Computer and Network Use

Policy Number: 3.3.101
Reviewed: 12/2013, 11/12/2024
Revised: 11/28/11, 8/31/17, 3/13/19, 9/21, 11/12/2024 pending BOT approval

Purpose

Middle Tennessee School of Anesthesia (MTSA) provides computing, networking, and information services to all students, faculty, and staff. As this system often holds confidential, sensitive, and privileged information, MTSA expects all users to operate and maintain a secure environment, and to protect the system from misuse, unauthorized access, and potential corruption of the network infrastructure.

This policy applies to both school provided and personal devices that have interaction both internally and externally via the MTSA shared network, school provided e-mail accounts, school related software program/app, social media, and internet.

User Rights and Responsibilities

MTSA computers and networks can provide access to resources on and off campus, as well as the ability to communicate with other users worldwide. Such access is a privilege and requires that individual users act responsibly. Users must respect the rights of other users, respect the integrity of the systems and related physical resources, and observe all relevant laws, regulations, and contractual obligations.

Misuse

Users will be held accountable for their conduct under current MTSA policies. Complaints alleging misuse of computing, networking, or information resources may result in the restriction of computing privileges and/or other internal disciplinary actions. Additionally, misuse can be prosecuted under applicable statutes. Reproduction or distribution of copyrighted works, including, but not limited to, images, text, or software, without permission of the owner is an infringement of U.S. Copyright Law and is subject to civil damages and criminal penalties including fines and imprisonment.

Examples of misuse include, but are not limited to, the activities in the following list:

- Using a computer account that you are not authorized to use. Obtaining a password for a computer account without the consent of the account owner.
- Using the Campus Network to gain unauthorized access to any computer systems.
- Knowingly performing an act which will interfere with the normal operation of computers, terminals, peripherals, or networks.
- Knowingly running or installing on any computer system or network, or giving to another user, a program intended to damage or to place excessive load on a computer system or network. This includes but is not limited to programs known as computer viruses, Trojan horses, and worms.
- Attempting to circumvent data protection schemes or uncover security loopholes.
- Violating terms of applicable software licensing agreements or copyright laws.

- Deliberately wasting computing resources.
- Using electronic mail to harass others (see *Computer Based Discrimination/Harassment* below).
- Masking the identity of an account or machine.
- Posting materials on electronic bulletin boards that violate existing laws or the University's codes of conduct.
- Attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner.

To report misuse of MTSA electronic resources, submit written communication to your immediate supervisor or the Director of IT.

Electronic Based Discrimination/Harassment

As per MTSA's *Discrimination/Harassment Policy* "It shall be a violation of this policy for any employee or any student to discriminate against or harass an employee or student through disparaging conduct or communication that is inherently discriminatory". This includes, but is not limited to, discrimination in regards to race, color, sex, age, disability, marital status, full or part-time status, religion, sexual orientation, gender identity, or national origin (see *Nondiscrimination Policy*).

This policy covers employee and student communication using MTSA issued e-mail (sent by or received to), school-based online programs/apps, and all employee and student social media accounts during their tenure when used as a representative of MTSA.

To report the misuse of MTSA electronic resources in relation to possible discrimination/harassment, a complaint may be submitted either orally, in writing, or electronically to the MTSA Title IX Coordinator (titleIXcoordinator@mtsa.edu).

MTSA Shared Network

The MTSA shared network is for staff and faculty use only. Permission to access files on the shared network will be requested for staff and faculty by administration. Requests will be sent to the MTSA IT Department. Requests for access will be approved after consideration of HIPAA and FERPA regulations related to the sharing of privileged information in the requested files (see *Release of Student Record Information* & *Stakeholder's Rights*).

At no time shall the following types of files be stored on the shared network: personal photos, music, videos, files that contain harmful components including malware, spyware, viruses, and/or tracking programs, pornography, or anything deemed harmful or illegal. The MTSA IT Department may access user files as required to protect the integrity of computer systems. For example, following organizational guidelines, IT may access or examine files or accounts that are suspected of unauthorized use or misuse, or that have been corrupted or damaged.

MTSA Issued E-Mail Addresses

MTSA currently issues each staff, faculty, and student an official MTSA e-mail account. This e-mail account is considered the official line of communication between these parties, as well as official MTSA communication outside of the school. This e-mail is not for personal use and is considered the property of MTSA.

This account is kept and maintained by the MTSA IT Department and is not considered a secure e-mail account to send privileged information across unless such attachments are encrypted or password protected.

