

Waseca School District Policy 524

Adopted: August 22, 1996
Reviewed: February 19, 2015
**Review Annually

524 ACCEPTABLE USE POLICY

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

I. PURPOSE

The purpose of this policy is to ensure the security of our district network system and the safety of our students and staff using our district network system.

II. GENERAL STATEMENT OF POLICY

District Administration will develop and enforce guidelines to ensure the security of our district network system and the safety of our students and staff using our district network system. These guidelines, located in Regulation 524, will support the following concepts:

- A. The access and use of our district network system must align with our Strategic Plan and District technology plan.
- B. Internet access and use is for educational purposes.
- C. The use of our district network system is a privilege and not a right. Depending on the nature and the degree of the violation, unacceptable use will result in consequences to be determined by the District.
- D. District information on the district network system is the property of the District and unauthorized accessing and altering of this data is prohibited.

I. UNACCEPTABLE USES

- A. 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 knowingly access, review, upload, download, share, 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 school district 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 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 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.
 5. 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 permission of that person.
 6. Users will not use the school district 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, 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 without permission of the person who sent the message.
 7. Users will not send email using another person's account or in the name of someone else.
 8. 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.

9. Users will not use the school district 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.
 10. Users will not use the school district system 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 the school district system for the purpose of encouraging other users toward a specific political lobbying viewpoint or agenda.
 12. Users will not send or forward unnecessary or frivolous emails or messages in any quantity to other users of the district email system. Transmission of chain letters, spamming, pyramid schemes, and jokes are strictly prohibited. Spamming is sending an annoying or unnecessary message to a large number of people.
 13. Users will not use school district technology resources for political lobbying or solicitation of any kind. (OR) Users may not use the system for political lobbying, as defined by the state statute. District employees and students may use the system to communicate with their elected representatives and to express their opinion on political issues.
 14. Users will respect private passwords and will keep their password private. Users are responsible for the use of their individual account and should take all reasonable precautions to prevent others from being able to use their account. Under no conditions should a user provide their password to another person or logon to allow another to use their account unsupervised. Using passwords belonging to others will be considered a violation of school district policies.
 15. Users will not use the school district system to engage in bullying or cyberbullying in violation of the school district'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. All users shall abide by security restrictions on all systems and information.
1. Distributing or making your password or another person's password or access code available to other or otherwise attempting to evade, disable or "crack" passwords, desktop security systems,

- or other security precautions, or assisting others in doing so threatens work, privacy and the integrity of school district information, and is a serious violation of school district policy.
2. Attempts to “bypass” virus protection software are violations of district security procedures.
 3. Software or applications are generally installed by District technology staff. Software or applications may only be installed by employees with specific permission from the District.
- C. 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 also may be in violation of this policy as well as other school district policies. In situations when the school district receives a report of an unacceptable use originating from a non-school computer or resource, the school district shall 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
- D. 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.

III. FILTER

- A. With respect to any of its computers with Internet access, the School District 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, video, audio, text, or any digital media or content 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 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.

IV. 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.

V. 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 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 minor child's files and email files.
- 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 the school district system may be subject to review, disclosure or discovery under Minn. Stat. Ch. 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.

VI. ELECTRONIC RECORD RETENTION – EMAIL MESSAGES

Email messages are potentially official government records. According to the State of Minnesota, the content of the message determines whether it is a record and how long the message needs to be retained.

All email messages that fall under the “record” category will be archived to fulfill the obligations of accountability following the policies of the State of Minnesota.

- A. All district email for both students and staff is stored for a period of three years from date of receipt through a backup process. Backups follow a rotation of 4 Daily, 5 Weekly, 6 Monthly, 3 Yearly. As time progresses the backup sets are re-used and replaced with current data.

VII. WEB 2.0 APPLICATIONS

Use of Weblogs, Blogs, Wikis, Podcasts and other Internet interactive applications will be treated as a classroom space.

- A. Assignments will abide by policies and procedures in the Student Handbook, including those policies regarding plagiarism and acceptable use of technology.
- B. Personal information such as last names, family member names, passwords, email address, and personal addresses should not be posted. Photographs may be published if parent/guardian does not object.

VIII. INTERNET USE GUIDELINES

- 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. Technology tools, including appropriate use of the Internet, are expected components of the Waseca K-12 learning experience.
- B. The Internet Use Guidelines are published in student and faculty handbooks, and on the district website. These guidelines are reviewed on a regular basis. It is the parent/guardian’s responsibility to be knowledgeable of the published Internet Use Guidelines.

