Reviewed: 5/12/16

Revised: 6/11/15 (MSBA Policy Review); 4/21/11; 10/8/09; 10/13/05; 3/8/01; 6/10/99

Adopted: 2/6/97

524 TECHNOLOGY ACCEPTABLE USE AND SAFETY POLICY

I. PURPOSE

The purpose of this policy is to provide guidelines for acceptable and safe use of the school district's electronic technologies for guests, students, and school district personnel (users) and to set guidelines for acceptable use of the school district's computer systems, hardware and software, web-based applications, electronic communications, school district web sites, and the Internet.

II. GENERAL STATEMENT OF POLICY

In making decisions regarding student and employee access to the school district's electronic technologies, the school district considers its own stated educational mission, goals, and objectives. Technology skills are now fundamental to prepare students to become responsible global citizens. The school district expects that users will blend thoughtful use of electronic technologies and the Internet throughout the curriculum.

III. LIMITED EDUCATIONAL PURPOSE

The school district is providing students and employees with access to the school district electronic technologies including Internet access. The school district systems have limited educational purpose, which includes use of the systems for classroom activities, educational research, collaboration, and professional or career development activities. Employees are required to follow data privacy policies and refrain from using email for communications containing private educational data or personnel data. Users are expected to use Internet access through the district systems to further educational and personal goals consistent with the mission of the school district and school policies. Employees may use the school district system for occasional personal needs consistent with other school board 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. Users shall not use the Internet, or email, for advertising purposes or to promote personal causes.

IV. USE OF SYSTEM IS A PRIVILEGE

The use of school district systems 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 systems 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. The following uses of school district systems and Internet resources or accounts are considered unacceptable:

1. Users will not use school district systems 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, terroristic, 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 school district systems or the Internet 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 consistent with school district and school policies.

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

4. Users will **not** use the school district system to do any of the following:

    a. Vandalize, damage or disable the property of another person or organization.
    b. Make deliberate attempts to degrade or disrupt equipment, software or system performance by loading, creating, or spreading computer viruses or by any other means.
    c. Tamper with, modify or change school district systems, software, hardware, or wiring.

d. Take any action to violate, bypass or disable school district security and safety systems.
e. Use school district systems to disrupt the use of the systems.

5. Users will not use school district systems 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. Users also will not modify information created by others without their permission.

6. Users will not engage in Cyberbullying. "Cyberbullying" means bullying using technology or other electronic communications, including, but not limited to, a transfer of a sign, signal, writing, image, sound, or data, including a post on a social network Internet website or forum, transmitted through a computer, cell phone, or other electronic device. The term applies to prohibited conduct which occurs on school premises, on school district property, at school functions or activities, on school transportation, or on school computers, networks, forums, and mailing lists, or off school premises to the extent that it substantially and materially disrupts student learning or the school environment.

7. Users will not use school district systems to post, transmit or distribute 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 without permission. Users 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 district related publications, websites, and social media 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-Protection and Privacy of Pupil Records; or

(2) such information is not classified by the school district as directory information but consent for release of the information to be posted has been obtained from a parent/guardian or eligible student in accordance with Policy 515-Protection and Privacy of Pupil Records.

These prohibitions specifically prohibit a user from utilizing the school district's systems to post personal information about a user or another individual on personal social networks.

8. Users must keep all account information and passwords on file with the designated school district official. 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. Messages and records on the school district system may not be encrypted without the permission of appropriate school authorities. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to school district systems or the Internet or both.

9. Users will not use school district systems 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. Users must assume that all communications and information accessible through the Internet is private property and copyright protected.

10. Users will not use school district systems for conducting business, for unauthorized commercial purposes or for financial gain unrelated to the mission of the school district. Users will not use the school district system to offer or provide goods or services or for product advertisement.

11. Users will not use school district systems for non-district supported software without the prior approval of the school district technology department.

12. Users will not save personal photos, music, files, etc. unrelated to educational purposes on a district share/home folder for an extended period of time. Personal data saved on workstations may be removed if they degrade the performance of the workstation or other district systems.

13. Users will not access the internal school district network, the Internet, or printers with personal electronic devices without prior approval.

B. A student or employee engaging in any of the foregoing unacceptable uses of the Internet when off school district premises and without the use of the school district

system may 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's systems are 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 academic sanctions or 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.

D. A user must notify the district technology department if a user identifies a security problem with school district systems or on the Internet. The user should not demonstrate the problem to other users.

E. Respect for privacy rights:

1. Students may only use personal electronic devices to record sound, pictures, or video of classroom instruction with prior approval from the teacher or staff member. It may be inappropriate to record any conversations or exchanges of communications without the knowledge and consent of all participating persons.

2. Students shall not photograph or videotape other individuals at school or at school sponsored activities without their knowledge and consent, except for activities considered to be in the public arena such as sporting events or public performances.

3. Students shall not e-mail, post to the Internet, or other otherwise electronically transmit images of other individuals taken at school without consent.

