

Policy #: 524
Title: APPROPRIATE USE OF ELECTRONIC COMMUNICATION AND TECHNOLOGY
Date of Initial Approval: 01-23-2003
Revision/Re-authorization Dates: 11-21-2013; 03-24-2016; 02-16-2017; 06-12-2018; 06-27-2019
Reviewers: MSA Superintendent and Informational Technology employees

I. PURPOSE

The Minnesota State Academies need to address the challenge of meeting legal requirements for access to information and providing adequate protection for proprietary information while at the same time maximizing the use of electronic communication devices and technology. This policy governs access to and the appropriate use of state-provided electronic tools and technology at all times, including both work and non-work time, by MSA employees, consultants, and contractors.

II. GENERAL STATEMENT OF POLICY

A. The Minnesota State Academies (MSA) provide a variety of electronic tools for employees, whose job performance require or would be enhanced by the use of technology.

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

- Desk telephones
- Video phones
- Mobile devices (e.g., iPhones, iPads, BlackBerry's, android phones, etc.)
- Computers
- Facsimile machines, printers and copiers
- Pagers
- Electronic mail (e-mail) systems
- Internet access and apps used by MSA
- Two-way radios

B. Employee access to and use of electronic tools is intended for business-related purposes. Limited and reasonable incidental use of these tools for occasional personal purpose that does not result in any additional costs or loss of time or resources for their intended business purpose is permitted. Incidental use is defined as minimal duration in length and frequency.

C. Employees of MSA are responsible for appropriate use of all state-owned electronic tools. They are expected to adhere to the highest ethical standards when conducting state business and to follow the Code of Ethics and related state statutes applicable to executive branch employees.

M.S. §43A.38, Subd. 4 provides "Use of state property":

1. *Employees [Staff] shall not use or allow the use of state time, supplies, or state-owned or leased property and equipment for the employee's private interest or any other use not in the interest of the state, except as provided by law.*
2. *An employee [staff] may use state time, property, or equipment to communicate electronically with other persons including, but not limited to, elected officials, the employer, or an exclusive bargaining representative under chapter 179A, provided this use, including the value of time*

spent, results in no incremental cost to the state or results in an incremental cost that is so small as to make accounting for it unreasonable or administratively impracticable.

3. *The commissioners of administration and management and budget shall issue a statewide policy on the use of electronic mail and other forms of electronic communications by executive branch state employees. The policy is not subject to the provisions of chapter 14 or 179A. Appointing authorities in the legislative and judicial branches shall issue policies on these issues for their employees. The policies shall permit state employees to make reasonable use of state time, property, and equipment for personal communications and shall address issues of privacy, content of communications, and the definition of reasonable use as well as other issues the commissioners and appointing authorities identify as necessary and relevant.*

M.S. §43A.39, Subd. 2 provides “Noncompliance”:

1. *Any employee [staff] who intentionally fails to comply with the provisions of Chapter 43A shall be subject to disciplinary action and action pursuant to Chapter 609.*

III. MANAGERS AND SUPERVISORS

- A. Managers and supervisors are responsible for ensuring that employees appropriately use all electronic tools by providing training, supervising, coaching and taking disciplinary action, when necessary.
- B. MSA are responsible for establishing internal policies regarding password management, encryption, data practices, monitoring access, records retention, and the like, and for communicating those policies to employees. MSA will ensure that the responsible authorities within the agency know who can access what, using what technology, and under what conditions.
- C. MSA will cooperate fully with local, state and federal authorities in any investigation concerning or related to any illegal activity.

IV. EMPLOYEE RESPONSIBILITIES

MSA employees need to use good judgment in the use of all state-provided electronic tools and technology. They are expected to ensure that messages conveyed are appropriate in both the types of messages created and the tone and content of those messages. Employee use of all state-provided electronic tools and technology must be able to withstand public scrutiny without embarrassment to MSA or the State of Minnesota.

