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; 8/13/18
6/10/19; 5/26/20; 6/14/21; 6/27/22; 6/26/23

474 STAFF INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY

I. PURPOSE

The purpose of this policy is to set forth policies and guidelines for staff 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.
For the purposes of this policy, "staff" includes all employees, volunteers, contractors and other outside agencies working on the district's behalf who are granted access to District Information Technology.

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 staff with access to District Information Technology. District Information Technology has a limited educational purpose, which includes its use for classroom activities, educational research, professional or career development, and the general operation of the district and its schools. Staff are expected to use District Information Technology to further educational and professional 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 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 termination of employment or civil or criminal liability under other applicable laws.

V. ACCEPTABLE USE EXPECTATIONS

A. The following Acceptable Use Expectations apply to all staff using District Information Technology:

1. Staff will not use District Information Technology to access, review, create, upload, download, store, print, post, distribute or otherwise publish any content that:

   a) is pornographic;

   b) promotes domestic violence;

   c) promotes crimes against children;

   d) promotes illegal drugs;

   e) threatens physical harm to another person;

   f) incites violence at school;

   g) creates, or could reasonably be predicted to create, a material and substantial disruption to school operations;

   h) creates, or could reasonably be predicted to create, an environment that is not conducive to learning;

   i) significantly interferes with the learning of students;

   j) ridicules, maligns, disparages, unlawfully discriminates, harasses, or otherwise expresses bias based on race, color, creed, religion, national origin, sex, marital status, status with regard to public assistance, familial status, disability, sexual orientation, or age; or

   k) jeopardizes the security or safety of students or staff at school.

2. Staff will not use District Information Technology to engage in any illegal act or violate any local, state or federal statute or law.

3. Staff will not use District Information Technology 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 system's security, and will not use District Information Technology in such a way as to disrupt the use of the system by other users.

4. Staff will not use District Information Technology to gain unauthorized access to information resources or to access another person's materials, information or files without direct permission of that person.

5. Staff will not use the District Information Technology to post private information about another person or to post personal contact information about themselves or other persons including, but not limited to, addresses, telephone numbers, school addresses, work addresses, identification numbers, account numbers, access codes or passwords, and 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 staff 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) Staff creating or posting school-related webpages may include personal contact information about themselves on a webpage. However, staff 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; or

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

In addition, prior to posting any personal contact or personally identifiable information on a school-related webpage, staff shall obtain written approval of the content of the postings from the building administrator.

c) These prohibitions specifically prohibit staff from using the District Information Technology to post personal information about staff members or students on social media networks.

6. Staff will protect and secure District Information Technology and the confidential information it stores and makes available by:

a) Keeping their user account information, including usernames and passwords, private;

b) Not attempting to gain unauthorized access to District Information Technology or use District Information Technology to gain unauthorized access to any other system;

c) Not using another person's account, or use computer accounts, access codes or network identification other than those assigned to them by the district;

d) Not allowing anyone other than themselves to use their login credentials to access District Information Technology;

e) Always locking or logging off district computers and devices connected to district resources before leaving them unattended, including the use of personal devices offsite that access District Information Technology;

f) Not attempting to encrypt messages and records on District Information Technology with tools other than those provided or approved by the district.

7. Staff will observe and comply with copyright laws, license agreements, and other intellectual property rights.

8. Staff will not use District Information Technology, including their district email address, for personal purposes, including personal shopping, personal social networking, personal subscriptions and other activities not related to their job duties or the district mission, vision and strategic plan.

9. Staff will not use District Information Technology for the conduct of a business, for unauthorized commercial purposes or for financial gain unrelated to the mission of the school district. Staff will not use the school district system to offer or provide goods or services or for product advertisement.

10. Staff will not use District Information Technology to engage in bullying or cyberbullying as defined in Policy (514 Bullying Prohibition). This prohibition includes using any technology or other electronic communication off district premises to the extent that student learning or the school environment is substantially and materially disrupted.

B. Staff engaging in unacceptable uses of District Information Technology when off district premises may also be in violation of this and other school district policies. 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.

C. If Staff using District Information Technology inadvertently access unacceptable materials or an unacceptable internet site, they will immediately disclose the inadvertent access to their direct supervisor and/or 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 a building or district administrator.

VI. CONSISTENCY WITH OTHER SCHOOL POLICIES

Use of District Information Technology and use of the internet shall be consistent with school district policies and the mission of the school district.

VII. LIMITED EXPECTATION OF PRIVACY

A. By authorizing use of 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 their actions and content stored on District Information Technology.

B. Routine maintenance and monitoring of District Information Technology may lead to 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. School district employees should be aware that data and other materials in files maintained on District Information Technology may be subject to review, disclosure or discovery under Minnesota Statutes, Chapter 13 (the Minnesota Government Data Practices Act) and may be subject to Freedom of Information Act requests.

E. 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 District Information Technology.

VIII. INFORMATION TECHNOLOGY ACCEPTABLE USE AGREEMENT

A. The proper use of District Information Technology systems and the educational value to be gained from proper use, is the joint responsibility of students, parents and employees of the school district.

B. The Staff Information Technology Acceptable Use Agreement must be signed by staff at the start of employment, and periodically thereafter as Information Technology changes require.

IX. 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 diskettes, 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.

