TECHNOLOGY ACCEPTABLE USE AND SAFETY POLICY 540

I. PURPOSE

The purpose of this policy is to set forth policies and guidelines for access to the school district computer systems 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 computer system and the Internet, including electronic communications, the school district 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 school district computer system and to the Internet enables students and employees to explore global resources. The school district expects that faculty will blend thoughtful use of the school district computer system and the Internet throughout the curriculum and will provide guidance and instruction to students in their use.

III. LIMITED EDUCATIONAL PURPOSE

The school district is providing students and employees with access to the school district 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 school district 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 district system 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. Acceptable uses are determined at the sole discretion of the district.

IV. USE OF SYSTEM IS A PRIVILEGE

While the school district's electronic systems are provided for the conduct of the school district's mission, it is understood that they may be used occasionally for personal use as well. Reasonable personal use is permitted, so long as it does not interfere with users' performance of their responsibilities and complies with applicable laws and policies. The personal use of both audio and video streaming media as well as the downloading of excessively large files for personal use interferes with the school district's use of the Internet and delivery of electronic mail and is therefore not acceptable personal use of the Internet.

The use of the school district 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 school district 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 school district policies, including suspension, expulsion, exclusion or termination of employment; or civil or criminal liability under other applicable laws.

V. UNACCEPTABLE USES

A. While not an exhaustive list, the following uses of the school district system and Internet resources or accounts are considered unacceptable:

1. Users will not use the school district 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. language or images that are inappropriate in the education setting or disruptive to the educational process;

   c. information or materials that could cause damage or danger of disruption to the educational process;

   d. language or images that advocate violence or discrimination toward other people (hate literature) or that may constitute harassment or discrimination, except as allowed in Policy 602 Controversial Issues.

2. Users shall not use district system as part of a political campaign to support or oppose a political issue or the nomination or election of a candidate for public office except as otherwise agreed upon in school district employment agreements.

3. Users will not use the school district system to knowingly or recklessly post, transmit or distribute false or defamatory information about a person or organization, or to harass or bully another person, or to engage in personal attacks, including prejudicial or discriminatory attacks.

4. Users will not use the school district system to engage in any illegal act or violate any local, state or federal statute or law.

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

6. Users will not use the school district system to gain unauthorized access to information resources or to access another person's materials, information or files without the implied or direct consent of that person. Consent is implied for all users whose materials, information or files must be accessed by personnel performing authorized system maintenance on behalf of the district.

7. Users will not attempt to gain unauthorized access to the school district system or any other system through the school district 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 without the implied or direct consent of that person. Consent is implied for all users whose materials, district information or files must be accessed by personnel performing authorized system maintenance on behalf of the district. Messages and records on the school district system may not be encrypted without the permission of appropriate school authorities.

8. Users will not use the school district system to violate copyright laws or usage licensing agreements, or otherwise to use another owner's property without the owner'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 school district system for conducting business, for unauthorized commercial purposes or for financial gain unrelated to the mission of the school district.

10. Users will not use the school district system to engage in bullying or cyberbulling in violation of the school district's bullying prohibition policy. 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. The school district has a special interest in regulating off-campus speech that materially disrupts classwork or involves substantial disorder or invasion of the rights of others. 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 may include, but are not limited to, serious or severe bullying or harassment

targeting particular individuals, threats aimed at teachers or other students, failure to follow rules concerning lessons, the writing of papers, the use of computers, or participation in other online school activities, and breaches of school security devices. 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 the school district computer system and the Internet 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 computers with Internet access, school district personnel will monitor the online activities of minors and employ technology protection measures during any use of such computers 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

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

C. Software filtering technology shall be narrowly tailored and shall not discriminate based on viewpoint

D. 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. It is prohibited for students or employees to attempt to bypass the district filter without permission.

E. 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 the school district computer system 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 the school district system, 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 the contents of personal files on the school district system.

B. Routine maintenance and monitoring of the school district system or other routine activities, (for example, responses to data requests) may lead to a discovery that a user has violated this policy, another school district policy, or the law.

C. If school authorities have a reasonable suspicion that an individual search of student accounts or devices will uncover a violation of law or school district policy or is necessary to protect the health or safety of a student or other person, school authorities will conduct such a search as permitted by Minnesota law.

D. Parents may have the right to investigate or review the contents of files generated by their student in accordance with the school district's Protection and Privacy of Pupil Records Policy. 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 e-mail files. In addition, school district employees should be aware that data and other materials

in files maintained on the school district system may be subject to review, disclosure or discovery under Minnesota Statutes, Chapter 13 (the Minnesota Government Data Practices Act).

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 the school district 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 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 the Internet.

X. LIMITATION ON SCHOOL DISTRICT LIABILITY

Use of the school district system is at the user's own risk. The system is 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 media, 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 loss or damage to personal devices or media attached to district equipment. The school district is not responsible for the accuracy or quality of any advice or information obtained through or stored on the school district system. The school district will not be responsible for financial obligations arising through unauthorized use of the school district system or the Internet.

XI. USER NOTIFICATION

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

B. This notification shall include the following:

1. Notification that Internet 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 physical drives or servers.

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 accounts.

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 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 or staff member through the Internet is the sole responsibility of the student and/or the student's parents/guardians or the staff member incurring the obligation.

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 505, Use of Student Records.

7. 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.

8. Notification that all provisions of the acceptable use policy are subordinate to local, state and federal laws.

XII. PARENTS' / GUARDIANS' RESPONSIBILITY

Outside of school, parents and/or guardians of students 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.