If there is suspected abuse/neglect of MTSA issued e-mail accounts, MTSA IT can access any MTSA e-mail account with a written request from the Executive Committee and Director of IT to review and retrieve e-mails in relation to the claim. At least one-half of the Executive Committee must approve this request. These e-mails will then be shared with the Executive Committee and Director of IT and may result in disciplinary action by Progressions Committee for students and the Executive Committee for employees.

E-mail accounts converted to Alumni status after a student graduates from MTSA. E-mail accounts will be deleted one (1) week after students are dismissed from the program. Students are responsible for notifying their contacts and carrying their contact list over to a personal e-mail before deletion. No information will be kept from deleted accounts unless an e-mail is preserved as a PDF in the student permanent file.

E-mail accounts will be deleted 90 days after a staff, faculty, or administrative member leaves the employ of MTSA. The departing member is responsible for notifying their contacts and carrying their contact list over to a personal e-mail before deletion.

MTSA Website & Social Media

MTSA has a website (www.mtsa.edu) that is maintained by the Office of Advancement & Alumni. Content to be posted to the website must be submitted to this office.

MTSA maintains school accounts on various social media platforms and will evaluate representation for the school on new platforms as they emerge. These accounts are also maintained by the Office of Advancement & Alumni, as well as the MTSA IT Department.

All policies, procedures, and guidelines regarding university trademarks, names, and symbols apply to the website and social media sites. The Department of Advancement & Alumni can offer guidance about how to properly use names, logos, etc., to resolve branding and copyright/trademark issues in these venues. MTSA does not permit explicit or implied institutional endorsements of any kind through use of its name, trademarks, logos, or images – including pictures of campus buildings.

MTSA does not prescreen content posted by third-person parties to social media sites, but it shall have the right to remove, in its sole discretion, any content that it considers to violate MTSA policies. MTSA does not endorse or take responsibility for content posted by third parties. MTSA, through the Department of Advancement & Alumni, will work to correct inaccuracies on MTSA sites by responding with correct, factual information and including source citations (links, video, contact information, etc.) when appropriate.

Acceptable content may be positive or negative in context to the conversation, regardless of whether it is favorable or unfavorable to MTSA. However, language that is illegal, obscene, defamatory, threatening, infringing of intellectual property rights, invasive of privacy, profane, libelous, harassing, abusive, hateful or embarrassing to any person or entity, or otherwise injurious or objectionable is unacceptable and shall be removed. MTSA will not tolerate content that infringes on proprietary information, or that is defamatory, pornographic, harassing, libelous or inhospitable to a reasonable work environment or not in harmony with the School's mission, vision, and core values.

MTSA AI Use

Artificial Intelligence, Large Language Models, and Machine Learning (hereafter referred to as AI) all rely on user input to generate effective responses. The quality of input is the responsibility of the user and directly impacts the accuracy and quality of any generated response by the AI tools.

Even with effective prompt writing and valid information as context for the prompt, AI can suffer from a phenomenon called "Hallucination." In the context of AI, hallucination is a confident response from an AI tool that is erroneous based on the data and training given to the tool. Therefore, all AI users at MTSA must recognize that the output of AI tools are the sole responsibility of the AI user and should be thoroughly inspected, validated, and vetted to ensure accuracy.

AI can be an effective tool for automation and assist with increasing task efficiency. However, any scripts, automations, alerts, or other functions must have a “procedural time out” to allow the owner of the information an opportunity validate the accuracy of any output before dissemination. An example of an acceptable use would be setting an AI tool to alert you or other members of your team of updates, changes, or tasking without manipulating the information. An unacceptable use would be allowing the AI tool to update someone's calendar based on the example above.

Microsoft Co-Pilot will be the default AI tool at MTSA as part of our Microsoft 365 tenant toolset. All other AI tools that come in contact with MTSA data must be approved based on an assessment by the Ed Tech department to ensure that data security standards are being met by the creators and administrators of the tool in question. A list of approved tools and the conditions of approval (paid subscription level, for example) will be maintained by the Ed Tech department.

Penalties

Abuse or misuse of MTSA computers, network, information services may not only be a violation of this policy or user responsibility, but it may also violate the criminal statutes. Therefore, MTSA will take appropriate action in response to alleged user abuse or misuse claims. Action may include, but not necessarily be limited to:

- suspension or revocation of computing privileges. Access to all computing facilities and systems can, may, or will be denied;
- reimbursement to the School for resources consumed;
- other legal action including action to recover damages;
- referral to law enforcement authorities;
- computer users (faculty, staff and/or students) will be referred to the appropriate office/committee for disciplinary action.

In connection with inquiries into possible abuses or misuse, MTSA reserves the right to examine files, programs, passwords, information, public website/social media posts, printouts or other material without notice.