IX. 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 tapes, hard drives or servers, 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 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.

X. USER NOTIFICATION

- A. All users shall be notified of the school district policies relating to Internet use.
(at time of employment, and through handbooks)
- 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 hard 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 uses 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 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.

XI. PARENT/GUARDIAN RESPONSIBILITY

Parent/guardian is 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.

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)
Layshock v. Hermitage Sch. Dist., 412 F.Supp. 2d 502 (2006)
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 514 (Bullying Prohibition Policy)
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)
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)

Adopted: August 22, 1996
Reviewed: February 19, 2015

Dear Parent/Guardian,

Your son or daughter has access to the Internet in our school. Internet is a global information system with great educational potential. The use of the Internet is a privilege, and students are expected to use it appropriately.

Students in the Waseca Public Schools may use the Internet to participate in distance learning activities, to consult experts, to communicate with other students, and to access materials to meet their educational needs. Educational resources to fulfill curriculum expectations are identified by teachers.

One of the objectives of the Waseca Public Schools is to provide learners with the greatest access to appropriate information. The district has installed an Internet filter that is set to block inappropriate websites. However, because information on the Internet constantly changes, it is not possible to completely control the vast Internet environment for students. If students do encounter information that may be offensive, they are taught the appropriate action to take. Use of the Internet shall be consistent with school district policies and the mission of the school district.

Opinions, advice, services and other information expressed on the Internet are those of others and not those of the Waseca Public Schools. Students, staff and parents are advised that some network sites may contain inappropriate or offensive material. School administrators and staff do not condone the use of such materials and do not permit usage of those materials in the school environment. Students who knowingly use such materials in school will be dealt with according to the discipline policies of the district and the individual school. The building administrators reserve the right to terminate the access privileges of any student who violates the guidelines. Civil and criminal liability may be incurred by the user in the event of unauthorized use. Refer to Regulation 524 section I.

Please read the attached information and guidelines for Internet use.

Thank you.

Sincerely,

Building Principal

OVER

Internet Use Guidelines

Access to the Internet is a privilege, not a right. You may use it to locate, use, and exchange information. In doing so, you are expected to abide by the following guidelines. Violations of these guidelines will result in disciplinary action and possible loss of access privileges.

- * Use the Internet for educational purposes related to school or classroom activities.
- * Respect current school policies and behavior standards.
- * Be polite and use appropriate language.
- * Respect the rights of others.
- * Abide by current copyright laws and statutes. Acknowledge your sources of information and graphics.
- * Accurately represent yourself, but don't reveal your personal address or phone number or anyone else's.
- * Note that e-mail is not private. People who manage the system have access to electronic documents and website history.
- * Respect the network. Use Internet time and limited resources wisely.
- * Respect system security.
- * Use of Weblogs, Wikis, Podcasts and other Internet interactive applications will be treated as classroom space.
- * Abide by district guidelines for student publishing on the Internet. Any items produced by students will not be posted without their permission and that of their instructor and parents/guardians. If permission is granted, items will be considered fair use and available to the public.

Civil and criminal liability may be incurred by the user in the event of unauthorized use. Refer to Regulation 524 section I.

524-12F

INTERNET USE AGREEMENT – STUDENT

STUDENT

I have read and do understand the school district policies relating to safety and acceptable use of the school district computer system and the Internet and agree to abide by them. I further understand that should I commit any violation, my access privileges may be revoked, school disciplinary action may be taken, and/or appropriate legal action may be taken.

User's Full Name (please print):

User Signature:

Date:

PARENT OR GUARDIAN

As the parent or guardian of this student, I have read the school district policies relating to safety and acceptable use of the school district computer system and the Internet. I understand that this access is designed for educational purposes. The school district has taken precautions to eliminate controversial material. However, I also recognize it is impossible for the school district to restrict access to all controversial materials and I will not hold the school district or its employees or agents responsible for materials acquired on the Internet. Further, I accept full responsibility for supervision if and when my child's use is not in a school setting. I hereby give permission to issue an account for my child and certify that the information contained on this form is correct.

Parent or Guardian's Name (please print):

Parent or Guardian's Signature:

Date:

INTERNET USE AGREEMENT – EMPLOYEE

SCHOOL DISTRICT EMPLOYEE

I have read and do understand the school district policies relating to safety and acceptable use of the school district computer system and the Internet and agree to abide by them. I further understand that should I commit any violation, my access privileges may be revoked, school disciplinary action may be taken, and/or appropriate legal action may be taken.

User's Full Name (please print):

User Signature:

Date: