MSBA/MASA Model Policy 524
Original: 2012
Revised: 2015. 2020
Adopted: June 16, 2020

524 TECHNOLOGY RESPONSIBLE USE AND SAFETY POLICY

I. PURPOSE

The purpose of this policy is to set forth policies and guidelines for access both on and off district property to school district technology resources 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 school district district technology resources, which includes district devices, Internet access, the local network, and electronic communications, the school district considers its own stated educational mission, goals, and objectives. Digital literacy skills are now fundamental to preparation of digital citizens and future employees. Access to the school district local network 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. The school district expects that faculty will blend thoughtful use of the school district technology resources, local network and the Internet throughout the curriculum and will provide guidance and instruction to students in their use.

The district recognizes the importance of online social media networks as a communication and learning tool. Social media includes websites and applications that enable users to create and share content or to participate in social networking. Toward that end, the District provides password-protected social media tools and District-approved technologies for e-learning and encourages use of District tools for collaboration by employees. However, public social media networks, outside of those sponsored by the District, may not be used for classroom instruction or school-sponsored activities without the prior authorization of the Superintendent, or designee, and parental consent for student participation on social networks.

Staff have the same responsibility for addressing inappropriate student behavior or activity on these networks as you would in a classroom, including requirements for mandated reporting.

III. LIMITED EDUCATIONAL PURPOSE

The school district is providing students and employees with access to district technology resources. The purpose is more specific than providing students and employees with general access to the Internet. District technology resources have a limited educational purpose, which includes use for classroom activities, educational research, and professional or career development activities. Users are expected to use district technology resources to further educational and personal goals consistent with the mission of the school district 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. Although district technology resources are intended for use related to the conduct of the school district business, employees may access district technology resources and/or Internet for limited, occasional, and brief personal use that does not interfere with the conduct of school district business, subject to state and federal law, the restrictions of board policy, district operating procedures on acceptable district technology use, and directives or guidelines of an employee's supervisor or other school district official. When utilizing district technology resources for personal use, employees should attempt to do so during non-duty hours.

IV. USE OF RESOURCES ARE A PRIVILEGE

The use of district technology resources and access to use of the Internet is a privilege, not a right.

Staff: Many of the duties required of staff depend on the responsible use of district technology resources, and irresponsible or illegal use of these technologies could put staff member's abilities to perform these duties at risk. Depending on the nature and degree of the violation and the number of previous violations, unacceptable use of district technology resources may result in one or more of the following consequences: payments for damages and repairs; discipline under other appropriate school district policies, termination of employment; or civil or criminal liability under other applicable laws.

Students: Depending on the nature and degree of the violation and the number of previous violations, unacceptable use of district technology resources 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 school district policies, including suspension, expulsion, exclusion, or civil or criminal liability under other applicable laws.

V. UNACCEPTABLE USES

A. The following uses of district technology resources or accounts are considered unacceptable:

1. Users will not use district technology resources 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 district technology resources 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 district technology resources to knowingly engage in any illegal act or violate any local, state, or federal statute or law.

4. Users will not use district technology resources 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 district technology resources software, hardware, or wiring or take any action to violate the school district's security system, and will not use district technology resources in such a way as to disrupt the use of the system by other users.

5. Users will not use district technology resources 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 district technology resources to knowingly 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.

a. This paragraph does not prohibit the posting of employee contact information on school district 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:

(1) such information is classified by the school district as directory information and verification is made that the school district 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

(2) such information is not classified by the school district 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 building administrator.

c. These prohibitions specifically prohibit a user from utilizing district technology resources to post personal information about a user or another individual on social networks, including, but not limited to, social networks such as "Instagram", "Snapchat", "Twitter", "TikTok", and "Facebook" except as approved by a supervising teacher or administrator.

7. Users will not attempt to gain unauthorized access to the school district network or any other system through the use of district technology

resources, , attempt to log in through another person's account, or use computer accounts, access codes, network identification, or digital signature other than those assigned to the user. Messages and records on district technology resources may not be encrypted without the permission of appropriate school authorities.

8. Users will not use district technology resources 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 district technology resources for conducting personal business, for unauthorized commercial purposes, or for financial gain unrelated to the mission of the school district. Users will not use district technology resources to offer or provide goods or services or for product advertisement. Users will not use district technology resources to purchase goods or services for personal use without authorization from the appropriate school district official. Unauthorized purchase of goods and services using district technology resources over the Internet could potentially result in unwanted financial obligations. Any financial obligation incurred by a student through the use of district technology resources is the sole responsibility of the student and/or the student's parents.

10. Users will not use district technology resources to engage in bullying or cyberbullying in violation of the school district's Bullying Prohibition 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 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 network is compromised or if a school district employee or student is negatively impacted. If the school district receives a report of an unacceptable use originating from a non-school computer or resource, the school district 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 district technology resources and discipline under other appropriate school district 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 an appropriate school district official. In the case of a school district employee, the immediate disclosure shall be to the employee's immediate supervisor and/or the building administrator. 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 school district employee, the building administrator.

VI. FILTER

A. With respect to any of its district technology resources, the school district will monitor the online activities of both minors and adults and employ technology protection measures during any use of such technology resources by minors and adults. The technology protection measures utilized will block or filter Internet access to any visual depictions that are:

1. Obscene;

2. Child pornography; or

3. Harmful to minors.

B. The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that:

1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; or

2. Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and

3. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

C. An administrator, supervisor, or other person authorized by the Superintendent may disable the technology protection measure, during use by an adult, to enable access for bona fide research or other lawful purposes.

D. The school district will educate students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

VII. CONSISTENCY WITH OTHER SCHOOL POLICIES

Use of district technology resources and use of the Internet shall be consistent with school district policies and the mission of the school district.