4. Use of cellular phones or other personal electronic devices is strictly prohibited in locker rooms and restrooms.

VI. DISTRICT WEB SITE

A. All communications and information accessible on Mahtomedi Public Schools' official websites are property of the school district.

B. The principal of each school building or an administrator designee (i.e. district communications coordinator, district technology coordinator, etc.) shall approve content on their web page consistent with school district policy, procedures, and guidelines. The content of district-wide pages shall be approved by the superintendent.

C. Individual student or staff web pages developed using school district systems or access shall be subject to this policy.

VII. FILTER

A. With respect to school district Internet access, the district will monitor and filter online activities of both minors and adults. The school district is required by Child Internet Protection Act (CIPA) to implement filtering measures that 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. 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.

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.

F. The school district reserves the right to block or filter sites that are deemed inappropriate for users or compromise the integrity of school district systems.

VIII. CONSISTENCY WITH OTHER SCHOOL POLICIES

A. Use of school district computer systems and use of the Internet shall be consistent with school district policies and the mission of the school district.

IX. LIMITED EXPECTATION OF PRIVACY

A. By authorizing use of school district systems, the school district does not relinquish control over materials on the systems or contained in files on the systems, whether onsite or offsite, or transmitted via the systems. Users should expect only limited privacy for personal content on school district systems.

B. Routine maintenance and monitoring of the school district system 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 e-mail.

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, online activity and e-mail. 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). The school district archives employee email for a period of up to three years.

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.

X. COMPUTER SYSTEMS AND INTERNET USE AGREEMENT

A. The proper use of the school district’s computer systems and the Internet, and the educational value to be gained from their proper use, is the joint responsibility of students, parents, employees, and guests 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 school district's computer systems and the Internet.

C. The Computer Systems and Internet Use Agreement form for students must be read and signed by the user and the parent or guardian upon beginning Wildwood Elementary School or O. H. Anderson Elementary School and yearly at Mahtomedi Middle School and Mahtomedi High School.

D. The Computer Systems and Internet Use Agreement form for employees must be signed by the employee upon hire or change in policy. The form must then be filed at the District Office.

E. Guest access to the wireless Internet will require digital verification that the user will abide by all district policies pertaining to acceptable and responsible use.

XI. LIMITATION ON SCHOOL DISTRICT LIABILITY

Use of school district systems is at the user's own risk. The Mahtomedi Public Schools, their employees and agents, make no warranties of any kind, whether expressed or implied, regarding the service it is providing. 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 systems or backup media, for delays or changes in service, for interruptions of service, or for mis-deliveries or non-deliveries 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 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.

XII. USER NOTIFICATION

A. All users shall be notified of the school district policies relating to district computer systems and 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 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 accounts.

4. Notification that, even though the school district may use technical means to limit student or employee 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 and any financial obligation incurred by an employee through the Internet is the sole responsibility of the employee.

6. Notification that the collection, creation, reception, maintenance and dissemination of data via the Internet, including electronic communications, is governed by Policy 435-Public and Private Personnel Data and Policy 509-Protection and Privacy of Pupil Records.

7. Notification that, should the user violate the school district's acceptable use policy, the user's access privileges may be revoked, student or employee 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.

XIII. PARENTS' RESPONSIBILITY: NOTIFICATION OF STUDENT COMPUTER SYSTEMS AND INTERNET USE

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 school district systems and of the Internet if the student is accessing school district systems from home or a remote location.

XIV. IMPLEMENTATION: POLICY REVIEW

A. The school district administration may develop appropriate user notification forms, login banners, 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 computer systems, Internet policies and procedures are available for review by all parents, guardians, staff and members of the community.

D. This policy will be annually reviewed and posted on the district website.

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. § 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. American Library Association, 539 U.S. 194, 123 S.Ct. 2297, 56 L.Ed.2d 221 (2003)
Doninger v. Niehoff, 527 F.3d 41(2nd Cir. 2008)
Tatro v. Univ. of Minnesota, 800 N.W.2d 811 (Minn. App. 2011)
Layshock v. Hermitage Sch. Dist., 650 F.3d 205 (3rd Cir. 2011)
J.S. v. Bethlehem Area Sch. Dist., 807 A.2d 847 (Pa. 2002)

Cross References:
Policy 403 (Discipline, Suspension, and Dismissal of School District Employees)
Policy 406 (Public and Private Personnel Data)
Policy 505 (Distribution of Nonschool-Sponsored Materials on School Premises by Students and Employees)
Policy 506 (Student Discipline)
Policy 514 (Bullying Prohibition Policy)
Policy 515 (Protection and Privacy of Pupil Records)
Policy 519 (Interviews of Students by Outside Agencies)
Policy 521 (Student Disability Nondiscrimination)
Policy 522 (Student Sex Nondiscrimination)
Policy 603 (Curriculum Development)
Policy 604 (Instructional Curriculum)
Policy 606 (Textbooks and Instructional Materials)
Policy 806 (Crisis Management Policy)
Policy 904 (Distribution of Materials on School District Property by Nonschool Persons)