South St. Paul
Public Schools

Office of the Superintendent

104 – 5th Avenue South ● South St. Paul, MN 55075-2332● (651) 457-9465● (651)457-9485 Fax

Adopted: October 23, 2000

Revised: 6/28/04; 3/12/07; 10/27/08; 1/11/10; 8/24/15
7/25/16; 4/24/17; 8/13/18; 6/10/19; 5/26/20
6/14/21; 6/27/22; 6/26/23

536 STUDENT INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY

I. PURPOSE

The purpose of this policy is to set forth policies and guidelines for student access to district and school information technology, known in this document as "District Information Technology," including but not limited to district computers, devices, printers and other accessories, networks, Internet access, electronic communications, and third-party systems the district licenses and makes available to employees and students.

II. GENERAL STATEMENT OF POLICY

In making decisions regarding student and staff access to District Information Technology, the school district considers its own stated educational mission, goals, and objectives. Electronic information research skills are fundamental to preparation of citizens and future employees. Access to the school district computer system and to the Internet enables the school community to explore thousands of libraries, databases, bulletin boards, and other resources while exchanging messages with people around the world. The school district expects that faculty will blend thoughtful use of District Information Technology throughout the curriculum and will provide guidance and instruction to students in their use.

III. PURPOSE LIMITED TO EDUCATION

The school district provides students with access to District Information Technology. District Information Technology has a limited educational purpose, which includes use of the system for classroom activities, educational research and professional or career development. Students are expected to use the district system to further educational goals consistent with the school district's mission, strategic plan and 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 DISTRICT TECHNOLOGY RESOURCES IS A PRIVILEGE

The use of District Information Technology and its access to 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 District Information Technology or the Internet may result in one or more of the following consequences: suspension, cancellation or restriction of use or access privileges, payments for damages and repairs, discipline under other appropriate school district policies, including suspension or expulsion of students, or civil or criminal liability under other applicable laws.

V. BRING YOUR OWN DEVICE (BYOD)

A. A student's personal device may be connected to the District's network or systems if it complies with district standards and is compatible with the district systems. All BYOD devices attached or connected to the district network are subject to the same policies and procedures established for the use of district-owned equipment.

B. All use of BYOD devices must adhere to the district STUDENT INFORMATION TECHNOLOGY 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.

C. District technicians will not service, repair, or maintain BYOD devices. The District will not provide software for installation on BYOD devices. District will not be held liable or responsible for physical damage, loss or theft of the device, loss of personal content stored on the device, or charges incurred during use of the device.

D. Student use of BYOD must support classroom instructional activities and adhere to all instructions given by staff.

E. Students are prohibited from using any personal device as a hotspot to circumvent the district wireless network and content filters.

F. The district reserves the right to limit Wi-Fi connectivity for personal devices that are not approved for BYOD use.

VI. ACCEPTABLE USE GUIDELINES FOR DISTRICT INFORMATION TECHNOLOGY

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

1. Using only accounts assigned to them.

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.

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, offensive or discomforting materials to a staff member 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, defamatory or meant to harass or bully).

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.

E. Students may, if in accord with district policies and under direction of staff:

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

2. Communicate electronically via tools such as email, chat, text, or videoconferencing.

3. Install or download software, in conformity with laws and licenses.

4. Use technology resources for educational purposes.

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 district policies up to and including suspension or expulsion depending on the degree and severity of the violation.

VII. CONSISTENCY WITH OTHER SCHOOL POLICIES

Use of the District Information Technology 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 District Information Technology, 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 for content they store 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 content their child has stored on the district system to the extent possible without compromising other students' privacy. Parents have the right to request the suspension of their child's individual account at any time.

E. Students 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. STUDENT INFORMATION TECHNOLOGY ACCEPTABLE USE AGREEMENT

A. The proper use of District Information Technology systems, including the Internet, and the educational value to be gained from proper 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 Student Information Technology Acceptable Use Agreement must be read and signed by the user and a parent or guardian prior to the student being granted access to the district system. Signed agreements will be retained by the district. The district may require students to re-sign the agreement periodically thereafter as Technology changes require. The content of this agreement shall be included in each school's student/parent handbook as an annual review.

X. LIMITATION ON SCHOOL DISTRICT LIABILITY

Use of District Information Technology 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 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 District Information Technology 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 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 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.

5. 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.

6. 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 or the student's parents.

7. Notification that should a student violate the school district's Acceptable Use Policy, the student’s access privileges may be revoked, 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. PARENT 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 will provide parents the option to request in writing alternative activities not requiring Internet access.

XIII. IMPLEMENTATION AND POLICY REVIEW

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

B. This policy will be reviewed annually and the administration will recommend changes as necessary.

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

XIV. CONTENT FILTERING

A. With respect to any of its computers with Internet Access, the school district will monitor the online activities of both minors and adults 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, 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. 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 interaction with other individuals on social networking websites and in chat rooms and cyber bullying awareness and response.

F. Although student use of the Internet at school is subject to content filtering and is supervised by staff, we cannot guarantee that students will not gain access to inappropriate materials. We encourage parents to have a discussion with their children about values and how those beliefs should guide student activities while using the Internet.

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.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)
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)