MID-STATE TECHNICAL COLLEGE

ADMINISTRATIVE POLICY

Policy Section: ADMINISTRATION

Policy Title: Employee use of College Digital Mediums

To remain competitive and provide employees the best tools to do their jobs, Mid-State Technical College continues to adopt and make use of new digital assets for information exchange and communication. The following are considered digital mediums for purposes of this policy, and may be revised by the College at any time: services such as digital and social media, voice mail, internet, intranet, wire, external electronic digital bulletin boards and online services and devices such as computers, printers, e-mail, telephones, cell phones, video conference equipment, and fax machines, and the like. This is not an all inclusive list.,

The College encourages the use of these mediums because they can make legitimate college information exchange and communication more efficient and effective. However, all employees and everyone connected with the organization should remember that digital mediums are the property and facilities of the College and are a privilege provided by the College to people affiliated with the college to support employment consistent with business objectives and to promote the interests of the College.

These mediums and associated services can also introduce a security threat to the network and liability to the college, therefore, the purpose of this policy is to ensure protection of the physical and logical integrity of these valuable college resources, reduce the risk of security incidents, and prohibit and prevent either intentional or negligent activities facilitated by any digital communications which:

- Are unlawful.
- Are contrary to principles of the equality of persons.
- Tend to create or increase any liability for the College.
- Interfere with the efficient operation of the College or its communication systems.
- May give the impression that unauthorized statements made by individuals associated with the College are official statements of the College.
- Violate any college policy.
- Are likely to compromise the security, availability, utility, integrity, authenticity or confidentiality of any college data, electronic mediums and/or services.
- Interfere with or are likely to interfere with an employee's work.
- Adversely affect or have the potential to adversely affect the mission or reputation of the College or the efficiency, morale or safety of college students, guests, employees, customers, affiliates or vendors.

The procedures in this policy apply to all digital mediums that are:

- Accessed on or from college premises and/or from the employee's personal devices while participating in college business.
- Accessed using college computer equipment or via college-paid access methods.
- Used in a manner that identifies the individual, references the College, its business, educational offerings, services, products, students, guests, employees, customers, affiliates or vendors.

While no policy can cover all potential issues and circumstances. If any employee has any question or concern about the application of this policy or any action taken or to be taken the employee should consult with the Vice President, Human Resources.

ENCOURAGED DIGITAL MEDIUM USE

The College encourages use of digital mediums to advance the college mission. Use should be consistent with the Core Values and reflect positively on the college. It is the responsibility of the employee to ensure copyright and trademark protections are not infringed upon, for clarification on using this content please contact the Employee Development Center (EDC) or Marketing for guidance**.**

The list below is intended to provide examples of prohibited activities which are contrary to such policy and purposes and is not all-inclusive:

- Discriminating, harassing, insulting, or attacking others based on race, national origin, sex, sexual orientation, age, religion, disability or any other legally protected class.
- Derogatory to any individual or group.
- Obscene, sexually oriented, or pornographic (Note: Any child pornography is a violation of law and will be reported to the appropriate authorities).
- Defamatory or threatening.
- Otherwise unlawful.
- Responding to and participating in Internet discussion groups, any social media sites, digital comment pages, and the like from Mid-State devices in any manner inconsistent with this policy.
- Conducting personal job searches outside Mid-State Technical College.
- Accessing, saving, and/or disseminating unauthorized, confidential, or proprietary documents or information.
- Accessing, saving, and/or disseminating, including printing, copyrighted materials (articles, software, etc.) in violation of copyright laws.
- Accessing, saving, and/or disseminating false, damaging, defamatory or misleading information.
- Operating a business or conducting any activity for personal gain.
- Conducting or participating in solicitations or promotions related to commercial ventures, religious or political causes, or solicitations or promotions other than those specifically approved by the Executive Committee.
- Theft, accessing, copying, or saving electronic files without permission.
- Communicating on another's or the College's behalf without consent or authorization.
- Unauthorized access to data or data restricted by government laws and regulations.

- Engaging in communications for any purpose that is illegal or contrary to the College's policy or interests.
- Using college communication or computer facilities to gain unauthorized access to data or electronic systems, whether internal or external to the College.
- Use of another person's password or identity.

- Flooding college system(s) with numerous or large messages.
- Bomb threats.

INCIDENTAL PERSONAL USE

Digital mediums are provided by the College primarily for authorized employees' college related use. Limited, occasional, or incidental use of electronic mediums (sending or receiving) for personal, non-college purposes is permitted except as specified in this policy. Employees are expected to demonstrate discretion when incidentally using the College mediums and services and must avoid:

- Prohibited activities
- Interference with the productivity of the employee or other employees.
- Consuming significant system resources or storage capacity.
- Transferring of large file or depletion of system resources available for college purposes.
- Costs to the College or increased risk and/or liability to the College.

MONITORING OF EMPLOYEE COMMUNICATION

The College reserves the right, at its discretion, to review any employee's electronic files, messages, and utilization to the fullest extent necessary to maintain the integrity of the system; provide regular service and optimum technical management of information resources; and ensure electronic mediums and services are being used in compliance with the law, this policy, and other college policies. In addition, such files, messages, or utilization become public via the discovery process in connection with legal actions brought against the College.

The College may intercept, monitor, copy, review, and download any employee communications or files created or maintained on these systems and all such files remain the property of Mid-State. As this information is not confidential, an employee should have no expectation of privacy. Employee access to electronic mediums may be denied at any time at the option of the College.

SECURITY/APPROPRIATE USE

Employees must respect the confidentiality of other individuals' electronic communications. Unauthorized employees are prohibited from engaging in, or attempting to engage in certain activities including, but not limited to:

- Monitoring or intercepting the files or electronic communications of other employees or third parties.
- Downloading or installing unauthorized software.
- Hacking or obtaining access to systems or accounts they are not authorized to use.
- Disabling college anti-virus or malware software.
- Using someone else's logins or passwords.
- Breaching, testing, or monitoring computer or network security measures.

Employees must immediately report any theft or loss of college electronic equipment (laptop, phone, etc.) and any suspected malware, ransomware or other suspected cyberware so that appropriate security measures can be taken.

CLEAR SCREEN

In order to protect information that has been entrusted to the College by employees, students, and the community, we promote a clear screen approach. Unattended computers must be locked or logged out.

EMAIL COMMUNICATION

Email is an essential component of business digital communication; Employees should keep the following in mind to help reduce the risk of email-related security incidents:

- Information that is considered confidential or propriety to Mid-State must be properly encrypted regardless of the recipient.
- Large files may occasionally need to be transferred and should be transferred using alternate methods such as Dropbox or WeTransfer.
- Use care when opening email attachments. Viruses, Trojans, and other malware can be easily delivered as an email attachment. Users should never open unexpected email attachments, never open email attachments from unknown senders, and never click links within email messages unless he or she is certain of the link's safety. It is often best to copy and paste the link into your web browser, or retype the URL, as specially formatted emails can hide a malicious URL.
- Unauthorized emailing of Mid-State data, confidential or otherwise, to external email accounts for the purpose of saving this data external to Mid-State systems is prohibited.
- Refer to Mid-State's Data Classification, Storage, Transmission, Retention, Encryption, & Mobile Devices Administrative Policy for additional information on encryption.

PARTICIPATION IN ON-LINE DIGITAL FORUMS FOR COLLEGE BUSINESS

The College utilizes official websites and other digital communication established and maintained by the College including social networking sites to advise the broader community of its educational offerings, services, employment opportunities and to elicit and exchange information pertinent to college business. Employees should remember that any messages or information sent on college-provided communication systems to one or more individuals via an electronic network – for example, internet mailing lists, bulletin boards, and on-line services – are statements identifiable and attributable to the College. Professional care and responsibility should always be exercised; when appropriate content should be identified as not representing Mid-State's views or positions.

Any college employee or other college representative engaging in online posting or digital dialogue as a designated College official is required to meet the following standards:

- Must limit their discussion to matters of fact and avoid expressing opinions while using the College's systems or a college-provided account.
- Disclose their employment or association with the College (e.g.,RLoggins@mstc.edu) in all communications when speaking on behalf of the College.
- Do not knowingly communicate information that is untrue or deceptive. Communications should be based on current, accurate, complete and relevant data.
- Do not conduct activities that are illegal or contrary to college policies.
- Maintain the confidentiality of information considered confidential.

Mid-State reserves the right to hide, block, or remove content of any post that violates these guidelines and the college policies. Content may be removed at any time without prior notice for any reason to be in the College's best interest. .

PARTICIPATION IN ON-LINE DIGITAL FORUMS FOR PERSONAL NETWORKING

Employees may maintain or participate in personal blogs, personal websites, bulletin boards, or other interactive web media, including postings on LinkedIn, Facebook, Instagram, MySpace, Twitter, YouTube, SnapChat, Reddit, TikTok and the like (herein collectively referred to as "blogs") either on or off college time or equipment. When employees publish information or opinions through a blog, employees are legally responsible for commentary and the posted information. A legal, moral, and ethical responsibility is associated with posting about the College or its employees, students, customers, visitors, affiliates, or vendors. Posts related to any of these may impact the workplace, the quality of the services provided, or the confidence the community, our students, and customers have in the College. Posts should be thoughtful, considerate, and professional. Be respectful of the College, District Board members and Advisory Committee members, other employees, students, customers, affiliates, and vendors.

Employees should not assume that personal blogs are confidential considering other individuals with access may bring these postings to the attention of the College. The following guidelines and considerations apply to personal blogs:

- Blogging or otherwise working on personal postings is prohibited on college time or utilizing college equipment or facilities unless sharing college educational content or college sponsored event content.
- Employees must use discretion when seeking or gaining access to the blog of any student while that student is enrolled in any program or course at the College.
- Managers must use discretion in "friending" or otherwise seeking or gaining access to the blog of any employee that directly reports to them.
- Employees will he held responsible for the release of any legally protected College information posted as part of a personal blog.
- The College will not defend any employee in any legal actions based on commentary or posting on any blog under any circumstances, whether suit is brought by another college employee, student, guest, customer, vendor, or someone who is not affiliated with the College.
- Employees may not post any materials owned by the College or use any college logos or trademarks without advance written authorization. This does not include re-posting college educational content or college sponsored event content.

Adopted: *August 2011*
Last Reviewed: *February 2021*
Last Revised: *February 2021*