

## **MATH AND SCIENCE ACADEMY**

*Adopted: August 5, 1999*

*Revised: September 6, 2001*

*Revised: March 4, 2003*

*Revised: December 7, 2006*

*Revised: October 30, 2009*

*Revised: April 8, 2010*

*Revised: February 15, 2012*

*Revised: August 15, 2015*

### **524 INTERNET ACCEPTABLE USE AND SAFETY POLICY**

*[Note: School districts are required by statute to have a policy addressing these issues.]*

#### **I. PURPOSE**

The purpose of this policy is to set forth policies and guidelines for access to the Math and Science Academy (MSA) computer system (system) and acceptable and safe use of the Internet, including electronic communications.

#### **II. GENERAL STATEMENT OF POLICY**

In making decisions regarding student and employee access to the MSA computer system and the Internet, including electronic communications, MSA considers its own stated educational mission, goals, and objectives. Electronic information research skills are now fundamental to preparation of citizens and future employees. Access to the MSA computer system and to the Internet enables students and employees to explore thousands of libraries, databases, bulletin boards, and other resources while exchanging messages with people around the world. MSA expects that faculty will blend thoughtful use of MSA the computer system and the Internet throughout the curriculum and will provide guidance and instruction to students in their use.

#### **III. LIMITED EDUCATIONAL PURPOSE**

MSA is providing students and employees with access to the MSA computer system, which includes Internet access. The purpose of the system is more specific than providing students and employees with general access to the Internet. The MSA computer system has a limited educational purpose, which includes use of the system for classroom activities, educational research, and professional or career development activities. Users are expected to use Internet access through the MSA computer system to further educational and personal goals consistent with the mission of MSA and school policies. Uses which might be acceptable on a user's private personal account on another system may not be acceptable on this limited-purpose network.

#### **IV. USE OF SYSTEM IS A PRIVILEGE**

The use of the MSA computer system and access to use of the Internet is a privilege, not a right. Depending on the nature and degree of the violation and the number of previous violations, unacceptable use of the MSA computer system or the Internet may result in one or more of the following consequences: suspension or cancellation of use or access privileges; payments for damages and repairs; discipline under other appropriate MSA policies, including suspension, expulsion, exclusion, or termination of employment; or civil or criminal liability under other applicable laws.

#### **V. UNACCEPTABLE USES**

A. The following uses of the MSA computer system and Internet resources or accounts are considered unacceptable:

1. Users will not use the MSA computer system to access, review, upload, download, store, print, post, receive, transmit, or distribute:
  - a. pornographic, obscene, or sexually explicit material or other visual depictions that are harmful to minors;
  - b. obscene, abusive, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, or sexually explicit language;
  - c. materials that use language or images that are inappropriate in the education setting or disruptive to the educational process;
  - d. information or materials that could cause damage or danger of disruption to the educational process;
  - e. materials that use language or images that advocate violence or discrimination toward other people (hate literature) or that may constitute harassment or discrimination.
2. Users will not use the MSA computer system to knowingly or recklessly post, transmit, or distribute false or defamatory information about a person or organization, or to harass another person, or to engage in personal attacks, including prejudicial or discriminatory attacks.
3. Users will not use the MSA computer system to engage in any illegal act or violate any local, state, or federal statute or law.
4. Users will not use the MSA computer system to vandalize, damage, or disable the property of another person or organization, will not make deliberate attempts to degrade or disrupt equipment, software, or system performance by spreading computer viruses or by any other means, will not tamper with, modify, or change the MSA computer system software, hardware, or wiring or take any action to violate MSA's security

system, and will not use the MSA computer system in such a way as to disrupt the use of the MSA computer system by other users.

5. Users will not use the MSA computer system to gain unauthorized access to information resources or to access another person's materials, information, or files without the implied or direct permission of that person.
6. Users will not use the MSA computer system to post private information about another person, personal contact information about themselves or other persons, or other personally identifiable information, including, but not limited to, addresses, telephone numbers, school addresses, work addresses, identification numbers, account numbers, access codes or passwords, labeled photographs, or other information that would make the individual's identity easily traceable, and will not repost a message that was sent to the user privately without permission of the person who sent the message.

