Davis Technical College
Responsible Use Policy

Effective Date: 18 May 2023

1. Purpose

Davis Technical College provides Users with access to Information Technology (IT) Resources. Access to College IT Resources advances the College's mission to provide instruction, public service, and administrative activities. The Responsible Use Policy (RUP) provides guidance for using College IT Resources and describes what Users agree to do and not do when using College IT Resources. The policy outlines action the College may take to perform College business and to protect College IT Resources, other College property, and Users.

2. Scope

The RUP applies to all Users and any device utilizing College IT Resources. All Users agree to comply with the RUP. At least each year, Users are required to review and accept the RUP and are responsible for maintaining an understanding of its current terms. The current version of the RUP is available in the College's Policy and Procedures Manual and electronically at www.davistech.edu.
In addition to the RUP, all Users of College IT Resources agree to abide by the Policies and regulations contained in applicable College handbooks, syllabi, guidelines and policy and procedure manuals, as well as the laws of the State of Utah and of the United States of America. We remind Users that state and federal laws apply to the use of campus networks and the Internet, including but not limited to those dealing with:

- copyright infringement
- defamation
- discrimination
- fraud
- harassment
- identity theft
- obscene materials
- records retention

3. Definitions

3.1 Automated Monitoring - Service or function of an autonomous monitoring tool that correlates and analyzes audit logs and alerts across multiple security technologies.
3.2 Electronic Resource - Any resource used for electronic communication, including but not limited to internet, Email, and social media.
3.3 Email - A means for exchanging digital messages between two parties sent via any electronic means.
3.4 Illegal Behavior - Any activity that it prohibited by local, state, or federal law or regulations
3.5 Information Asset - Data or knowledge stored in any electronic manner and recognized as having value for the purpose of enabling College to perform its business functions.
3.6 Information System - An Application or group of Servers used for the electronic storage, processing, or transmitting of any College data or Information Asset.
3.7 IT Resources - A Server, Workstation, Mobile Device, networking device, web camera or other monitoring device, or other device/resource that is a) owned by the College or used to conduct College business regardless of ownership; b) connected to the College's network; and/or c) that is creating, accessing, maintaining, or transmitting Information Assets and used for electronic storage, processing or transmitting of any data or information.
3.8 Reasonable Suspicion - A legal term used to describe a set of circumstances that indicate the basis for taking some action in connection with an individual. in order to qualify as "reasonable", the suspicion must be tied to a particular employee rather than a group of employees, and the suspicion must be based on specific and articulable facts, along with rational inferences taken from those facts.
3.9 Signature-based Detection - Identifying potential incidents by matching each input event against defined patterns that model malicious activity, and executing actions based on Policies defined in the detection system. Signature-based detection systems are tuned to identify attacks with a level of accuracy that reduces the occurrence of false positive results.
3.10 User - Any person, including students, staff, faculty, permanent and temporary employees, contractors, vendors, and third-party agents, who accesses any College Electronic Resources, Information Systems,

and/or IT Resources.

3.11 Electronic Communication - Digital correspondence, including, but not limited to email, text-messaging, instant messaging, and social networks.

4. Policy

4.1. The College has the right to monitor and audit any email communications and electronic files received, sent, or created by employees, faculty, staff, students and other Users of IT Resources, Information Systems and Electronic Resources.

4.2. The College reserves the right to limit or restrict the use of IT Resources based on business reasons, technical priorities, and financial considerations, as well as when it is presented with reasonable suspicion of a violation of College policies, contractual agreements, or local, state, federal or applicable international laws and regulations.

4.3. The College monitors and reviews activities and content on its IT Resources utilizing Signature-based Detection and Automated Monitoring for the purposes of efficiency, security, and operations.

4.4. The College further reserves the right to monitor, review and access material stored on, processed, or transmitted through its IT Resources at any time based on reasonable suspicion of Illegal Behavior. The College also reserves the right to access, monitor, and review information on IT Resources for business operations purposes in the case of a User who is unable to perform College duties due to medical illness or emergency, unavailability, or refusal to perform duties.

4.5. Authorized Use

4.5.1. Authorized Users

4.5.1.1. An authorized User is any individual who has been granted authority by the College to access its IT Resources.

4.5.1.2. Unauthorized use is strictly prohibited.

4.5.1.3. If a User ceases being authorized to use College IT Resources or if such User is assigned a new position and responsibilities, any use for which that User is not specifically authorized in their new position or circumstances shall cease. A User must not engage in unauthorized use even if the User is mistakenly granted access to or unintentionally permitted to maintain IT Resources.

4.5.2. Personal Use

4.5.2.1. The College allows Users to make reasonable and limited personal use of its IT Resources to the extent that such use does not interfere with College duties. Individuals using the College's IT Resources for personal business, political campaigning, or other commercial purposes must disclaim a connection between their activities and the College. The College reserves the right to prohibit personal use at any time without prior notice when there is reasonable suspicion of Illegal Behavior, or a violation of College regulation has occurred or is occurring.

