POLICY MANAGEMENT
Adopted: 2016
Reviewed/ Revised: 11/16/2023*, 10/13/2026**
Mandatory: Yes
Frequency: Y
Annual Distribution: Website

524 – Internet Acceptable Use and Safety Policy

Purpose

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

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. Electronic information research skills are now fundamental to preparation of citizens and future employees. Access to the school district computer system and to the Internet enables students and employees 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 the school district computer system and the Internet throughout the curriculum and will provide guidance and instruction to students in their use.

Policy Specifics

Limited Educational Purpose

The school district is providing students and employees with access to the school 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 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 Internet access through the district system to further educational and personal goals consistent with the mission of the school 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.

Use of System is a Privilege

Access restrictions and discipline shall comply with applicable Minnesota pupil-dismissal law and IDEA, Section 504, and ADA protections. The school shall preserve required instruction, disability-related

services, and accessible alternatives; an access restriction shall not itself deny a free appropriate public education.

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

Unacceptable Uses

While not an exhaustive list, the following uses of the school district system and Internet resources or accounts are considered unacceptable:

Users will not use the school district system to access, review, upload, download, store, print, post, receive, transmit, or distribute:

- pornographic, obscene, or sexually explicit material or other visual depictions that are harmful to minors;
- obscene, abusive, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, or sexually explicit language;
- materials that use language or images that are inappropriate in the education setting or disruptive to the educational process;
- information or materials that could cause damage or danger of disruption to the educational process;
- materials that use language or images that advocate violence or discrimination toward other people (hate literature) or that may constitute harassment or discrimination.
- Users will not use the school district system to knowingly or recklessly post, transmit, or distribute false or defamatory information about a person or organization, or to harass another person, or to engage in personal attacks, including prejudicial or discriminatory attacks.
- Users will not use the school district system to engage in any illegal act or violate any local, state, or federal statute or law.
- Users will not use the school district system to vandalize, damage, or disable the property of another person or organization, will not make deliberate attempts to degrade or disrupt equipment, software, or system performance by spreading computer viruses or by any other means, will not tamper with, modify, or change the school district system software, hardware, or wiring or take any action to violate the school district's security system, and will not use the school district system in such a way as to disrupt the use of the system by other users.
- Users will not use the school district system to gain unauthorized access to information resources or to access another person's materials, information, or files without the implied or direct permission of that person.

- Users will not use the school district system to post private information about another person, personal contact information about themselves or other persons, or other personally identifiable information, including, but not limited to, addresses, telephone numbers, 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.
- This paragraph does not prohibit the posting of employee 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).
- 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:
- 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
- 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, employees shall obtain written approval of the content of the postings from the building administrator.
- These prohibitions specifically prohibit a user from utilizing the school 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," "Reddit," and similar websites or applications.
- Users shall safeguard passwords and authentication factors and use school-authorized account-management and recovery procedures. Staff shall not require disclosure of personal-account passwords. Authorized administrators may manage school accounts through approved administrative tools. Users will not attempt to gain unauthorized access to the school district system or any other system through the school district system, attempt to log in through another person's account, or use computer accounts, access codes, or network identification other than those assigned to the user. Messages and records on the school district system may not be encrypted without the permission of appropriate school authorities.

- Users will not use the school district system to violate copyright laws or usage licensing agreements, or to use protected works without permission, a valid license, or an applicable legal exception such as fair use, 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.
- Users will not use the school district system for conducting business, for unauthorized commercial purposes, or for financial gain unrelated to the mission of the school district. Users will not use the school district system to offer or provide goods or services or for product advertisement. Users will not use the school district system to purchase goods or services for personal use without authorization from the appropriate school district official.
- Users will not use the school district system to engage in bullying or cyberbullying in violation of the school district's Bullying Prohibition Policy. 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.
- The school district has a special interest in regulating off-campus speech that materially disrupts classwork or involves substantial disorder or invasion of the rights of others. A student or employee engaging in the foregoing unacceptable uses of the Internet when off school district premises also may be in violation of this policy as well as other school district policies. Examples of such violations may include, but are not limited to, serious or severe bullying or harassment targeting particular individuals, threats aimed at teachers or other students, failure to follow rules concerning lessons, the writing of papers, the use of computers, or participation in other online school activities, and breaches of school security devices. 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. Students or employees may be subject to disciplinary action for such conduct, including, but not limited to, suspension or cancellation of the use or access to the school district computer system and the Internet and discipline under other appropriate school district policies, including suspension, expulsion, exclusion, or termination of employment.

Off-campus enforcement shall respect applicable constitutional expression rights and the school's reduced authority over students' private off-campus speech. Mere offensiveness or disagreement with a viewpoint does not establish a lawful basis for discipline. Administrators shall identify the school-related basis and evidence supporting intervention, considering material disruption, threats, harassment, and other legally recognized grounds and the distinct protections applicable to employee speech.