XIII. NOTIFICATION REGARDING TECHNOLOGY PROVIDERS

A. "Technology provider" means a person who:

1. contracts with the school district, as part of a one-to-one program or otherwise, to provide a school-issued device for student use; and

2. creates, receives, or maintains educational data pursuant or incidental to a contract with the school district.

B. "Parent" means a parent of a student and includes a natural parent, a guardian, or an individual acting as a parent in the absence of a parent or a guardian.

C. Within 30 days of the start of each school year, the school district must give parents and students direct and timely notice, by United States mail, e-mail, or other direct form of communication, of any curriculum, testing, or assessment technology provider contract affecting a student's educational data. The notice must:

1. identify each curriculum, testing, or assessment technology provider with access to educational data;

2. identify the educational data affected by the curriculum, testing, or assessment technology provider contract; and

3. include information about the contract inspection and provide contact information for a school department to which a parent or student may direct questions or concerns regarding any program or activity that allows a curriculum, testing, or assessment technology provider to access a student's educational data.

D. The school district must provide parents and students an opportunity to inspect a complete copy of any contract with a technology provider.

E. A contract between a technology provider and the school district must include requirements to ensure appropriate security safeguards for educational data. The contract must require that:

1. the technology provider's employees or contractors have access to educational data only if authorized; and

2. the technology provider's employees or contractors may be authorized to access educational data only if access is necessary to fulfill the official duties of the employee or contractor.

F. All educational data created, received, maintained, or disseminated by a

technology provider pursuant or incidental to a contract with a public educational agency or institution are not the technology provider's property.

XIV. SCHOOL-ISSUED DEVICES

A. "School-issued device" means hardware or software that the school district, acting independently or with a technology provider, provides to an individual student for that student's dedicated personal use. A school-issued device includes a device issued through a one-to-one program.

B. Except as provided in paragraph C, the school district or a technology provider must not electronically access or monitor:

1. any location-tracking feature of a school-issued device;

2. any audio or visual receiving, transmitting, or recording feature of a school-issued device; or

3. student interactions with a school-issued device, including but not limited to keystrokes and web-browsing activity.

C. The school district or a technology provider may only engage in activities prohibited by paragraph B if:

1. the activity is limited to a noncommercial educational purpose for instruction, technical support, or exam-proctoring by school district employees, student teachers, staff contracted by the school district, a vendor, or the Minnesota Department of Education, and notice is provided in advance;

2. the activity is permitted under a judicial warrant;

3. the school district is notified or becomes aware that the device is missing or stolen;

4. the activity is necessary to respond to an imminent threat to life or safety and the access is limited to that purpose;

5. the activity is necessary to comply with federal or state law, including but not limited to Minnesota Statutes section 121A.031; or

6. the activity is necessary to participate in federal or state funding programs, including but not limited to the E-Rate program.

D. If the school district or a technology provider interacts with a school-issued device as provided in paragraph C, clause 4, it must, within 72 hours of the

access, notify the student to whom the school-issued device was issued or that student's parent and provide a written description of the interaction, including which features of the device were accessed and a description of the threat. This notice is not required at any time when the notice itself would pose an imminent threat to life or safety, but must instead be given within 72 hours after that imminent threat has ceased.

XV. LIMIT ON SCREEN TIME FOR CHILDREN IN PRESCHOOL AND KINDERGARTEN

A child in a publicly funded preschool or kindergarten program may not use an individual-use screen, such as a tablet, smartphone, or other digital media, without engagement from a teacher or other students. This section does not apply to a child for whom the school has an individualized family service plan, an individualized education program, or a 504 plan in effect.

XVI. IMPLEMENTATION; POLICY REVIEW

A. The school district may develop appropriate user notification forms, guidelines and procedures necessary to implement this policy.

B. The school district 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 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, the school board shall conduct a periodic review of this policy.

Legal References:
Minn. Stat. § 13.32 (Educational Data)
Minn. Stat. § 124D.166 (Limit on Screen Time for Children in Preschool and Kindergarten)
15 U.S.C. § 6501 et seq. (Children's Online Privacy Protection Act)
17 U.S.C. § 101 et seq. (Copyrights)
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 (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 565 (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)

Cross References:
MSBA/MASA Model Policy 403 (Discipline, Suspension, and Dismissal of School District Employees)
Policy 406 (Public and Private Personnel Data)
Policy 421 (Student Sex Nondiscrimination)
Policy 504 (Interviews of Students by Outside Agencies)
Policy 505 (Use of Student Records)
MSBA/MASA Model Policy 505 (Distribution of Nonschool-Sponsored Materials on School Premises by Students and Employees)
MSBA/MASA Model Policy 515 (Protection and Privacy of Pupil Records)
Policy 515 (Student Discipline)
Policy 536 (Student Disability Nondiscrimination)
Policy 538 (Crisis Management Policy)
Policy 539 (Instructional Materials – Films)
Policy 541 (Bullying Prohibition Policy)
MSBA/MASA Model Policy 603 (Curriculum Development)
MSBA/MASA Model Policy 604 (Instructional Curriculum)
Policy 605 (Instructional Materials Selection Policy)
Policy 623 (Procedure for Review of Curriculum Content and Alternative Instruction
MSBA/MASA Model Policy 904 (Distribution of Materials on School District Property by Nonschool Persons)

ADOPTED: May 6, 2002
June 7, 2004
October 5, 2006
November 1, 2007 (No Changes)
January 7, 2010
March 3, 2011
January 5, 2012 (No Changes)
January 3, 2013

December 5, 2013 (No Changes)
January 8, 2015 (No Changes)
January 7, 2016
February 2, 2017
December 7, 2017 (No Changes)
December 6, 2018 (No Changes)
December 5, 2019
December 3, 2020 (No Changes)
December 2, 2021
February 2, 2023
March 14, 2024