***[Note: School districts should consider the impact of this paragraph on present practices and procedures, including, but not limited to, practices pertaining to employee communications, school or classroom websites, and student/employee use of social networking websites. Depending upon school district policies and practices, school districts may wish to add one or more of the following clarifying paragraphs.]***

- a. This paragraph does not prohibit the posting of employee contact information on MSA webpages or communications between employees and other individuals when such communications are made for education-related purposes (i.e., communications with parents or other staff members related to students).
- b. Employees creating or posting school-related webpages may include personal contact information about themselves on a webpage. However, employees may not post personal contact information or other personally identifiable information about students unless:
  - i. such information is classified by MSA as directory information and verification is made that MSA has not received notice from a parent/guardian or eligible student that such information is not to be designated as directory information in accordance with Policy 515; or
  - ii. such information is not classified by MSA as directory information but written consent for release of the information to be posted has been obtained from a parent/guardian or eligible student in accordance with Policy 515.

In addition, prior to posting any personal contact or personally identifiable information on a school-related webpage, employees shall obtain written approval of the content of the postings from the MSA Director.

- c. These prohibitions specifically prohibit a user from utilizing MSA to post personal information about a user or another individual on social networks, including, but not limited to, social networks such as "MySpace" and "Facebook."

7. Users must keep all account information and passwords on file with the designated MSA Director or designee. Users will not attempt to gain unauthorized access to the MSA computer system or any other system through the MSA computer system, attempt to log in through another person's account, or use computer accounts, access codes, or network identification other than those assigned to the user. Messages and records on the MSA computer system may not be encrypted without the permission of appropriate school authorities.
  8. Users will not use the MSA computer system to violate copyright laws or usage licensing agreements, or otherwise to use another person's property without the person's prior approval or proper citation, including the downloading or exchanging of pirated software or copying software to or from any school computer, and will not plagiarize works they find on the Internet.
  9. Users will not use the MSA computer system for conducting business, for unauthorized commercial purposes, or for financial gain unrelated to the mission of MSA. Users will not use the MSA computer system to offer or provide goods or services or for product advertisement. Users will not use the MSA computer system to purchase goods or services for personal use without authorization from the MSA Director or designee.
  10. Users will not use the MSA computer system to engage in bullying or cyberbullying in violation of MSA's Bullying Prohibition Policy (MSBA/MASA Model Policy 514). This prohibition includes using any technology or other electronic communication off school premises to the extent that student learning or the school environment is substantially and materially disrupted.
- B.** A student or employee engaging in the foregoing unacceptable uses of the Internet when off MSA premises may be in violation of this policy as well as other MSA policies. Examples of such violations include, but are not limited to, situations where MSA system is compromised or if a MSA employee or student is negatively impacted. If MSA receives a report of an unacceptable use originating from a non- school computer or resource, MSA may investigate such reports to the best of its ability. Students or employees may be subject to disciplinary action for such conduct, including, but not limited to, suspension or cancellation of the use or access to MSA computer system and the Internet and discipline under other appropriate MSA policies, including suspension, expulsion, exclusion, or termination of employment.
- C.** If a user inadvertently accesses unacceptable materials or an unacceptable Internet site, the user shall immediately disclose the inadvertent access to the MSA Director or appropriate MSA official. This disclosure may serve as a defense against an allegation that the user has intentionally violated this policy. In certain rare instances, a user also may access otherwise unacceptable materials if necessary to complete an assignment and if done with the prior approval of and with appropriate guidance from the appropriate teacher or, in the case of a MSA employee, the MSA Director.

## **VI. FILTER**

*[Note: Pursuant to state law, school districts are required to restrict access to inappropriate*

*materials on school computers with Internet access. School districts which seek technology revenue pursuant to Minn. Stat. § 125B.26 or certain federal funding, such as e-rate discounts, for purposes of Internet access and connection services and/or receive funds to purchase Internet accessible computers are subject to the federal Children's Internet Protection Act, effective in 2001. Those districts are required to comply with additional standards in restricting possible access to inappropriate materials. Therefore, school districts should select one of the following alternative sections depending upon whether MSA is seeking such funding and the type of funding sought.]*

#### **ALTERNATIVE NO. 1**

*For a school district which does not seek either state or federal funding in connection with its computer system, the following language should be adopted. It reflects a mandatory requirement under state law, Minn. Stat. § 125B.15.*

All computers equipped with Internet access and available for student use at each school site will be equipped to restrict, by use of available software filtering technology or other effective methods, all student access to materials that are reasonably believed to be obscene, child pornography or harmful to minors under state or federal law. Software filtering technology shall be narrowly tailored and shall not discriminate based on viewpoint.