4.5.2.2. Authorized Users are responsible for exercising good judgment regarding the reasonableness of personal use, but College management reserves the right to define and approve what constitutes reasonable personal use. Prior use of College Information Systems, Information Assets, and Electronic Resources for personal use does not constitute approval. Personal use of College Information Systems, Information Assets, and Electronic Resources must not interfere with work

performance or with the College's ability to use its resources for business purposes. Personal use must not violate polices, statutes, contractual obligations, or other standards of acceptable behavior. All personal use must be consistent with College regulation. Violation may result in disciplinary action against a College employee or other reasonable action may occur against other Users.

4.5.3. Email Use

Information that is classified as Restricted should not be sent via Email, regardless of the recipient, without an approved business need and applicable technical controls. The use of encryption is required for Emails containing Restricted data sent to any non-College Email recipient as per the Data Classification and Encryption Policy.

4.5.4. Social Media Use

Users are prohibited from posting on behalf of the College to public newsgroups, websites, blogs, social media or other public media sites without prior management approval. Any social media postings that could reasonably be construed as being on behalf of the College must contain a disclaimer stating that the opinions expressed are strictly the User's own and not necessarily those of the College unless the User is authorized to post on behalf of the College.

4.5.5. Cloud Provider Use

Information that is classified as Restricted should not be stored with a cloud provider unless there is a contractual agreement in place between the College and the cloud service provider that **protects the confidentiality of the information and data.**

4.6. Responsible Use

4.6.1. Protecting College Assets

All College employees are entrusted with protecting the property, equipment, and other assets of the College.

Misuse of assets takes many forms and can involve some deception or misrepresentation of facts and information for personal gain as well as deliberate appropriation of property or funds for personal use.

4.6.2. Ethical Use

4.6.2.1. Computing Resources

The College provides resources to support the work of faculty, staff, and students. Users of the College’s resources (including computer networks, telecommunication systems, electronic and magnetically stored information) must know and adhere to College policies.

4.6.2.2. Computing Resources Restrictions

Authorized persons may use College resources for purposes related to instruction, coursework, and administration. The resources are not to be used for commercial use or reselling of network services if it is not directly related to the College’s mission. The College computing and network facilities may not be used for improper or illegal purposes, such as unauthorized use of licensed software, intent to breach security, sending chain letters, and introduction of computer viruses/malware. Individuals are responsible for protecting assigned access codes, passwords, and

other authentication data and not sharing credentials and passwords with other Users, contractors, or vendors.

4.6.2.3. Telecommunications

The College telecommunications system is provided to conduct official business. Use of these resources for personal business or pleasure should be kept to a minimum. Any personal toll charges should be paid by the individual to the College.

4.6.2.4. Email

Users should separate personal email communications from official College email communications and create their own personal email account, solely managed by the employee.

4.6.3. Protection of Confidential Information

All Users must maintain the protection of the College's Confidential Information Assets. This requires Users to exercise precautions that include complying with College regulation and taking other precautions to guard Confidential data.

4.6.4. Illegal Activities

Under no circumstances are Users authorized to engage in Illegal Behavior while using College IT Resources, Information Systems, Information Assets, and Electronic Resources.

4.6.5. Forgery of Communications

Altering electronic communications to hide identity or impersonate another person is considered forgery and is prohibited.

4.6.6. Soliciting Business

Users must not use College IT Resources for soliciting business, selling products, or otherwise engaging in commercial activities other than those expressly permitted by College management or other College regulation.

4.6.7. Fraud

Users must not use College IT Resources to make fraudulent offers for products, items, or services, or make statements about warranty, expressly or implied.

4.6.8. Bandwidth and Overuse

Excessive use of the College's network bandwidth or other Electronic Resources is not permitted.

Large file downloads or other bandwidth-intensive tasks that may degrade network capacity or performance should be performed during times of low College-wide usage.

4.7. Internet Use

4.7.1. Risk of Use

4.7.1.1. Users access the Internet with College facilities at their own risk.

4.7.1.2. The College is not responsible for material viewed, downloaded, or received by Users via the internet. Responsible attitudes and appropriate behavior are essential in using this resource.

4.7.1.3. To protect personal safety and privacy, Internet Users should not give out personal information to others on public resources, without taking into consideration the risks of doing so.

4.7.2. Internet Web Browsing

4.7.2.1. Personal use of College systems to access the Internet is permitted during, before, and after business hours, if such use follows pertinent policies and guidelines and does not have an adverse effect on the College, its customers, or on the User's job performance.

4.7.2.2. All web browsing will be filtered, and certain content will be prohibited if it is objectionable in any way to the common User and in accordance with state and federal laws.

4.8. Privacy Expectations

4.8.1. Monitoring

4.8.1.1. The College's Information Security Office employees' signature-based and automated monitoring activities to ensure compliance with federal, state, and College regulations.

4.8.1.2. The College reserves the right to authorize specific individuals or groups, at times including contracted business partners, to utilize signature-based and automated monitoring activities to monitor IT Resources to ensure compliance with federal, state, and College regulations.

4.8.2. Privacy of Stored Personal Information and Electronic Communications

College Users have diminished expectations of privacy for any personal information stored on or sent or received utilizing College-owned IT Resources.

4.8.3. User Authentication

All College client networks must require Users to authenticate via password or other secure authentication mechanisms which allows Users to be uniquely identified.

Approvals
4.10.2023 Expanded President's Council