South Washington County Schools
Cottage Grove, MN

524 TECHNOLOGY ACCEPTABLE USE AND SAFETY POLICY

BELIEF STATEMENT

It is the belief of South Washington County Schools that students, staff, and community members should have access to district communication systems, networks, and an array of emerging technology resources to enhance the educational process of teaching, learning and the delivery of curriculum.

Each user is responsible for his/her use of technology, whether personal or district provided. It is a joint responsibility of district personnel and all users to become educated about the responsibilities and expectations of using technology.

I. PURPOSE

The purpose of this policy is to set forth policies and guidelines for the use of district and personal technology resources, access to the school district computer system and acceptable and safe use of digital resources, including electronic communications.

II. GENERAL STATEMENT OF POLICY

In making decisions regarding user access to the school district technology resources, including electronic communications, the school district considers its own stated educational mission, goals, and objectives. Access to the school district technology resources enables users to explore countless resources such as libraries, databases, bulletin boards, other resources which expand students' world view while interacting with people locally and globally. The school district expects that employees will blend thoughtful use of the school district technology resources throughout the curriculum and will provide guidance and instruction to students in their use. Digital citizenship instruction of students and staff will be mandatory.

III. LIMITED EDUCATIONAL PURPOSE

The school district is providing students and employees with access to the school district digital resources which includes, but is not limited to desktops, laptops, tablets, district maintained servers, networks, and 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 technology resources and Internet access through the district system to further educational and personal goals consistent with the mission of the school district, strategic plan and school policies. Uses which might be acceptable on a user's private personal account on another system may not be acceptable on this limited-purpose network.

IV. USE OF DIGITAL RESOURCES IS A PRIVILEGE

The use of the school district digital resources and 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, digital resources, 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. BRING YOUR OWN TECHNOLOGY (BYOT)

Personal technology may be connected to the District's network or systems if it complies with district standards and is compatible with the district systems. All BYOT (Bring Your Own Technology) attached or connected to the district network are subject to the same policies and procedures established for the use of district owned equipment. The use of BYOT must adhere to the district Acceptable Use Policy (AUP)

The student and parent/guardian must have signed and returned the AUP prior to using the device and accessing the district network. District technicians will not service, repair, or maintain any BYOT. District will not be held liable for personal content housed on the device. Any software residing on the BYOT must not interfere with the normal operation of district owned resources and must be properly licensed. District is not responsible for any physical damage, loss, or theft of the device. Internet usage or texting charges are the responsibility of the student. All BYOT must be clearly marked with the student's First and Last name. Students are responsible for taking the BYOT home each day and

returned the next day with a full charge. Students are responsible for keeping the BYOT in a secure location when not in use. Student use of BYOT must support the instructional activities of the classroom and must be turned off and put away when requested by a teacher. Students may use BYOT during non-instructional time only in adult supervised areas and at the discretion of the school.

VI. ACCEPTABLE USE GUIDELINES

A. Users must respect and protect the privacy of others by:

   1. Using only assigned accounts.

   2. Only viewing, using, or copying passwords, data, or networks to which they are authorized.

   3. Refraining from distributing private information about others or themselves.

B. Users must respect and protect the integrity, availability, and security of all electronic resources by:

   1. Observing all district Internet filters and posted network security practices.

   2. Reporting security risks or violations to a teacher or network administrator.

   3. Not destroying or damaging data, networks, or other resources that do not belong to them, without clear permission of the owner.

   4. Conserving, protecting, and sharing these resources with other users.

   5. Notifying a staff member or administrator of computer or network malfunctions through the creation of a service request.

C. Users must respect and protect the intellectual property of others by:

   1. Following copyright laws (not making illegal copies of music, games, or movies).

   2. Citing sources when using others' work (not plagiarizing).

D. Users must respect and practice the principles of community by:

1. Communicating only in ways that are kind and respectful.

2. Reporting threatening or discomforting materials to a teacher or administrator.

3. Not intentionally accessing, transmitting, copying, or creating material that violates the school's code of conduct (such as messages/content that are pornographic, threatening, rude, discriminatory, or meant to harass).

4. Not intentionally accessing, transmitting, copying, or creating material that is illegal (such as obscenity, stolen materials, or illegal copies of copyrighted works).

