

---

**Policy Title: ELECTRONIC COMMUNICATIONS MEDIA**

To remain competitive and give our talented workforce the best tools to do their jobs, Mid-State Technical College continues to adopt and make use of new means of communication and information exchange. This means that many of our employees have access to one or more forms of electronic media and services, including computers, printers, e-mail, telephones, cell phones, voice mail, video conference equipment, fax machines, external electronic bulletin boards, wire services, on-line services, intranet, and the Internet. The College may modify this policy as necessary. This policy does not constitute a contract.

The College encourages the use of these media and associated services because they can make legitimate college communication more efficient and effective. However, all employees and everyone connected with the organization should remember that electronic media, hardware, software, and services provided by the College are the property and facilities of the College. Their purpose is to facilitate and support college business and education consistent with the college mission and vision; however, they can also introduce a security threat to the network. 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 electronic 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 media, 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 following procedures apply to all electronic media and services that are:

- Accessed on or from college premises and/or from the employee's personal computer.

- Accessed using college computer equipment or via college-paid access methods.
- Used in a manner that identifies the individual with the College or references the College, its business, educational offerings, services, products, students, guests, employees, customers, affiliates or vendors.

No policy can cover all of the 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.

### **PROHIBITED COMMUNICATIONS**

Electronic media cannot be used for transmitting, retrieving, displaying, or storing any communication or activity contrary to the purpose for which this policy has been developed, as stated above. The list below is intended to provide examples of communications or activities which are contrary to such policy and purposes, and it is not meant to be all-inclusive and may be modified at any time.

- Sending, saving, forwarding, or displaying information that is contrary to policy, including but not limited to:
  - Discriminating, harassing, insulting, or attacking others based on race, national origin, sex, sexual orientation, age, religion, disability or any other legally protected class.
  - Derogatory or offensive 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.
- Sending chain letters.
- Responding to and participating in Internet discussion groups, any social media sites, www comment pages, and the like from Mid-State computers in any manner inconsistent with this policy.
- Conducting 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.

Policy Section: Administration

Policy Title: Electronic Communications Media

- 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.
- Downloading or sharing music, videos, etc.
- 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**

Electronic media and services are provided by the College primarily for authorized employees' college-related use. Limited, occasional, or incidental use of electronic media (sending or receiving) for personal, non-college purposes is permitted except as specified in this policy. Employees are expected to demonstrate a sense of responsibility and not abuse this privilege.

The College allows limited, occasional, or incidental personal use of its e-mail and/or internet system subject to the following non-inclusive conditions and restrictions:

Personal use must be infrequent, must demonstrate good judgment, and must be in accordance with all policies of the College. Personal use must not:

- Involve any prohibited activity.
- Interfere with the productivity of the employee or other employees.
- Consume significant system resources or storage capacity.
- Involve large file transfers or otherwise deplete system resources available for college purposes.
- Result in any direct cost to the College or expose the College to risks or liability.
- Involve any personal social networking or "blogs" as defined in this policy.

## **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 media 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 communications or files you create or maintain 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 media 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.
- Accessing external e-mail services from within the college network.
- Hacking or obtaining access to systems or accounts they are not authorized to use.
- Disabling college anti-virus software.
- Using someone else's log-ins 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.) so that appropriate security measures can be taken.

## **CLEAR DESK/CLEAR SCREEN**

In order to protect information that has been entrusted to the College by employees, students, and the community, we promote a clear desk and clear screen approach. Unattended computers must be locked or logged out and any print materials or electronic media containing operational or confidential information which is not currently being used must be securely locked away.

## **EMAIL COMMUNICATION**

Email is an essential component of business communication; however, it can introduce a security incident to the network as well as have an effect on Mid-State's liability by creating a written record of

communication. Employees should keep the following in mind to help reduce the risk of email-related security incidents:

- Email is an insecure method of communication, thus information that is considered confidential or propriety to Mid-State may not be sent via email, regardless of the recipient, without proper encryption.
- Email systems were not designed to transfer large files and as such emails should not contain attachments of excessive file size.
- Users should 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.
- Mid-State may use methods to block what it considers to be dangerous emails or strip potentially harmful email attachments as it deems necessary.
- 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.
- Encrypting e-mail messages or attached files sent, stored, or received on the College's e-mail system is *prohibited* except where explicitly authorized. Employees with a college need to encrypt messages should submit a written request to the systems administrators, with a copy sent to their supervisor. Refer to Mid-State's Data Classification, Storage, Transmission, Retention, Encryption, & Mobile Devices Administrative Policy for additional information on encryption.

