

Policy #: 524
Title: STUDENT USE OF ELECTRONIC COMMUNICATION AND TECHNOLOGY
Date of Initial Approval: 01-23-2003 (Original)
Revision/Re-authorization Dates: 11-21-2013; 03-24-2016; 02-16-2017; 06-12-2018; 06-27-2019; 09-17-2025
Reviewers: MSA Superintendent, MSA Instructional Leadership Team, and Instructional Technology staff

I. PURPOSE

The Minnesota State Academies (MSA) need to have clear rules about students' use of MSA technology and electronic communication. This policy explains how students at MSA can use technology for learning and communication at MSA, following limits established in different federal and state laws.

II. GENERAL STATEMENT OF POLICY

A. MSA provides a variety of electronic tools for students to assist in their learning activities.

These electronic tools include, but are not limited to, the following:

- Tablets
- Laptop computers
- Assistive Technology Devices (switches, refreshable braille displays, Augmentative and Alternative Communication Devices, etc.)
- Electronic mail (e-mail) systems
- Internet access and apps

B. Students' use of MSA-provided electronic tools is intended for school-related purposes. Students may use those tools for personal purposes from time to time but must follow all school rules about the use of technology in and out of the classrooms. Students are responsible for appropriate use of all MSA devices, apps, and network access.

C. Students may bring personal technology devices (cell phones, tablets, laptops, gaming devices, etc.) to campus. Students must follow all school and dorm rules about using their personal devices and limitations related to the use of the school internet network.

III. MSA RESPONSIBILITIES

A. MSA administrators and staff are responsible for ensuring that students appropriately use all electronic tools by providing training, supervising, coaching, and taking disciplinary action, when necessary.

B. MSA is responsible for establishing internal policies regarding password management, encryption, data practices, monitoring access, records retention, inventory, and the like, and for communicating those policies to students. MSA will ensure that the students understand when and how they can use technology.

C. MSA will cooperate fully with local, state, and federal authorities in any investigation concerning or related to any illegal activity.

IV. STUDENT AND PARENT RESPONSIBILITIES

A. Students are expected to follow all MSA rules and regulations for use of school-provided technology, including computers, other electronic devices, e-mail, and

Internet Access. Students who break the rules will have appropriate consequences as outlined in the student handbook, including possible suspension of their computer/Internet privileges for a period of time.

- B. Even when students are not on our campuses, if they engage in the foregoing unacceptable uses of the Internet may also be in violation of this policy as well as other MSA policies. Students may not use school equipment or network resources to earn money (e.g., monetization of social media accounts, etc.)

Examples of such violations include but are not limited to situations where the MSA technology network system is compromised or if a student is negatively impacted. If MSA receives a report of unacceptable use originating from a non-school computer or resource, MSA may investigate such reports to the best of its ability. Students may be subject to disciplinary action for such conduct, including but not limited to, suspension or cancellation of the use or access to MSA's computer and network system, and discipline under other appropriate MSA policies, including suspension, or expulsion.

- C. Outside of school, parents bear responsibility for the same guidance of Internet use as they exercise with information sources such as television, telephones, radio, movies, and other possibly offensive media.

Parents are responsible for monitoring their student's use of the MSA technology network system and of the Internet if the student is accessing the MSA technology network system from home or a remote location.

Parents will be notified that their students will be using MSA resources/accounts to access the Internet and that MSA will provide parents with the option to request alternative activities not requiring Internet access. This notification should include:

1. A copy of the user notification form provided to the student user.
2. A description of parent/guardian responsibilities.
3. A notification that the parents have the option to request alternative educational activities not requiring Internet access and the material to exercise this option.
4. A statement that the Internet Use Agreement must be signed by the user, the parent or guardian, and the campus director prior to use by the student.
5. A statement that MSA's acceptable use policy is available for parental review.

V. MONITORING

MSA-provided electronic communication devices such as mobile devices, tablets/laptops, e-mail systems and Internet access, any and all software, data, or other information stored on a state-owned device are state property. Like the other state-owned resources, they are intended to be used for school purposes and other MSA-sanctioned activities.

State-owned electronic communication devices may be monitored, read, examined, seized, or confiscated as necessary. Accordingly, MSA reserves the right to monitor any and all electronic communication device activity. Electronic monitoring of e-mail and Internet activities will only occur if necessary as part of an ongoing investigation.

Students should not expect that any state-owned electronic communication device activity will remain private¹. The State reserves the right to monitor any use of these systems,

¹ Similarly, other State-owned property, including, but not limited to, locked/unlocked desk drawers and cabinets, vehicles, and equipment may also be seized, confiscated, and/or searched as necessary. Students should not expect any personal property that is maintained and/or stored in state owned property would remain private.

including use of these devices while the student is on their own time, to access any information on these systems, and to take any action it determines to be appropriate with respect to that information.

Students should understand that electronic data may not be completely secure. They should also understand that e-mail messages and Internet transactions, including those they delete or erase from their own files, may be backed up or recorded and stored centrally for system security and investigative purposes. E-mails and records of Internet activities may be retrieved and viewed by someone else with proper authority at a later date. It is the user's responsibility to use care in communicating information not meant for public viewing.

VI. FILTERING

- A. With respect to any of its computers with Internet access, MSA will monitor the online activities and employ technology protection measures during any use of these computers by minors or adults. The technology protection utilized will block, filter or limit Internet access to any text or visual depictions that are: 1) Obscene; 2) Pornographic; or 3) Harmful to minors.
- B. The term "harmful to minors" means any picture, image, graphic or visual depiction that:
 - 1. Taken as a whole and with respect to minors, appeals to an interest in nudity or sex, an actual or simulated sexual act or lewd exhibition; or
 - 2. Depicts, describes, or represents information in a patently offensive way with respect to what is suitable for minors.
- C. An administrator (or another person with written authorization by the superintendent) may disable the technology protection measures, with supervision by an adult, to enable access for bona fide research or other lawful purposes.

VII. RECORD RETENTION SCHEDULES

Record retention schedules are the same regardless of the medium used to create or store the record. Many electronic records and e-mail messages are official records of MSA and must be retained in accordance with MSA's approved record retention schedule appropriate for the type, nature, and content of the record. The same rules that are used to determine if a paper, microform, or videotaped record should be retained apply to electronic records or e-mail messages.

Additional References:

Statewide Policy – Zero Tolerance for Sexual Harassment
MN. STAT. 1.50 – Freedom From Violence
MN. STAT. 15.86 – State Agency Actions
MN. STAT. Chapter 13 – Government Data Practices
MN. STAT. 138.17 – Government Records; Administration
MN. STAT. 43a.38, Subd. 4 – Use of State Property
MN. STAT. 169.475 – Use of Wireless Communications Device

Appendix:

524-A: Student/Parent Electronic Communication and Technology Agreement