If a user inadvertently accesses unacceptable materials or an unacceptable Internet site, the user shall immediately disclose the inadvertent access to an appropriate school

district official. In the case of a school district employee, the immediate disclosure shall be to the employee's immediate supervisor and/or the building administrator. This disclosure may serve as a defense against an allegation that the user has intentionally violated this policy. In certain rare instances, a user also may access otherwise unacceptable materials if necessary to complete an assignment and if done with the prior approval of and with appropriate guidance from the appropriate teacher or, in the case of a school district employee, the building administrator.

An assignment or permission does not authorize unlawful material or disabling a required CIPA protection measure during use by a minor. Any lawful instructional exception remains subject to applicable filtering, privacy, and age-appropriate safeguards.

Filter

With respect to any of its computers with Internet access, the school district will monitor minors' online activities as required by CIPA when applicable and employ applicable technology protection measures during use by minors and adults. Monitoring shall comply with the School-Issued Devices and Limited Expectation of Privacy sections. The technology protection measures utilized will block or filter Internet access to any visual depictions that are:

Obscene;

Child pornography; or

Harmful to minors, during use by minors.

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

Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; and

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

Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

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

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.

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.

The school shall satisfy Minnesota Statutes, section 125B.15, including its statutory expense limitation. When receiving federal support subject to CIPA, the school shall meet the applicable filtering, Internet-safety-policy, minor-monitoring, education, certification, and public-notice requirements. CIPA does not require tracking every user's Internet activity.

Consistency with other School Policies

Authorized Applications and Student Data: Staff shall obtain school authorization before using applications, websites, or artificial-intelligence services that receive private student data. Disclosures require a lawful basis under FERPA and Minnesota law. When relying on FERPA's school-official exception, the provider must perform an institutional function, be under school control concerning record use and maintenance, and satisfy the school's annual-notice criteria; access shall be limited to legitimate educational interests and authorized uses and redisclosures. Signing this policy's Internet Use Agreement is not blanket consent to release education records.

For covered online-service operators collecting personal information from children under 13, the school shall verify compliance with COPPA and 16 C.F.R. part 312. School authorization may substitute for parental consent only within FTC guidance for school-benefit educational uses without other commercial purposes; the operator must provide the required notice and remains responsible for COPPA compliance. The school shall support applicable parent access and deletion requests. Uses outside school authorization require the operator's applicable parental notice and consent process.

Vendor review shall address the amended COPPA rule's applicable requirements, including biometric identifiers, written information-security safeguards, purpose-limited retention and deletion, and separate verifiable parental consent for third-party disclosures unless integral to the service. Minnesota's educational-data restrictions apply independently.

Accessible Technology: The school shall provide effective communication, reasonable modifications, and required assistive technology under ADA Title II, Section 504, and IDEA. School web content and mobile applications, including covered vendor content, shall meet applicable ADA Title II accessibility requirements, including WCAG 2.1 Level AA by the applicable compliance date, subject to lawful exceptions. Existing disability-access duties continue before that date.

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

Limited Expectation of Privacy

By authorizing use of the school district system, the school district does not relinquish control over materials on the system or contained in files on the system. Users

should expect only limited privacy in the contents of personal files on the school district system.

All maintenance, monitoring, searches, and disclosures under this policy are subject to the School-Issued Devices section, Minnesota data-practices law, FERPA, and applicable constitutional protections. An acknowledgment, ownership of equipment, or generalized lack-of-privacy statement does not waive those protections.

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.

A student search by school officials must be justified at its inception by reasonable grounds to expect evidence of a law or policy violation and reasonably related in scope to its purpose; it shall not be excessively intrusive in light of the student's age, sex, and the nature of the suspected violation. Confiscation alone does not authorize searching device contents. School-issued-device monitoring must also satisfy the specific limits below. Law-enforcement searches require their own lawful authority.

Parents may have the right at any time to investigate or review the contents of their child's files and e-mail files in accordance with the school district's Protection and Privacy of Pupil Records Policy. Parents have the right to request the termination of their child's individual account at any time.

School district employees should be aware that the school district may investigate or review school-system files and e-mail consistent with authorized purposes, applicable law, and constitutional protections. 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 Minnesota Statutes chapter 13 (Minnesota Government Data Practices Act).

The school district will cooperate with local, state, and federal authorities through lawful disclosures consistent with FERPA, Minnesota data-practices law, and applicable legal process 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.

Internet Use Agreement

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.

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.

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

Limitation on School Direct 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 diskettes, tapes, hard drives, or servers, or for delays or changes in or interruptions of service or misdeliveries or nondeliveries of information or materials, subject to applicable law. Nothing in this policy waives legal rights or eliminates the school's statutory or constitutional duties or liabilities. 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.

