind of response received indicates whether the port is used and can therefore be probed for weakness.

2.11. A Honeypot is a program that simulates one or more network services that you designate on your computer's ports. An attacker assumes you are running vulnerable services that can be used to break into the machine. A honeypot can be used to log access attempts to those ports including the attacker's keystrokes. This could give you advanced warning of a more concerted attack.

2.12. Spam is electronic junk mail or junk newsgroup postings.

3. Policy

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

3.1. System and Network Activities

The following activities are strictly prohibited, with no exceptions:

3.1.1. Any use for financial gain;

3.1.2. Any use for product advertisement or political lobbying

3.1.3. Violations of the rights of any person or company 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 Davis Tech.

3.1.4. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Davis Tech or the end user does not have an active license is strictly prohibited.

3.1.5. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

3.1.6. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

3.1.7. 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.

3.1.8. Using a Davis Tech computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

3.1.9. Making fraudulent offers of products, items, or services originating from any Davis Tech account.

3.1.10. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

3.1.11. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. 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 for malicious purposes.

3.1.12. Port scanning or security scanning is expressly prohibited.

3.1.13. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

3.1.14. Circumventing user authentication or security of any host, network or account.

3.1.15. Introducing honeypots, honeynets, or similar technology on the Davis Tech network.

3.1.16. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack). 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.

3.2. Email and Communication Activities

3.2.1. 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).

3.2.2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

3.2.3. Unauthorized use, or forging, of email header information.

3.2.4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

3.2.5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

3.2.6. Use of unsolicited email originating from within Davis Tech's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Davis Tech or connected via Davis Tech's network.

3.2.7. Posting the same or similar non-business-related messages to large numbers of newsgroups (newsgroup spam).

3.3. Blogging and Social Media

3.3.1. Blogging by employees, whether using Davis Tech’s property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Davis Tech’s systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Davis Tech’s policy, is not detrimental to Davis Tech’s best interests, and does not interfere with an employee's regular work duties. Blogging from Davis Tech’s systems is also subject to monitoring.

3.3.2. Employees are prohibited from revealing any Davis Tech confidential or proprietary information, trade secrets.

3.3.3. Employees shall not engage in any blogging or social media posts that may harm or tarnish the image, reputation and/or goodwill of Davis Tech and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing.

3.3.4. Employees may also not attribute personal statements, opinions or beliefs to Davis Tech when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Davis Tech. Employees assume any and all risk associated with blogging.

3.3.5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Davis Tech's trademarks, logos and any other Davis Tech intellectual property may also not be used in connection with any blogging activity.

3.4. Privacy of Information - Great care is taken by the College Information Technology Department to ensure the right of privacy of users. However, all communications and information accessible via the College network should be assumed College property and are subject to review and inspection by the College network administrator as governed by applicable federal and state laws and College policy. College property includes employee e-mails. Employees should expect that nothing delivered or received via e-mail is private, and should understand that the College is obligated to disclose e-mail messages to law enforcement or other authorized personnel without prior notice. Caution should be taken by employees not to engage in prohibited e-mail activity including illegal messaging, electronic chain letters, and mailbox contents which consume inordinate amounts of system resources.

3.5. Use of College Owned Computer Equipment - Employees are expected to use College-owned equipment primarily for official business in connection with their jobs. College policy also allows College-owned equipment to be used for incidental personal use. However, the use or possession of College-owned equipment must substantially outweigh the personal benefit derived by the employee from the incidental use. Additionally, network 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 by unauthorized persons.

3.5.1. 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 employee. Additionally, employees will be held accountable for any wear or damage caused by use of the equipment for non-approved or inappropriate purposes.

3.5.2. All employees must sign an agreement to comply with this policy before using any computing equipment or given any access to College network resources. All employees must be given ample opportunities to review this policy and are to understand that use of College network resources constitute an agreement to be bound by this policy.

3.6. Policy Consent and Infractions - In the event that the Information Technology Services Department suspects or detects an infraction of this policy, they will report findings to Human Resources for further investigation and/or appropriate action.

3.7. Infractions - In the case of infractions of this policy, notice is provided through individual notification or, if necessary, through the disabling of an account, which provides an opportunity to discuss this action and violations with the appropriate system administrator and Human Resources. A determination is then followed by the appropriate suspension or revocation of any or all network privileges and/or disciplinary action.

3.8. Telecommunication System - The College telecommunication equipment is provided to conduct official College business and the use of telecommunication resources for personal use should be kept to a minimum.

3.9. Authorization and Installation of Software - Information Technology Services Department is responsible for ensuring compatibility between software applications used at the College. Therefore, it is recommended that College employees notify and receive consent from IT when installing software applications to reduce incompatibility issues and possible associated downtime. Installation of personal copies of software by College employees is discouraged due to possible licensing infringements. This policy is intended to ensure compliance with software licensing obligations and also to safeguard against avoidable introduction of computer viruses, as well as to avoid unnecessary potential overloading of memory and hard disc storage capacity of College owned equipment.

3.9.1. Prohibition on Copying College installed Software - Under no circumstances may unauthorized employees copy College owned software for installation on personal or any other computer equipment. In some cases, College employees 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 Departmental Manager, related College owned software may be installed on the College employees' personal computer equipment, but only by Information Technology staff members. An inventory of College owned software installed on College employees' personal PCs will be maintained, and the software will be deleted and the deletions verified when an employee terminates employment with the College.

3.10. Internet Access and Use - College employees are expected to exercise sound judgment in limiting their use of this feature primarily to official College-related purposes, and to incidental and off-duty personal uses appropriate to standards of ethical behavior. College employees with off-premises access to the Internet are required to safeguard against its use by unauthorized persons. Information Technology staff will monitor and periodically check the sites addressed using College Internet access.