Inappropriate Use:

Examples of inappropriate use include, but are not limited to:

1. Illegal activities;
2. Wagering, betting, or selling;
3. Harassment, cyber bullying, disparagement of others, stalking, and/or illegal discrimination;
4. Fund-raising for any purpose unless agency sanctioned;
5. Commercial activities, e.g., personal for-profit business activities;
6. Promotion of political or religious positions or activities;
7. Receipt, storage, display or transmission of material that is or may be reasonably regarded as violent, harassing, discriminatory, obscene, sexually explicit, or pornographic, including any depiction, photograph, audio recording, or written word;
8. Unauthorized accessing of non-public data or any attempt to post, transmit or distribute non-public or personal data;

9. Non-State employee use (e.g. family member or friend) at work or at home;
10. Introduction of information or materials that could cause damage or danger of disruption to the educational process;
11. Uses that are in any way disruptive, harmful to the reputation or business of the State or that are inappropriate in the education setting or to the educational process;
12. Purposes other than state business, except incidental or minimal use;
13. Attempts to vandalize, to degrade or to disrupt equipment, software or system performance by spreading computer viruses or other means;
14. Attempts to tamper with modify or change the MSA's system software, hardware or wiring or any action to disrupt Academies security systems; and
15. Attempts to violate copyright laws or usage licensing agreements, including downloading or exchanging pirated software.

Employees engaging in any of the above listed activities may be subject to discipline, up to and including dismissal.

The traditional communication rules of reasonableness, respect, courtesy and common sense and legal requirements also apply to electronic communication. Actions that are considered illegal such as gambling and sexual harassment are not up to the discretion of individual agencies or individual managers or supervisors, and such actions will subject the employee to disciplinary action up to and including dismissal.

Employees should be aware that they might receive inappropriate, unsolicited e-mail messages. Any such message should be deleted before opening if an employee does not believe the e-mail is coming from a reputable person or organization. If an employee does open an e-mail and discover it to be inappropriate in nature, or a potential security threat such as a virus, they should report it immediately to the MSA Informational Technology team. Under no circumstances should employees forward or reply to these messages prior to consulting with the IT team.

While employees may make personal use of state technology such as e-mail and Internet access, the amount of use during working hours is expected to be de minimis. De minimis use is defined as so small or minimal in difference that it does not matter or the law does not take it into consideration. Excessive time spent on such personal activities during working hours will subject the employee to disciplinary action.

Cellular Phones and/or Mobile Devices

A. Business Use Justification Requirements:

Cellular phones and/or mobile devices and service are provided for official state business use and are made available to employees in positions where the associated benefits justify the additional operating costs. Employees who meet the following criteria established by the Superintendent's office may be assigned MSA-assigned cellular phones and/or mobile devices.

1. Employees who need to respond to emergencies (i.e. Directors, Nurses)
2. Employees who spend more than 40% of their work time outside of their offices (i.e. Interpreters, Outreach Orientation and Mobility providers)

*The superintendent will consider unique circumstances in determining additional assignments of cellular phones and/or mobile devices.

** "Shared" cellular phones/mobile devices may be checked out for occasional use when employees are out of the office for an extended period of time.

B. Shared Cellular Telephones and/or mobile devices:

Whenever frequency of use does not justify individual assignment, the sharing of state-owned cellular telephones and/or mobile devices is encouraged to reduce costs.

C. Individual Assignment and Self-Management:

When sharing of state-owned cellular telephones/mobile devices does not meet operational needs, employees may be individually assigned a cellular telephone/mobile device.

MSA shall review and assign mobile devices and services consistent with their internal procedures.

Employees will acknowledge the receipt and acceptance of the conditions for the individual assignment of a state-owned cellular telephone/mobile device using the Minnesota State Academies form developed for this purpose. See *Minnesota State Academies Equipment Sign Out (Appendix 524-C)*.

MSA are responsible for keeping the Receipt Form on file for the duration of the individual assignment of a cellular telephone/mobile device to an employee. When the employee leaves his/her position or is no longer an authorized user, the state cellular/mobile device must be returned to the employee's supervisor or other designated official.

D. Public Information:

Call detail (e.g., time, number called, date, duration) of calls appearing on the state cellular telephone billing account is public information, except when exempt by statute.

E. Use of State Cellular Phone/Mobile Device for Personal Calls:

The use of state-owned cellular phones/mobile devices and service is intended for state business. Personal use of state-owned cellular phones/mobile devices is allowable only for incidental use.