User Notification

All users shall be notified of the school district policies relating to Internet use.

This notification shall include the following:

Notification that Internet use is subject to compliance with school district policies.

Disclaimers limiting the school district's liability relative to:

Information stored on school district diskettes, hard drives, or servers.

Information retrieved through school district computers, networks, or online resources.

Personal property used to access school district computers, networks, or online resources.

Unauthorized financial obligations resulting from use of school district resources/accounts to access the Internet.

A description of the privacy rights and limitations of school sponsored/managed Internet accounts.

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.

Notification that goods and services can be purchased over the Internet that could potentially result in unwanted financial obligations and that responsibility for any

financial obligation is determined by applicable law and the circumstances, rather than automatically imposed on a student or parent by this policy.

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

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.

Notification that all provisions of the acceptable use policy are subordinate to local, state, and federal laws.

Parent's Responsibility; Notification of Student Internet Use

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.

Home use does not relieve the school or its providers of school-issued-device monitoring limits, data-protection obligations, or required disability supports.

Parents will be 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 alternative activities not requiring Internet access. This notification should include:

A copy of the user notification form provided to the student user.

A description of parent/guardian responsibilities.

A notification that the parents have the option to request alternative educational activities not requiring Internet access and the material to exercise this option.

A statement that the Internet Use Agreement must be signed by the user, the parent or guardian, and the supervising teacher prior to use by the student.

A statement that the school district's acceptable use policy is available for parental review.

Notification Regarding Technology Providers

"Technology provider" means a person who:

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

creates, receives, or maintains educational data pursuant or incidental to a contract with the school district

"Parent" means a parent of a student and includes a natural parent, a guardian, or an individual acting as a parent in the absence of a parent or a guardian.

Within 30 days of the start of each school year, the school district must give parents 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:

identify each curriculum, testing, or assessment technology provider with access to educational data;

identify the educational data affected by the curriculum, testing, or assessment technology provider contract; and

include information about the contract inspection and provide contact information for a school department to which a parent 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.

The school district must provide parents and students an opportunity to inspect a complete copy of any contract with a technology provider.

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:

the technology provider's employees or contractors have access to educational data only if authorized; and

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.

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 are not the technology provider's property.

Technology providers shall provide the school all breach information needed for legally required notice; return or destroy educational data within 90 days after contract expiration unless renewal is reasonably anticipated; and refrain from selling, sharing, disseminating, or commercially using the data except as Minnesota Statutes, section 13.32, subdivision 13, permits. A permitted contract assignment or delegation must bind the successor to the same restrictions. Authorized de-identified aggregate service-improvement uses remain subject to that subdivision. Contracts shall reflect applicable data-practices, security, and FERPA requirements.

School-Issued Devices

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

Except under one of the six expressly permitted circumstances listed below, the school district or a technology provider must not electronically access or monitor:

any location-tracking feature of a school-issued device;

any audio or visual receiving, transmitting, or recording feature of a school- issued device; or

student interactions with a school-issued device, including but not limited to keystrokes and web-browsing activity.

The school district or a technology provider may only engage in ~~activities~~ the electronic access or monitoring otherwise prohibited in this section only if:

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;

the activity is permitted under a judicial warrant;

the school district is notified or becomes aware that the device is missing or stolen;

the activity is necessary to respond to an imminent threat to life or safety and the access is limited to that purpose;

the activity is necessary to comply with federal or state law, including but not limited to Minnesota Statutes section 121A.031; or

the activity is necessary to participate in federal or state funding programs, including but not limited to the E-Rate program.

If the school district or a technology provider interacts with a school-issued device to respond to an imminent threat to life or safety under the fourth exception above, it must, within 72 hours of the access, notify the student to whom the school-issued device was issued or that student's parent and provide a written description of the interaction, including which features of the device were accessed and a description of the threat. This notice is not required at any time when the notice itself would pose an imminent threat to life or safety, but must instead be given within 72 hours after that imminent threat has ceased.

Cell Phone Use

Cell phone and personal electronic communication device possession, use, exceptions, searches, confiscation, and return procedures are governed by the school's standalone Policy 524.5. Use of school technology remains subject to this policy, including applicable privacy, data-protection, accessibility, and school-issued-device safeguards.

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 school has an individualized family service plan, an individualized education program, or a 504 plan in effect.

Implementation; Policy Review

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.

The administration shall revise the user notifications, including student and parent notifications, if necessary, to reflect the adoption of these guidelines and procedures.

The school district Internet policies and procedures are available for review by all parents, guardians, staff, and members of the community.

Because of the rapid changes in the development of the Internet, the school board shall conduct an annual review of this policy.

