

[Language in red is proposed to be added in accordance with MSBA's model policy changes to align policies with statutory provisions adopted during the 2023 legislative session. Language required due to statutory changes can be adopted by the board in a single meeting. The red-lined changes closely track the new statutory language. As always, text in blue indicates changes initiated by the district. ]

Policy 524

## Students

### Internet Acceptable Use and Safety Policy

#### I. Purpose

~~The purpose of this policy is to set forth policies and~~ This policy sets forth guidelines for access to the school district computer system and acceptable and safe use of the Internet, including electronic communications.

#### II. General Statement of Policy

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

#### III. Definitions

- A. "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.

B. "School-issued device" means hardware or software that the school district, acting independently or with a technology provider, provides to an individual student or employee for that student's or employee's dedicated personal use. A school-issued device includes a device issued through a one-to-one program.

C. "Technology provider" means a person who:

1. contracts with the school district, as part of a one-to-one program or otherwise, to provide a school-issued device for student use; and
2. creates, receives, or maintains educational data pursuant or incidental to a contract with the school district.

### III. Limited Educational Purpose

The school district is providing students and employees with access to the district computer system, which includes Internet access. The purpose of the system is more specific than providing students and employees with general access to the Internet. **The Internet is accessible in the district for use as an educational resource. Other use is prohibited.** ~~The 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 Internet access through the district system to further educational and personal goals consistent with the mission of the district 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 System is a Privilege

The use of the school district system 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 district system 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 district policies, including suspension, expulsion, exclusion, or termination of employment; or civil or criminal liability under other applicable laws.

### V. Unacceptable Uses

A. **While not an exhaustive list,** the following uses of the school district

system and Internet resources or accounts are considered unacceptable:

1. Users will not use the district system to create, record, access, review, upload, download, store, print, post, receive, transmit, or distribute:
  - a. Pornographic, obscene, or sexually explicit material or other visual depictions;
  - b. Obscene, abusive, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, or sexually explicit language or images;
  - c. Materials that use language or images that are inappropriate in the education setting or disruptive to the educational process;
  - d. Materials that use language or images that advocate violence or discrimination toward other people, or that may constitute harassment, or discrimination, or that threatens the safety of others;
  - e. Orders for shopping online during time designated as work or academic time by the district; ~~and~~
  - f. Storage of personal photos, videos, music, or files not related to educational and extra-curricular purposes for any length of time; and
  - g. Use of social media for non-academic purposes and/or use of social media by students under the age of 13.
2. Users will not use the 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 district system to engage in any illegal act or violate any local, state, or federal statute or law.
4. Users will not use the 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 engaging in "spamming," or by any other means, will not tamper with, modify, or change the district system software, hardware, or wiring, or take any action to violate the district's security system,

and will not use the district system in such a way as to disrupt the use of the system by other users.

5. Users will not use the district system to gain unauthorized access to information resources, or to access another person's materials, information, or files without the direct permission of that person. [This clause is not applicable to district technology staff who need to access a system due to a threat, troubleshooting, diagnosing issues, or other IT-related needs that uphold this and other district policies.](#)
6. Users will not use the 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, 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, 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 employee contact information on district webpages or communications between employees and other individuals when such communications are made for education-related purposes (i.e., communications with parents/guardians or other staff members related to students). Refer to Policy 515 (Protection and Privacy of Student Records) for direction on directory information for students and how this can be used.
  - b. Employees creating or posting school-related webpages may include personal contact information about themselves on a webpage. However, employees may not post personal contact information or other personally identifiable information about students unless:
    - (1) such information is classified by the district as directory information and verification is made that the 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~~ [district policy](#); or
    - (2) such information is not classified by the 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~~ [district policy](#).

In addition, prior to posting any personal contact or personally identifiable information on a school-related webpage, employees ~~shall~~ [will](#) obtain written approval of the content of the postings from the building administrator.

- c. These prohibitions specifically prohibit a user from utilizing the district system to post personal information about a user or another individual on social networks, including, but not limited to, social networks such as “Facebook,” “Twitter,” “Instagram,” “Snapchat,” “TikTok,” ~~and~~ “Reddit,” and similar websites or applications.
7. ~~Users must keep all account information and passwords on file with the designated district official.~~ Users will not attempt to gain unauthorized access to the district system or any other system through the 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 district system may not be encrypted without the permission of appropriate school authorities.
  8. Users will not use the 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.
  9. Users will not use the district system for conducting business, for unauthorized commercial purposes, or for financial gain unrelated to the mission of the district. Users will not use the district system to offer or provide goods or services or for product advertisement. Users will not use the district system to purchase goods or services for personal use without authorization from the appropriate district official.
  10. Users will not use the district system to engage in [harassment](#), [bullying](#), or [cyberbullying](#) in violation of [district policy](#). ~~the district’s Policy 514 (Bullying Prohibition) Policy (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. A student or employee who engages in the foregoing unacceptable uses

of the Internet or district equipment when they are off district premises may be in violation of this policy, in addition to other district policies. Regardless of whether district equipment was used for the unacceptable use, the district has the right and may be obligated to regulate the off-campus speech or conduct of its students or employees when that speech or conduct materially disrupts the school environment, involves substantial disorder, or constitutes an invasion of the rights of others. Examples of such violations include, but are not limited to, where the ~~school~~-district system is compromised or if a ~~school~~-district employee or student is negatively impacted. If the district receives a report of an unacceptable use originating from a non-school computer or resource, the district may 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 district computer system and the Internet and discipline under other appropriate 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~~ will immediately disclose the inadvertent access to an appropriate ~~school~~-district official. In the case of a district employee, the immediate disclosure ~~shall~~ will 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.

## VI. Filter

### ~~Alternative No. 4~~

- A. With respect to any of its computers with Internet access, the school district will ~~monitor~~ filter 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, 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.~~

~~EB.~~ Software filtering technology ~~shall~~ will be narrowly tailored and ~~shall~~ will not discriminate based on viewpoint.

~~BC.~~ An administrator, supervisor, or other person authorized by the ~~S~~superintendent may disable the technology protection measure, during use by an adult, to enable access for bona fide research or other lawful purposes.

~~ED.~~ The ~~school~~district will educate students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat ~~rooms~~ -enabled environments and cyberbullying awareness and response.

#### VII. Consistency with Other School [District](#) Policies

Use of the school district computer system and use of the Internet ~~shall~~ will be consistent with district policies and the mission of the district.

#### VIII. Limited Expectation of Privacy

A. By authorizing use of the school district system, the 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 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 district policy, or the law.

C. An individual investigation or search will be conducted if ~~school~~ [district](#) authorities have a reasonable suspicion that the search will uncover a violation of law or district policy.

D. Parents/guardians have the right at any time to investigate or review the contents of their child's files and e-mail [email](#) files in accordance with ~~the school district's Protection and Privacy of Pupil Records Policy. 515~~ [\(Protection and Privacy of Pupil Records\)](#). Parents/guardians have the right to request the termination of their child's individual account at any

time.

- E. ~~School-d~~District employees should be aware that the district retains the right at any time to investigate or review the contents of their files and ~~e-mail~~ email files. In addition, district employees should be aware that data and other materials in files maintained on the 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 district policies conducted through the district system.

#### IX. 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/guardians, and employees of the school district.
- B. This policy requires the permission of and supervision by the ~~school's~~ district's designated professional staff before a student may use a ~~school~~ district account or resource to access the Internet.
- C. The Internet ~~Acceptable~~ Use Agreement form for students must be read and signed by the user, and the parent/ or guardian, ~~and the supervising teacher~~. This form is signed annually via the Parent Portal. The Internet ~~Acceptable~~ Use Agreement form for employees must be signed by the employee. The form must then be filed at the school office or with a department supervisor. ~~As supervising teachers change, the agreement signed by the new teacher shall will be attached to the original agreement.~~

#### X. 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 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~~, cloud services, 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 district is not responsible for the accuracy or quality of any advice or information obtained through or stored on the district system. The district will not be responsible for financial obligations arising through unauthorized use of the district system or the Internet.

#### XI. User Notification



- A. All users ~~shall~~ will be notified of the school district policies relating to Internet use.
- B. This notification ~~shall~~ will include the following:
1. Notification that Internet use is subject to compliance with ~~school~~ district policies.
  2. Disclaimers limiting the district's liability relative to:
    - a. Information stored on ~~district-diskettes~~ cloud services, tapes, hard drives, or servers.
    - b. Information retrieved through district computers, networks, or online resources.
    - c. Personal property used to access district computers, networks, or online resources.
    - d. Unauthorized financial obligations resulting from use of district resources/accounts to access the Internet.
  3. A description of the privacy rights and limitations of ~~school~~-district sponsored/managed Internet accounts.
  4. Notification that, even though the 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/guardians.
  6. Notification that the collection, creation, reception, maintenance, and dissemination of data via the Internet, including electronic communications, is governed by district policy. Policy 406, (~~Public and Private Personnel Data~~), and Policy 515, (~~Protection and Privacy of Pupil Records~~).
  7. Notification that, should the user violate the 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.

## XII. Parents'/Guardians' Responsibility; Notification of Student Internet Use

- A. Outside of school, parents/guardians 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/guardians are responsible for monitoring their student's use of the school district system and of the Internet if the student is accessing the district system from home or a remote location.
- B. Parents/guardians will be notified that their students will be using ~~school~~ district resources/accounts to access the Internet and that the district will provide parents/guardians the option to request alternative activities not requiring Internet access. This notification should include:
  1. A copy of the user notification form provided to the student user.
  2. A description of parent/guardian responsibilities.
  3. A statement that the Internet **Acceptable** Use Agreement must be signed by the user, **and** the parent/~~or~~ guardian, ~~and the supervising teacher~~ prior to use by the student.
  4. A statement that the district's acceptable use policy is available for parental/guardian review.

## XIII. Notification Regarding Technology Providers

- A. Within 30 days of the start of each school year, the school district must give parents/guardians and students direct and timely notice, by United States mail, e-mail, or other direct form of communication, of any curriculum, testing, or assessment technology provider contract affecting a student's educational data. The notice must:
  1. identify each curriculum, testing, or assessment technology provider with access to educational data;
  2. identify the educational data affected by the curriculum, testing, or assessment technology provider contract; and
  3. include information about the contract inspection and provide contact information for a school department to which a parent/guardian or student may direct questions or concerns regarding any program or activity that allows a curriculum, testing, or assessment technology provider to access a student's

educational data.

- B. A contract between a technology provider and the ~~school~~-district must include requirements to ensure appropriate security safeguards for educational data. The contract must require that:
  - 1. the technology provider's employees or contractors have access to educational data only if authorized; and
  - 2. the technology provider's employees or contractors may be authorized to access educational data only if access is necessary to fulfill the official duties of the employee or contractor.
- C. Upon request, the ~~school~~-district must provide parents/guardians and students an opportunity to inspect a complete copy of any contract with a technology provider.
- D. All educational data created, received, maintained, or disseminated by a technology provider pursuant or incidental to a contract with ~~a public~~ ~~educational agency or institution~~ the district are not the technology provider's property.

#### XIV. School-issued Devices

- A. Except as provided in paragraph ~~C~~B, the school district or a technology provider must not electronically access or monitor:
  - 1. any location-tracking feature of a school-issued device;
  - 2. any audio or visual receiving, transmitting, or recording feature of a school-issued device; or
  - 3. student interactions with a school-issued device, including but not limited to keystrokes and web-browsing activity.
- B. The ~~school~~-district or a technology provider may only engage in activities prohibited by paragraph B A if:
  - 1. the activity is limited to a noncommercial educational purpose for instruction, technical support, or exam-proctoring by ~~school~~-district employees, student teachers, staff contracted by the ~~school~~-district, a vendor, or the Minnesota Department of Education, and notice is provided in advance;
  - 2. the activity is permitted under a judicial warrant;
  - 3. the ~~school~~-district is notified or becomes aware that the device is

missing or stolen;

4. the activity is necessary to respond to an imminent threat to life or safety and the access is limited to that purpose;
  5. the activity is necessary to comply with federal or state law, ~~including but not limited to Minnesota Statutes section 121A.034;~~ or
  6. the activity is necessary to participate in federal or state funding programs, including but not limited to the E-Rate program.
- C. If the ~~school~~-district or a technology provider interacts with a school-issued device as provided in paragraph C B, clause 4, it must, within 72 hours of the access, notify the student to whom the school-issued device was issued or that student's parent/guardian. Such notice must include a written description of the interaction, including which features of the device were accessed and a description of the threat. ~~If this notice is not required at any time when the notice itself would pose an imminent threat to life or safety, but this notice must instead be given within 72 hours after that imminent threat has ceased.~~ In the instance in which notification would pose a threat to life or safety, notification will instead be given within 72 hours following the resolution of the imminent threat.

#### XV. Cell Phone Use

- A. Students are prohibited from using a cell phone or other electronic communication device to engage in conduct prohibited by school district policies including, but not limited to, cheating, bullying, harassment, and malicious and sadistic conduct.
- B. If the ~~school~~-district has a reasonable suspicion that a student has violated a ~~school~~ district policy, rule, or law by use of a cell phone or other electronic communication device, the ~~school~~-district may search the device. The search of the device will be reasonably related in scope to the circumstances justifying the search.
- C. Students who use an electronic communication device during the school day and/or in violation of ~~school~~-district policies may be subject to disciplinary action pursuant to the district's ~~school's~~ discipline policy. In addition, a student's cell phone or electronic communication device may be confiscated by the district ~~school~~ and, if applicable, provided to law enforcement. Cell phones or other electronic communication devices that are confiscated and retained by the ~~school~~-district will be returned in accordance with school building procedures.

#### XVI. Limit on Screen Time for Children in Preschool and Kindergarten

A child in a publicly funded preschool or kindergarten program may not use an individual-use screen, such as a tablet, smartphone, or other digital media, without engagement from a teacher or other students. This section does not apply to a child for whom the district ~~school~~ has an individualized family service plan, an individualized education program, or a 504 plan in effect.

XIII XVII. 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~~ **will** be an addendum to this policy.
- B. The administration ~~shall~~ **will** revise the user notifications, including student and parent/guardian notifications, if necessary, to reflect the adoption of these guidelines and procedures.
- C. The district Internet policies and procedures are available for review by all parents, guardians, staff, and members of the community.
- D. ~~Because of the rapid changes in the development of the Internet, the school board shall~~ **will** conduct an annual review of this policy.

Legal References:

Minn. Stat. Ch. 13 (Minnesota Government Data Practices Act)  
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. § 1232g (Family Educational Rights and Privacy Act)  
47 U.S.C. § 254 (Children’s Internet Protection Act of 2000 (CIPA))  
~~47 C.F.R. § 54.520 (FCC rules implementing CIPA)~~ [Children’s Internet Protection Act](#)  
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 [Aet Aid](#))  
*v B.L.*, 594 U.S., 141 S. Ct. 2038 (2021)  
*Tinker v. Des Moines Indep. Cmty. Sch. Dist.*, 393 U.S. 503 (1969)  
*United States v. Amer. Library Assoc.*, 539 U.S. 194 (2003)  
*Sagehorn v. Indep. Sch. Dist. No. 728*, 122 F.Supp.2d 842 (D. Minn. 2015)  
*R.S. v. Minnewaska Area Sch. Dist. No. 2149*, 894 F.Supp.2d 1128 (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 (8<sup>th</sup> Cir. 2012)  
*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)~~

[Policy 413 \(Harassment and Violence Prohibition, Students and Employees\)](#)

~~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 Interviews by Outside Agencies)~~

~~MSBA/MASA Model Policy 521 (Student Disability Nondiscrimination)~~

~~MSBA/MASA Model Policy 522 (Title IX Sex Nondiscrimination Policy, Grievance Procedures and Process)~~

[Policy 601 Educational Competencies, Academic Standards and Instructional Curriculum](#)

~~MSBA/MASA Model Policy 603 (Curriculum and Program Review and Development)~~

~~MSBA/MASA Model Policy 604 (Instructional Curriculum)~~

~~MSBA/MASA Model Policy 606 (Selection and Objection of Instructional Textbooks, and Instructional Materials and Content)~~

[Policy 634 \(Electronic Technologies Acceptable Use\)](#)

~~MSBA/MASA Model Policy 806 (Crisis Emergency Management Policy)~~

~~MSBA/MASA Model Policy 904 (Distribution or Display of Materials on School District Property by Nonschool Nondistrict Persons or Organizations)~~

Policy

adopted:

8/8/22

INDEPENDENT SCHOOL DISTRICT NO. 273

Edina, Minnesota