*[Note: The purchase of filtering technology is not required by state law if the school site would incur more than incidental expense in making the purchase. In the absence of filtering technology, school sites still are required to use "other effective methods" to restrict student access to such materials.]*

### **VII. CONSISTENCY WITH OTHER SCHOOL POLICIES**

Use of the MSA computer system and use of the Internet shall be consistent with MSA policies and the mission of MSA.

### **VIII. LIMITED EXPECTATION OF PRIVACY**

- A. By authorizing use of the MSA computer system, MSA does not relinquish control over materials on the system or contained in files on the MSA computer system. Users should expect only limited privacy in the contents of personal files on the MSA computer system.
- B. Routine maintenance and monitoring of the MSA computer system may lead to a discovery that a user has violated this policy, another MSA policy, or the law.
- C. An individual investigation or search will be conducted if the MSA Director has a reasonable suspicion that the search will uncover a violation of law or MSA policy.
- D. Parents have the right at any time to investigate or review the contents of their student's files and e-mail files. Parents have the right to request the termination of their student's individual account at any time.

- E. MSA employees should be aware that MSA retains the right at any time to investigate or review the contents of their files and e-mail files. In addition, MSA employees should be aware that data and other materials in files maintained on the MSA computer system may be subject to review, disclosure or discovery under Minn. Stat. Ch. 13 (the Minnesota Government Data Practices Act).
- F. MSA will cooperate fully with local, state and federal authorities in any investigation concerning or related to any illegal activities or activities not in compliance with MSA policies conducted through the MSA computer system.

## **IX. INTERNET USE AGREEMENT**

- A. The proper use of the Internet, and the educational value to be gained from proper Internet use, is the joint responsibility of students, parents, and employees of MSA.
- B. This policy requires the permission of, and supervision by, the school's designated professional staff before a student may use a school account or resource to access the Internet.
- C. The Internet Use Agreement form for students must be read and signed by the user and the parent or guardian. The Internet Use Agreement form for MSA employees must be signed by the employee. The forms must be filed at the school office.

## **X. LIMITATION ON SCHOOL DISTRICT LIABILITY**

Use of the MSA computer system is at the user's own risk. The system is provided on an "as is, as available" basis. MSA will not be responsible for any damage users may suffer, including, but not limited to, loss, damage, or unavailability of data stored on MSA diskettes, tapes, hard drives, or servers, or for delays or changes in or interruptions of service or mis-deliveries or non-deliveries of information or materials, regardless of the cause. MSA is not responsible for the accuracy or quality of any advice or information obtained through or stored on the MSA computer system. MSA will not be responsible for financial obligations arising through unauthorized use of the MSA computer system or the Internet.

## **XI. USER NOTIFICATION**

- A. All users shall be notified of MSA policies relating to Internet use.
- B. This notification shall include the following:
  - 1. Notification that Internet use is subject to compliance with MSA policies.
  - 2. Disclaimers limiting MSA's liability relative to:
    - a. Information stored on MSA diskettes, hard drives, or servers.
    - b. Information retrieved through MSA computers, networks, or online resources.

- c. Personal property used to access MSA computers, networks, or online resources.
  - d. Unauthorized financial obligations resulting from use of MSA resources/accounts to access the Internet.
3. A description of the privacy rights and limitations of school sponsored/managed Internet accounts.
  4. Notification that, even though MSA may use technical means to limit student Internet access, these limits do not provide a foolproof means for enforcing the provisions of this acceptable use policy.
  5. Notification that goods and services can be purchased over the Internet that could potentially result in unwanted financial obligations and that any financial obligation incurred by a student through the Internet is the sole responsibility of the student and/or the student's parents.
  6. Notification that the collection, creation, reception, maintenance, and dissemination of data via the Internet, including electronic communications, is governed by Policy 406, Public and Private Personnel Data; and Policy 515, Protection and Privacy of Pupil Records.
  7. Notification that, should the user violate MSA's acceptable use policy, the user's access privileges may be revoked, school disciplinary action may be taken and/or appropriate legal action may be taken.
  8. Notification that all provisions of the acceptable use policy are subordinate to local, state, and federal laws.