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 removable 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; and
    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) and Policy 515 (Protection and Privacy of Pupil Records).
5. Notification that, even though the school district may use technical means to limit student and staff internet access, these limits do not provide a foolproof means for enforcing the provisions of this Acceptable Use policy.
6. Notification that staff are personally responsible for unauthorized financial obligations incurred over the Internet or other electronic means.
7. Notification that should the user violate the school district's Acceptable Use Policy, the employee's access privileges may be revoked, and appropriate disciplinary and/or legal action may be taken.
8. Notification that all provisions of the Acceptable Use Policy are subordinate to local, state and federal laws.

XI. IMPLEMENTATION AND POLICY REVIEW

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

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

XII. INTERNET 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. Pornographic; or
3. Harmful to minors.

B. The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that:

1. When 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. When 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. When used by an adult, an administrator, supervisor or other person authorized by the Superintendent may disable the technology protection measure to enable access for bona fide research or other lawful purposes.

XIII. STAFF PERSONAL EQUIPMENT USE

A. All staff are provided access to dedicated or shared computing devices as needed for the performance of their duties.

B. Staff may connect personal devices to the district's guest network.

C. The district may restrict connection bandwidth of some or all personal devices or otherwise block access in order to prioritize the district's learning and other operations, and to protect District Information Technology.

D. Staff are responsible for ensuring that any connected personal device has been updated with all applicable security updates for its operating system and software, and has appropriate virus and malware protection installed and activated.

E. Use of personal devices brought onto school property must adhere to the policies and guidelines of this policy.

F. Staff are prohibited from using personal computing devices as wireless hotspots to circumvent the district wireless network and content filters.

G. District Technology staff cannot provide direct assistance with the configuration, installation or use of personal computing devices.

XIV. STAFF SOCIAL MEDIA USE

A. **Social Media** is defined as the variety of online resources that allow people to communicate, share information, photos, videos and audio, and exchange text and other multimedia files with others through an online or cellular network platform. Examples of social media include, but are not limited to, websites, blogs, wikis, social networks, online forums, virtual worlds, and such social networks as Facebook, Twitter, LinkedIn, Flickr, YouTube, Snapchat, and Instagram.

B. **Personal Social Media Use** is defined as the use of social media to communicate with friends and family, advance one's employment or career beyond the scope of one's district duties, engage in business activities, or publicly express personal opinions.

C. **Professional Social Media Use** is defined as use of social media that is directly related to job duties and is performed with a supervisor's permission. Examples include but are not limited to use that is integrated into classroom instruction, tied directly to professional learning, or needed to communicate with partner agencies or job-related networks.

D. **Establishment and Regulation of Social Media Sites.** The district may establish social media sites and accounts for the district and its schools and may monitor and regulate the content of information on its sites and accounts. The district's Facebook, Twitter and Instagram accounts are examples of a district social media site. The Superintendent or their designee, must approve the establishment of all district social media sites and school media sites.

E. **General Guidelines**

1. **Speaking on Behalf of the District.** The Superintendent or their designee is the authorized spokesperson for the district. Without prior written authorization from the Superintendent, employees may not use social media during the duty day or outside the duty day to state or imply:

   a) that they are speaking for, or on behalf of, the district;

   b) that they are authorized to speak for, or on behalf of, the district; or

   c) that their views represent the views of the district.

2. **Branding of Personal Social Media Accounts with District Logos, Names or Trademarks.**

   a) Staff will not brand their personal accounts in such a way that they may be mistaken as officially representing the district or its schools. Staff are additionally encouraged to include disclaimers on their personal social media profiles to eliminate any confusion and clarify that they are speaking as private individuals, and not as district employees, and that their views do not necessarily reflect the views of the district.

3. **Non-Protected Speech**

   a) As a general matter, public employees have a First Amendment right to use personal social media to express their views on matters of public interest. However, this right is not absolute. When public employees make statements pursuant to their official job duties, they are not speaking as private citizens for First Amendment purposes and, therefore, their speech is not constitutionally protected. When employees are speaking pursuant to their official job duties, they must follow their supervisor's directives and the district approved curriculum. Employees may be disciplined for speech that is not protected under the Constitution or a federal or state law.

4. **Prohibition of Speech that Interferes with Efficient.**

a) Even when speech touches on a matter of public concern and is not pursuant to an employee's job duties, an employee's free speech rights must be balanced against the district's right to maintain efficient operations and an environment that is conducive to working and learning. When balancing these rights, the courts have held that a public employee's speech is not protected if it would create disharmony in the workplace, impede the employee's ability to perform his or her job duties, significantly impair the working relationship with other employees who work closely with the speaker, or significantly harm the employer's image. Accordingly, employees may be disciplined for speech that creates disharmony in the workplace, impedes the employee's ability to perform his or her job duties, significantly impairs the working relationship with other employees who work closely with the speaker, or significantly harms the district's image.

5. **Maintaining Appropriate Boundaries.**

a) All employees must maintain professional boundaries with students. Employees may not engage in communications with students that give the impression of peer-to-peer communications, unless the employee and student are related. Additionally, employees may not have extensive social involvement or develop personal or private relationships with individual students through social media, unless they are closely related.

F. Social Media Use During the Duty Day

1. Staff may engage in Professional Social Media Use during work hours.

2. Staff are encouraged to create separate professional social media accounts using their district email addresses for work purposes only. Personal accounts may not be used when using social media with students.

3. Personal Social Media Use using District Information Technology is prohibited during work hours.

4. Incidental Personal Social Media Use on personal devices is allowed during work hours to the extent that it does not interfere with job duties or responsibilities as determined by supervisors.

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)