VIII. LIMITED EXPECTATION OF PRIVACY

A. By authorizing use of district technology resources, the school district does not relinquish control over materials on the system or contained in files on the system. Users should expect only limited privacy in contents of personal files on district technology resources. Users should expect only limited privacy in the use of their personal electronic devices on the district network.

B. Routine maintenance and monitoring of the district technology resources may lead to a discovery that a user has violated this policy, another school district policy, or the law.

C. An individual investigation or search will be conducted if school authorities have a reasonable suspicion that the search will uncover a violation of law or school district policy.

D. Parents have the right at any time to investigate or review the contents of their child's files and email files. Parents have the right to request the termination of their child's individual account at any time.

E. School district employees should be aware that the school district retains the right at any time to investigate or review the contents of their files and email files. In addition, school district employees should be aware that data and other materials in files maintained on district technology resources may be subject to review, disclosure or discovery under Minn. Stat. Ch. 13 (the Minnesota Government Data Practices Act). In addition, school district employees should be aware that the school district may have lawful grounds under certain circumstances to search an employee's personal electronic devices, even if the district technology resources were not used.

F. The school district 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 school district policies conducted through district technology resources .

G. School district employees should be aware that when connecting personal devices to your school email accounts, including personal smartphones, the district requires your device to set a passcode to protect data you will be retrieving from our servers, the district may also gain the ability to remotely lock, and remotely erase your personal device to protect sensitive data in the event of a loss or theft.

All lost devices connected to the district network resources (I.E.: e-mail, cloud storage, or wireless networks) should be reported to the Technology Department as soon as possible.

IX. TECHNOLOGY RESPONSIBLE USE AGREEMENT

A. The proper use of district technology, and the educational value to be gained from proper technology use, is the joint responsibility of students, parents, and employees of the school district.

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 district technology resources .

C. The Technology Responsible Use Agreement form for students must be read and signed by the user, the parent or guardian, and the supervising teacher. The Technology Responsible Use Agreement form for employees must be signed by the employee. The form must then be filed at the school office.

X. LIMITATION ON SCHOOL DISTRICT LIABILITY

Use of the district technology resources is at the user's own risk. Technology resources are provided on an "as is, as available" basis. The school district will not be responsible for any damage users may suffer, including, but not limited to, loss, damage, or unavailability of data stored on school district storage mediums or systems, or for delays or changes in or interruptions of service or misdeliveries or nondeliveries of information or materials, regardless of the cause. The school district is not responsible for the accuracy or quality of any advice or information obtained through or stored on the district technology resources. The school district will not be responsible for financial obligations arising through unauthorized use of district technology resources.

XI. USER NOTIFICATION

A. All users shall be notified of the school district policies relating to district technology use.

B. This notification shall include the following:

1. Notification that district technology use is subject to compliance with school district policies.

2. Disclaimers limiting the school district's liability relative to:

a. Information stored on school district storage mediums or systems.

b. Information retrieved through school district computers, networks,

or online resources.

c. Personal property used to access school district computers, networks, or online resources.

d. Unauthorized financial obligations resulting from use of school district resources/accounts to access the Internet.

3. A description of the privacy rights and limitations of school sponsored/managed Internet-based accounts available upon request.

4. Notification that, even though the school district 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 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.

6. Notification that, should the user violate the school district'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.

7. 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 district technology resources and 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 district technology resources and the Internet if the student is using district technology resources from home or a remote location.

B. Parents will be notified that their students will be using school district technology and that the school district will provide parents the option to request alternative activities not requiring technology 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 Technology Responsible Use Agreement must be signed annually by the user and the parent or guardian prior to use.

5. A statement that the school district's acceptable use policy is available for parental review.

XIII. IMPLEMENTATION; POLICY REVIEW

A. The school district administration may develop appropriate user notification forms, guidelines, and procedures necessary to implement this policy for submission to the school board for approval. Upon approval by the school board, such guidelines, forms, and procedures shall be an addendum to this policy.

B. The administration shall revise the user notifications, including student and parent notifications, if necessary, to reflect the adoption of these guidelines and procedures.

C. The school district technology resource use 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 technology resources, the school board 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.0695 (School Board Policy; Prohibiting Intimidation and Bullying)
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 (2nd 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 (8th Cir. 2012)
Kowalski v. Berkeley County Sch., 652 F.3d 656 (4th Cir. 2011)
Layshock v. Hermitage Sch. Dist., 650 F.3d 205 (3rd 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: MSBA/MASA Model Policy 403 (Discipline, Suspension, and Dismissal of School District Employees)
MSBA/MASA Model Policy 406 (Public and Private Personnel Data)
MSBA/MASA Model Policy 505 (Distribution of Nonschool-Sponsored Materials on School Premises by Students and Employees)
MSBA/MASA Model Policy 506 (Student Discipline)
MSBA/MASA Model Policy 515 (Protection and Privacy of Pupil Records)
MSBA/MASA Model Policy 519 (Interviews of Students by Outside Agencies)
MSBA/MASA Model Policy 521 (Student Disability Nondiscrimination)
MSBA/MASA Model Policy 522 (Student Sex Nondiscrimination)
Policy 524.1 (Bring Your Own Device)
MSBA/MASA Model Policy 603 (Curriculum Development)
MSBA/MASA Model Policy 604 (Instructional Curriculum)
MSBA/MASA Model Policy 606 (Textbooks and Instructional Materials)
MSBA/MASA Model Policy 806 (Crisis Management Policy)
MSBA/MASA Model Policy 904 (Distribution of Materials on School District Property by Nonschool Persons)