## **XII. PARENTS' RESPONSIBILITY; NOTIFICATION OF STUDENT INTERNET USE**

- A. 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 computer system and of the Internet if the student is accessing the MSA computer system from home or a remote location.
- B. Parents will be notified that their students will be using MSA resources/accounts to access the Internet and that MSA 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 MSA's acceptable use policy is available for parental review.

### **XIII.IMPLEMENTATION; POLICY REVIEW**

- A. MSA administration may develop appropriate user notification forms, guidelines, and procedures necessary to implement this policy for submission to the Board of Directors (BOD) for approval. Upon approval by the BOD, such guidelines, forms, and procedures shall be an addendum to this policy.
- B. The MSA administration shall revise the user notifications, including student and parent notifications, if necessary, to reflect the adoption of these guidelines and procedures.
- C. MSA Internet policies and procedures are available for review by all parents, guardians, staff, and members of the community.
- D. Because of the rapid changes in the development of the Internet, the BOD shall conduct an annual review of this policy.

**Legal References:** 15 U.S.C. § 6501 *et seq.* (Children's Online Privacy Protection Act) 17 U.S.C. § 101 *et seq.* (Copyrights)  
 20 U.S.C. § 6751 *et seq.* (Enhancing Education through Technology Act of 2001)  
 47 U.S.C. § 254 (Children's Internet Protection Act of 2000 (CIPA))  
 47 C.F.R. § 54.520 (FCC rules implementing CIPA)  
 Minn. Stat. § 121A.031 (School Student Bullying Policy)  
 Minn. Stat. § 125B.15 (Internet Access for Students)  
 Minn. Stat. § 125B.26 (Telecommunications/Internet Access Equity Act)  
*Tinker v. Des Moines Indep. Cmty. Sch. Dist.*, 393 U.S. 503, 89 S.Ct. 733, 21 L.Ed.2d 731 (1969)  
*United States v. Amer. Library Assoc.*, 539 U.S. 194, 123 S.Ct. 2297, 56 L.Ed.2d 221 (2003)  
*Doninger v. Niehoff*, 527 F.3d 41 (2<sup>nd</sup> Cir. 2008)  
*R.S. v. Minnewaska Area Sch. Dist. No. 2149*, No. 12-588, 2012 WL 3870868 (D. Minn. 2012)  
*Tatro v. Univ. of Minnesota*, 800 N.W.2d 811 (Minn. App. 2011), *aff'd* on other grounds 816 N.W.2d 509 (Minn. 2012)  
*S.J.W. v. Lee's Summit R-7 Sch. Dist.*, 696 F.3d 771 (8<sup>th</sup> Cir. 2012)  
*Kowalski v. Berkeley County Sch.*, 652 F.3d 656 (4<sup>th</sup> Cir. 2011)  
*Layshock v. Hermitage Sch. Dist.*, 650 F.3d 205 (3<sup>rd</sup> Cir. 2011)  
*Parents, Families and Friends of Lesbians and Gays, Inc. v. Camdenton R-III Sch. Dist.*, 853 F.Supp.2d 888 (W.D. Mo. 2012)  
*M.T. v. Cent. York Sch. Dist.*, 937 A.2d 538 (Pa. Commw. Ct. 2007)  
*J.S. v. Bethlehem Area Sch. Dist.*, 807 A.2d 847 (Pa. 2002)



***Cross References:*** MSA Policy 406 (Public and Private Personnel Data)  
MSA Policy 505 (Distribution of Nonschool-Sponsored Materials on School  
Premises by Students and Employees)  
MSA Policy 506 (Student Discipline)  
MSA Policy 514 (Bullying Prohibition Policy)  
MSA Policy 515 (Protection and Privacy of Pupil Records)  
MSA Policy 521 (Student Disability Nondiscrimination)  
MSA Policy 522 (Student Sex Nondiscrimination)  
MSA Policy 603 (Curriculum Development)  
MSA Policy 806 (Crisis Management Policy)  
MSA Policy 904 (Distribution of Materials on School District Property by  
Nonschool Persons)