For CIPA-covered support, the school shall provide reasonable public notice and hold at least one public hearing or meeting to address the proposed Internet safety policy as required by 47 C.F.R. 54.520. Annual review does not create an annual federal hearing requirement.

Legal References:

Minn. Stat. §§ 13.05, subd. 11; 13.055; 13.32, subds. 13–14 (Contracts, Breaches, Educational Data, School-Issued Devices)

Minn. Stat. § 121A.73 (School Cell Phone Policy); §§ 121A.41–121A.56 (Pupil Fair Dismissal Act)

16 C.F.R. part 312 (COPPA Rule, as amended); 34 C.F.R. part 99 (FERPA)

29 U.S.C. § 794; 34 C.F.R. part 104 (Section 504); 20 U.S.C. §§ 1400–1482; 34 C.F.R. part 300 (IDEA)

42 U.S.C. §§ 12131–12134; 28 C.F.R. part 35, including subpart H (ADA Title II)

U.S. Const. amends. I, IV; New Jersey v. T.L.O., 469 U.S. 325 (1985); Riley v. California, 573 U.S. 373 (2014)

Minn. Stat. Ch. 13 (Minnesota Government Data Practices Act)

Minn. Stat. § 13.32 (Educational Data)

Minn. Stat. § 121A.031 (School Student Bullying Policy)

Minn. Stat. § 124D.166 (Limit on Screen Time for Children in Preschool and Kindergarten)

Minn. Stat. § 125B.15 (Internet Access for Students)

Minn. Stat. § 125B.26 (Telecommunications/Internet Access Equity 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)

Mahanoy Area Sch. Dist. v. B.L., 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 (8th 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:

Policy 524.5 (Standalone Cell Phone Policy)

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 (Title IX Sex Nondiscrimination Grievance Procedures and Process)

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)

Review notes and legal sources

This draft distinguishes corrections to legal requirements from school implementation safeguards in the comments. The provided monitoring exceptions, 72-hour imminent-threat notice, parent technology-provider notices, and preschool/kindergarten screen-time language are substantially retained. Cell-phone operational provisions are struck and redirected to Policy 524.5; that standalone policy was not supplied for review.

Before adoption, confirm actual school administrator titles, discipline and record-policy numbers, approved applications, vendor contracts and notices, device-monitoring configurations, and CIPA funding/certification status. The references to MSBA/MASA model policies must be matched to the school's adopted policies. Review Policy 524.5 separately for disability/medical exceptions and lawful search, confiscation, and return procedures. The Internet Use Agreement and notification forms were not supplied and must be aligned with this draft.

Accessibility date: DOJ's April 2026 interim final rule extended the web/mobile rule compliance dates to April 26, 2027 for entities with populations of 50,000 or more, and April 26, 2028 for smaller entities and special district governments. Confirm the charter school's applicable public-entity classification; student enrollment alone does not determine the deadline. Existing ADA/Section 504 duties continue. COPPA's 2025 amendments reached their general operator compliance date on April 22, 2026.

Minnesota educational data and device privacy
https://www.revisor.mn.gov/statutes/cite/13.32

Minnesota government contractor data duties
https://www.revisor.mn.gov/statutes/cite/13.05

Minnesota breach notification
https://www.revisor.mn.gov/statutes/cite/13.055

Minnesota student Internet filtering
https://www.revisor.mn.gov/statutes/cite/125B.15

Minnesota cell-phone policy requirement
https://www.revisor.mn.gov/statutes/cite/121A.73

Preschool and kindergarten screen-time limits
https://www.revisor.mn.gov/statutes/cite/124D.166

CIPA implementation and public process
https://www.ecfr.gov/current/title-47/chapter-I/subchapter-B/part-54/subpart-F/section-54.520

CIPA statutory definitions
https://www.govinfo.gov/content/pkg/USCODE-2024-title47/html/USCODE-2024-title47-chap5-subchapII-partII-sec254.htm

COPPA final rule and compliance date
https://www.govinfo.gov/content/pkg/FR-2025-04-22/html/2025-05904.htm

FTC COPPA school authorization guidance
https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions

FERPA regulations
https://www.ecfr.gov/current/title-34/subtitle-A/part-99

ADA web-rule implementation and extended dates
https://www.ada.gov/resources/web-rule-first-steps/

Off-campus expression: Mahanoy
https://www.supremecourt.gov/opinions/20pdf/20-255_g3bi.pdf

Student search: T.L.O.
https://www.govinfo.gov/content/pkg/USREPORTS-469/pdf/USREPORTS-469-325.pdf

Law enforcement phone search: Riley
https://www.govinfo.gov/content/pkg/USREPORTS-573/pdf/USREPORTS-573-373.pdf

Copyright fair use
https://www.copyright.gov/fair-use/