5. Not using the resources to further other acts that are criminal or violate the school's code of conduct.

6. Avoiding spam, chain letters, or other mass unsolicited mailings.

7. Refraining from buying, selling, advertising, or otherwise conducting business, unless approved as a school project.

8. Not using any personal or school district device, such as a tablet, smartphone, computer, camera, or other electronic device, to take or electronically capture during school hours or at a school sponsored event an image (including a picture, video, or audio recording) of another student(s) or school employee(s) and then, at any time, post, share, or distribute an image of another student(s) or school employee(s) if the posting, sharing, or distributing of that image results in disruption of school operations, could be reasonably anticipated to disrupt school operations, or violates the data privacy rights of others.

E. Users may, if in accord with the policy above:

1. Design and post web pages and other material from school resources.

2. Communicate electronically via tools such as email, chat, text, or videoconferencing (students require a teacher's permission).

3. Install or download software, if also in conformity with laws and licenses (students must be under the supervision of a teacher).

4. Use the resources for any educational purpose.

F. Consequences for Violation

Violations of these rules may result in disciplinary action, including the loss of a user's privileges to use the school's digital resources. Further discipline may be imposed in accordance with the Board's Code of Conduct up to and including suspension or expulsion depending on the degree and severity of the violation.

G. Supervision and Monitoring

The use of District owned information technology resources is not private. School and network administrators and their authorized employees monitor the use of information technology resources to help ensure that uses are secure and in conformity with this policy. Administrators reserve the right to examine, use, and disclose any data found on the school's information networks in order to further the health, safety, discipline, or security of any student or other person, or to protect property. They may also use this information in disciplinary actions, and will furnish evidence of crime to law enforcement. The district reserves the right to determine which uses constitute acceptable use and to limit access to such uses. The district also reserves the right to limit the time of access and use.

VII. 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, 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/designee 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.

VIII. CONSISTENCY WITH OTHER SCHOOL POLICIES

Use of the District technology resources 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 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 that all communications transmitted or received on the district system are PUBLIC INFORMATION and can be given to law enforcement agencies WITHOUT the user's prior consent.

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 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 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 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.

G. Works created by district employees in the course of their duties and using the district system are the property of the district as works made for hire.

X. 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.

C. The Internet Use Agreement form for students must be read and signed by the user, the parent or guardian, and the supervising teacher. The employee must sign the Internet Use Agreement form for employees. The form must then be filed at the school office. As supervising teacher's change, the agreement signed by the new teacher shall be attached to the original agreement.

XI. 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 storage media, hard drives or servers, or for delays or changes in or interruptions of service or misdeliveries 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's policies related 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 storage media, 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 may use technical means to limit student Internet access, these limits do not provide a foolproof means for enforcing the provisions of this acceptable use policy.

5. Notification that goods and services can be purchased over the Internet that could potentially result in unwanted financial obligations and that any financial obligation incurred by a student through the Internet is the sole responsibility of the student and/or the student's parents.

6. Notification that the collection, creation, reception, maintenance, and dissemination of data via the Internet, including electronic communications, is governed by Policy 406, Public and Private Personnel Data, and Policy 515, Protection and Privacy of Pupil Records

7. Notification that, should the user violate 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.

XIII. PARENTS' RESPONSIBILITY; NOTIFICATION OF STUDENT INTERNET USE

A. Outside of school, parents bear responsibility for the same guidance of Internet use as they exercise with information sources such as television, telephones, radio, movies, and other possibly offensive media. Parents are responsible for monitoring their student's use of the school district system and of the Internet if the student is accessing the school district system from home or a remote location.

B. Parents are herein notified that their students will be using school district resources/accounts to access the Internet and that the school district provides parents the option to request in writing alternative activities not requiring Internet access.

XIV. 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/guardian notifications, if necessary, to reflect the adoption of these guidelines and procedures.

C. The school district Internet policies and procedures are available for review by all parent/guardian, staff and members of the community.

D. Because of the rapid changes in the development of the Internet, 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)
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. § 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 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 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)

POLICY ADOPTED: February 17, 2009
POLICY REVIEWED: July, 2013; July 2015, September 15, 2016
POLICY REVISED: August 8, 2013; August 20, 2015, August 17, 2017, November 1, 2018; April 25, 2019, September 10, 2020