### **PARTICIPATION IN ON-LINE FORUMS**

The College utilizes official websites and other electronic communication opportunities 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.

The College recognizes that voluntary participation in some professional forums might be important to the performance of an employee's job. Employees who post information on listservs or newsgroups must include the following disclaimer in all of their postings to public forums: *"The views, opinions, and judgments expressed in this message are solely those of the author. The message contents have not been reviewed or approved by Mid-State Technical College."*

Even with a disclaimer, a connection with the College exists and a statement could be imputed legally to the College. Therefore, employees should not rely on disclaimers as a way of insulating the College from the comments and opinions they contribute to forums.

Any college employee or other college representative engaging in online posting or electronic 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 at the discretion of Mid-State page administrators and the Marketing & Communications Department.

### **PERSONAL SOCIAL NETWORKING**

In addition to the foregoing rules on the appropriate use of electronic media, special concerns surround the personal use of social media either on or off college time or equipment. Some employees maintain or participate in personal blogs, personal websites, bulletin boards, or other interactive web media, including postings on LinkedIn, Facebook, MySpace, Twitter, YouTube and the like (herein collectively referred to as "blogs"). When you publish information or your opinions through a blog, you are legally responsible for your commentary and the posted information. 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.
- Employees are prohibited from "friending" or otherwise seeking or gaining access to the blog of any student while that student is enrolled in any program or course at the College. Similarly no employee may offer or give access to their own personal blog to any student while that student

is enrolled in any program or course at the College. The only exception is for a student who is an immediate family member of the employee.

- Managers are prohibited from “friending” or otherwise seeking or gaining access to the blog of any employee that directly reports to them. The only exception is for an employee who is an immediate family member of the supervisor or manager.
- Blogging, even when it occurs during off duty time and on an employee’s own equipment may not interfere with your work, or adversely affect or have the potential to adversely affect the reputation of the College, or the efficiency, morale, or safety of other employees, students, customers, affiliates, or vendors.
- Employees may be personally liable for comments deemed to be defamatory (i.e., making false allegations even if the information is believed to be true).
- Employees will be held responsible for the release of any legally protected information posted from the College as part of a personal blog.
- Employees may also be personally liable for other conduct that is deemed to be tortious (i.e., violate the legal rights of others, such as posting information that invades the privacy rights of other employees, students, individuals, or the College, even if the information posted is true).
- 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.
- Employees must not post anything in violation of the law or college policies including, but not limited to, release of confidential information of the College, its employees, students, customers, or vendors.
- Posting anonymously or under a pseudonym may not protect your identity. Similarly, posting information without naming the person or identifying the situation will not ensure that those who read the post will not be able to identify the person or situation. In addition a “friend” may post a response which otherwise identifies the information you intended to shield.
- 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.

### **COLLEGE PRIVILEGED INFORMATION**

All employees are expected and required to protect the College’s confidential information. College confidential information should never be transmitted or forwarded to outside individuals or recipients not authorized to receive the information. The College also requires its employees to use electronic media in a way that respects the confidential and proprietary information of others. Employees are prohibited

Policy Section: Administration

Policy Title: Electronic Communications Media

from copying or distributing copyrighted material - for example, software, database files, documentation, or articles - using electronic media.

Any questions about whether information is confidential, proprietary, copyrighted, or otherwise appropriate for posting or release should be referred to the Vice President, Human Resources.

**POLICY VIOLATIONS**

Employees violating the College’s electronic communications policy and/or other college policies utilizing electronic communications including personal blogs as defined herein, are subject to revocation of electronic media privileges as well as discipline, up to and including termination to the extent permitted by state and federal law. Employees using the system for defamatory, illegal, or fraudulent purposes and employees who break into unauthorized areas of the College’s electronic media systems are also subject to civil liability and criminal prosecution.

*Adopted: August 2011*  
*Last Reviewed: July 2017*  
*Last Revised: February 2016*