F. Essential Personal Calls:

Essential personal calls are defined as calls of minimum duration and frequency that are urgent in nature and cannot be made at another time or from a different telephone. Examples of essential personal calls are calls to arrange for care of a child or other family emergency, to alert a family member of an unexpected delay due to a change in work schedule, or to arrange for transportation or service in the event of car trouble.

G. Potential Disciplinary Action:

Employees are expected to use state cellular phones/mobile devices responsibly and in accordance with this policy and any applicable work rules. Personal use of a state

mobile device in violation of this policy or MSA's work rules may result in revocation of the cellular phone/mobile device assignment and possible disciplinary action against the employee. In addition, employees must reimburse the state within 30 days for the costs of all non-essential personal calls at the state's costs (i.e., the contracted per minute rate, any additional amounts for applicable toll or roaming charges, miscellaneous fees and taxes).

H. Monthly Mobile Device Billing Review and Annual Service Reviews:

MSA Fiscal Services is responsible for reviewing monthly mobile device billings, not unlike any other type of billing it receives. Employees are responsible for identifying their personal calls and texts. Any personal use of a state cellular phone or mobile device shall be identified by the employees and submitted monthly to his/her supervisor or designated individual.

Fiscal Services will conduct an annual review of the individual cellular telephone/mobile device assignments to determine if there is a continuing need and if it remains cost-justified.

I. Use of a Personal Cellular Phone and/or Mobile Device for State Business:

Employees should not use their personal device to conduct state business without prior authorization given. In the event that an individual uses their personal cellular telephone/mobile device to conduct state business, the employee understands that any costs will not be reimbursed by MSA. Employees will be required to sign forms acknowledging their personal responsibility for devices and costs associated with monthly use and/or repairs/replacement.

J. Number Portability:

In the event of a change of vendors for the state's cellular contract, cellular numbers may be ported (transferred) from one vendor to another in most cases. Porting a personal cellular number to a state billing account is prohibited, as is porting a state cellular number to a personal billing account. This will avoid commingling of personal and business calls.

K. Employee Safety:

MSA employees are prohibited from using a cellular phone and/or mobile device to make a phone call while operating a motor vehicle in the conduct of state business, except for the purpose of making a phone call to obtain or render emergency assistance. Further, the use of a cellular phone/mobile device is prohibited in all contracts the state has entered into with rental car agencies, with the only exception being its use in an emergency situation. Additionally, employees are reminded that the use of a mobile device for non-telephone communication (e.g., texting) is illegal in Minnesota while operating a motor vehicle. (See Minnesota Statute 169.475 below)

169.475 USE OF WIRELESS COMMUNICATIONS DEVICE.

Subdivision 1. Definition.

For purposes of this section, "electronic message" means a self-contained piece of digital communication that is designed or intended to be transmitted between

physical devices. An electronic message includes, but is not limited to, e-mail, a text message, an instant message, a command or request to access a World Wide Web page, or other data that uses a commonly recognized electronic communications protocol. An electronic message does not include voice or other data transmitted as a result of making a phone call, or data transmitted automatically by a wireless communications device without direct initiation by a person.

Subd. 2. Prohibition on use.

No person may operate a motor vehicle while using a wireless communications device to compose, read, or send an electronic message, when the vehicle is in motion or a part of traffic.

Subd. 3. Exceptions.

This section does not apply if a wireless communications device is used:

- (1) solely in a voice-activated or other hands-free mode;*
- (2) for making a cellular phone call;*
- (3) for obtaining emergency assistance to (i) report a traffic accident, medical emergency, or serious traffic hazard, or (ii) prevent a crime about to be committed;*
- (4) in the reasonable belief that a person's life or safety is in immediate danger; or*
- (5) in an authorized emergency vehicle while in the performance of official duties.*

V. STUDENT AND PARENT RESPONSIBILITIES

- A. Students are expected to comply by the same rules and regulations listed above for employees while using school-provided technology, including computers, other electronic devices, e-mail, and Internet Access. Students who are observed in violation of rules shall face consequences as outlined in the student handbook, including possible suspension of their computer/Internet privileges for a period of time.
- B. A student engaging in the foregoing unacceptable uses of the Internet when off school district premises also may be in violation of this policy as well as other school district policies. Examples of such violations include, but are not limited to, situations where the school district system is compromised or if a student is negatively impacted. If the school district receives a report of unacceptable use originating from a non-school computer or resource, the school district 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 the school district computer system and the Internet and discipline under other appropriate school district 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 school district system and of the Internet if the student is accessing the school district system from home or a remote location.

