Davis Applied Technology College: A Utah College of Applied Technology Campus Network Resources Acceptable Use Policy

1. Purpose

The Davis Applied Technology College: a Utah College of Applied Technology Campus (College Campus) establishes this Network Resources Acceptable Use Policy to ensure that all employees consistently support the purpose, goal, and mission of the College Campus through their appropriate use of College network resources. Additionally, the policy seeks to protect the College Campus network resources from damage and undue wear caused by inappropriate use or harsh treatment. The College Campus 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 Campus. While some internet sites information accessed via College Campus network resources may contain material that is illegal, defamatory, offensive or inaccurate, neither the UCAT, the Utah State Board of Regents, nor does the College Campus have control of such information.

Further, the College Campus 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. Financial gain is defined as gain derived from any activity recognized under current U.S. Tax Code as qualifying as a business.

2.2. Illegal activities are defined as a violation of local, state, and/or federal laws.

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

2.4. Objectionable is defined as materials that are identified as such by the rules and policies of the Utah State Board of Regents that relate to curriculum materials and text book adoption.

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

2.6. 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.

2.7. File Sharing uses P2P technology to swap copyrighted files, which potentially violates copyright law.

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

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

2.10. Social Media. 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.

3. **Policy**

3.1. The following uses are prohibited:
3.1.1. Any use for financial gain;
3.1.2. Any use for product advertisement or political lobbying;
3.1.3. Any use which shall serve to disrupt the use of the network by other users.
3.1.4. Any File Sharing or P2P file sharing allowing computing devices to upload/download information from any other computing device violating copyright infringement.
3.1.5. Any use of the College Campus network resources for illegal or inappropriate purposes or to access materials that are objectionable in an Applied Technology Education environment, or in support of such activities, material or communication that is deemed to be offensive, such as pornographic or sexually explicit material, in the opinion of a reasonable person in an educational setting, is also prohibited.
3.1.6. Access private, protected or controlled records regardless of the electronic form without management authorization;
3.1.7. Divulge or make known his/her own password(s) to another person;
3.1.8. Distribute offensive, disparaging or harassing statements including those that might incite violence or that are based on race, national origin, sex, sexual orientation, age, disability or political or religious beliefs;
3.1.9. Use College-provided IT resources to violate any local, state, or federal law;
3.1.10. Represent oneself as someone else including either a fictional or real person;
3.1.11. Knowingly or recklessly spread computer viruses, including acting in a way that effectively opens file types known to spread computer viruses particularly from unknown sources or from sources from which the file would not be reasonably expected to be connected with;

3.2. Network Monitoring - Mechanisms to monitor and control computer and network access will be implemented, maintained and monitored by the Information Technology Department.

3.3. Authorized Network Use - Only the authorized owner of the account shall use the College Campus network resource accounts. Account owners are ultimately responsible for all activity under their account. Employees are required to change their passwords every 60 days.

3.4. Network Access Time - Excessive and open-ended use of the network in terms of access time cannot be accommodated due to cost. Employees are encouraged to apply good judgment and mutual consideration in the exercise of their rights as users of this shared resource.

3.5. Privacy of Information - Great care is taken by the College Campus Information Technology Department to ensure the right of privacy of users. However, all communications and information accessible via the College Campus network should be assumed to be College Campus property and are subject to review and inspection by the College Campus network administrator as governed by applicable federal and state laws and College Campus policy. College Campus property includes employee e-mails. Employees should expect that nothing delivered or received via e-mail is private, and should understand that the College Campus 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.

3.6. Use of College Campus-Owned Computer Equipment - Employees are expected to use College Campus-owned equipment primarily for official business in connection with their jobs. College Campus policy does not prohibit incidental personal use of the equipment. However, 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.

3.6.1. 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.

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

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

3.8. Infractions and Due Process - In the case of infractions of this policy, notice and hearing 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. As with other College Campus policies, rights of appeal or grievance are provided as appropriate. A determination is then followed by the appropriate suspension or revocation of any or all network privileges and/or disciplinary action.

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

3.10. Authorization and Installation of Software - Information Technology Department is responsible for ensuring compatibility between software applications used at the College. Therefore, it is recommended that College Campus 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 Campus 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 Campus-owned equipment.

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

3.11. Internet Access and Use - On a need to have basis, Information Technology will activate access to the Internet. College Campus employees are expected to exercise sound judgment in limiting their use of this feature primarily to official College Campus-related purposes, and to incidental and off-duty personal uses appropriate to standards of ethical behavior. College Campus 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 Campus Internet access.

3.12. Social Media - College Campus employees are free to express themselves as private citizens on social media sites to the degree that their speech does not impair or impede their performance as employees. Employees are expected to be aware of and comply with any laws relevant to social media such as copyright, fair use, intellectual property, right to privacy, slander, defamation, and libel. Harassment, bullying, discrimination, or retaliation that would not be permissible in the workplace is not permissible between co-workers online, even if it is done outside of work hours, using personal computers or devices. The College Campus shall investigate and address known violations of established policy.