Parents will be notified that their students will be using school district resources/accounts to access the Internet and that the school district will provide parents 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 supervising teacher prior to use by the student.
5. A statement that the school district's acceptable use policy is available for parental review.

VI. UNION USE

In the interest of maintaining effective labor management relationships and efficient use of state time and resources, state e-mail systems may be used by employee representatives of the union for certain union activities, in accordance with provisions of applicable bargaining unit agreements.

State-owned property or services including the e-mail system may not be used for political activities, fund-raising, campaigning for union office, union organizing activities, or solicitation of employees for union membership.

Union use of electronic communication technology is subject to the same conditions as employee use of such technology, as set forth in this Policy Memorandum. This includes the conditions set forth in the paragraph below entitled, "Monitoring."

VII. MONITORING

Electronic communication devices such as mobile devices, desk telephones, two-way radios, videophones, facsimile machines, pagers, state e-mail systems and Internet access, any and all software, data, or other information stored on a state-owned computer are state property. Like the other state-owned resources, they are intended to be used for state business and other MSA-sanctioned activities. State-owned electronic communication devices may be monitored, read, examined, seized or confiscated as necessary. Accordingly, MSA reserve the right to monitor any and all electronic communication device activity. Electronic monitoring of telephone¹, facsimile, pager, e-mail and Internet activities that conversations will only occur if proper notice has been given, in accordance with the Federal regulations for Stored Wire and Electronic Communications and Transactional Records Access (Federal Wire Tap Regulations) – see 21 U.S.C. 2701-2711.

Employees should not expect that any state-owned electronic communication device activity will remain private². The State reserves the right to monitor any use of these systems, including use of these devices while the employee is on their own time, to

¹ However, electronic monitoring of telephone conversations will only occur if proper notice has been given, in accordance with Federal regulations for Stored Wire and Electronic Communications and Transactional Records access (Federal Wire Tap Regulations) – See 21 U.S.C. §§2701-2711.

² 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. Staff should not expect any personal property that is maintained and/or stored in state owned property would remain private.

access any information on these systems, and to take any action it determines to be appropriate with respect to that information.

Data that agencies maintain electronically are government data and, as such, are subject to classification and access under the Minnesota Government Data Practices Act, Minnesota Statutes, Chapter 13. Employees 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.

Because electronic communication systems, such as facsimile, e-mail and Internet systems may not be secure, it is recommended that employees not send any data classified under the Minnesota Government Data Practices Act as not public (private or confidential data on individuals or nonpublic or protected nonpublic data not on individuals) through unsecured facsimiles or over the e-mail or Internet systems unless the data are encrypted or encoded.

VIII. FILTERING

A. With respect to any of its computers with Internet access, the Minnesota State Academies 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.

Please see Appendix 524-B "Category Objects for Web Filtering" for detailed listing of blocked, filtered or limited internet access categories.

- 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, supervisor or other person with written authorization by the superintendent may disable the technology protection measures, during use by an adult, to enable access for bona fide research or other lawful purpose.

IX. RECORD RETENTION SCHEDULES

Record retention schedules are the same regardless of the medium used to create or store the record. As a result, many electronic records and e-mail messages are official records of the agency and must be retained in accordance with MSA's approved record retention schedule appropriate for the type, nature and content of the record. Improper disposal may subject the employee and MSA to legal sanctions and other administrative

or legal consequences. 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:

Administrative Procedure 1.2 – Harassment Prohibited
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. 43a.39, Subd. 2 - Noncompliance
MN. STAT. 169.475 – Use of Wireless Communications Device

Appendixes:

524-A: Personal Phone Use
524-B: Category Objects for Web Filtering
524-C: Minnesota State Academies Equipment Sign-Out
524-D: Student/Parent Electronic Communication and Technology Agreement
524-E: Employee Electronic Communication and Technology Agreement