524 INTERNET, AND TECHNOLOGY ACCEPTABLE USE AND SAFETY POLICY

[Note: Education districts are required by statute to have a policy addressing these issues.]

I. PURPOSE

The purpose of this policy is to set forth policies and guidelines for access to the education district computer system and acceptable and safe use of the Internet.

II. GENERAL STATEMENT OF POLICY

In making decisions regarding student and employee access to the education district computer system and the Internet, the education 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 education 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 education district expects that faculty will blend thoughtful use of the education district computer system and the Internet throughout the curriculum and will provide guidance and instruction to students in their use.

It is the Freshwater Education District Policy to monitor the online activities of minors. The Freshwater Education District will also provide educational information to students regarding appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response behaviors.

BOYD (bring your own device) implications of this policy, for both students and staff, are understood to be the very same as Freshwater owned electrical devices. Freshwater is not liable for the loss, damage, misuse, or theft of personally owned items brought into Freshwater facilities or events and activities. Likewise, students and staff are not required to bring in outside technology into the school. Freshwater requires all technology to be used for educational purposes only.

Personal devices used at school will not be afforded Freshwater technology support, charging access, or storage.

Students will be permitted guest access to the Freshwater network only, not private networks such as Hot Spot, 3G, 4G, or other content providers.

Students are not permitted to use any electronic device to record audio or video media or take pictures of any student or staff member without their permission. The distribution of any unauthorized media may result in discipline, including but not limited to, suspension, criminal charges, and expulsion. This policy prohibits the use of technology devices in locker rooms, restrooms, and nurses offices.

Students may not utilize any technology to harass, threaten, demean, humiliate, intimidate, embarrass, or annoy classmates or staff.

Freshwater reserves the right to monitor, inspect, copy, and review a personally owned device or file when staff has a reasonable suspicion that a violation has occurred.

III. LIMITED EDUCATIONAL PURPOSE

The school district is providing students and employees with access to the education 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 education 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 education 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 education 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 education 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 education 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 education district system and Internet resources or accounts are considered unacceptable:

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

a. pornographic, obscene, or sexually explicit material or other visual depictions that are harmful to minors;

b. obscene, abusive, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, or sexually explicit language;

c. materials that use language or images that are inappropriate in the education setting or disruptive to the educational process;

d. information or materials that could cause damage or danger of disruption to the educational process;

e. materials that use language or images that advocate violence or discrimination toward other people (hate literature) or that may constitute harassment or discrimination.

2. Users will not use the education 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 education district system to engage in any illegal act or violate any local, state, or federal statute or law.

4. Users will not use the education 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 education district system software, hardware, or wiring or take any action to violate the education district's security system, and will not use the education district system in such a way as to disrupt the use of the system by other users.

5. Users will not use the education 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.

6. Users will not use the education 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. ***[Note: Education districts should consider the impact of this paragraph on present practices and procedures, including, but not limited to, practices pertaining to employee communications, school or classroom websites, and student/employee use of social networking***

websites. Depending upon education district policies and practices, education districts may wish to add one or more of the following clarifying paragraphs.]

a. This paragraph does not prohibit the posting of employee contact information on education 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. 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 education district as directory information and verification is made that the education 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 education 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.

c. These prohibitions specifically prohibit a user from utilizing the education 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.

7. Users must keep all account information and passwords on file with the designated education district official. Users will not attempt to gain unauthorized access to the education district system or any other system through the education 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 education district system may not be encrypted without the permission of appropriate school authorities.

8. Users will not use the education 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 education districts computer, and will not plagiarize works they find on the Internet.

9. Users will not use the education district system for conducting business, for unauthorized commercial purposes, or for financial gain unrelated to the mission of the education district. Users will not use the education district system to offer or provide goods or services or for product advertisement. Users will not use the education district system to purchase goods or services for personal use without authorization from the appropriate education district official.

10. 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.

B. The education 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 education district premises also may be in violation of this policy as well as other education 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 devise. If the education district receives a report of an unacceptable use originating from a non-school computer or resource, the education 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 education district computer system and the Internet and discipline under other appropriate education 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 immediately disclose the inadvertent access to an appropriate education district official. In the case of an education 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 an education district employee, the building administrator.

VI. FILTER

[Note: Pursuant to state law, education districts are required to restrict access to inappropriate materials on school computers with Internet access. Education districts seeking technology revenue pursuant to Minnesota Statutes section 125B.26 or certain federal funding, such as e-rate discounts, for purposes of Internet access and connection services and/or receive funds to purchase Internet accessible computers are subject to the federal Children's Internet Protection Act, effective in 2001. Those districts are required to comply with additional standards in restricting possible access to inappropriate materials. Therefore, education districts should select one of the following alternative sections depending upon whether the education district is seeking such funding and the type of funding sought.]

ALTERNATIVE NO. 1

[Note: For an education district that does not seek either state or federal funding in connection with its computer system, the following language should be adopted. It reflects a mandatory requirement under Minnesota. Statute section 125B.15.]

All computers equipped with Internet access and available for student use at each school site will be equipped to restrict, by use of available software filtering technology or other effective methods, all student access to materials that are reasonably believed to be obscene, child pornography or harmful to minors under state or federal law. Software filtering technology shall be narrowly tailored and shall not discriminate based on viewpoint.

[Note: The purchase of filtering technology is not required by state law if the school site would incur more than incidental expense in making the purchase. In the absence of filtering technology, school sites still are required to use "other effective methods" to restrict student access to such materials.]

ALTERNATIVE NO. 2

[Note: Technology revenue is available to education districts that meet the additional condition of also restricting adult access to inappropriate materials. Education districts that seek such state technology revenue may adopt or retain the following language. However, the education district is not required to do so.]

A. All education district computers with Internet access and available for student use will be equipped to restrict, by use of available software filtering technology or other effective methods, all student access to materials that are reasonably believed to be obscene, child pornography or harmful to minors under state or

federal law.

B. All education district computers with Internet access, not just those accessible and available to students, will be equipped to restrict, by use of available software filtering technology or other effective methods, adult access to materials that are reasonably believed to be obscene or child pornography under state or federal law.

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

ALTERNATIVE NO. 3

[Note: Education districts that receive certain federal funding, such as e-rate discounts, for purposes of Internet access and connection services and/or receive funds to purchase Internet accessible computers are subject to the federal Children's Internet Protection Act, effective in 2001. This law requires education districts to adopt an Internet safety policy that contains the provisions set forth below. Also, the Act requires such education districts to provide reasonable notice and hold at least one public hearing or meeting to address the proposed Internet safety policy prior to its implementation. Education districts that do not seek such federal financial assistance need not adopt the alternative language set forth below nor meet the requirements with respect to a public meeting to review the policy. The following alternative language for education districts that seek such federal financial assistance satisfies both state and federal law requirements.]

A. With respect to any of its computers with Internet access, the education district will monitor the online activities of both minors and adults and employ technology protection measures during any use of such computers by minors and adults. The technology protection measures utilized will block or filter Internet access to any visual depictions that are:

1. Obscene;

2. Child pornography; or

3. Harmful to minors.

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

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

2. Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and

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

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

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

E. The education 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.

[Note: Although education districts are not required to adopt the more restrictive provisions contained in either Alternative No. 2 or No. 3 if they do not seek state or federal funding, they may choose to adopt the more restrictive provisions as a matter of school policy.]

VII. CONSISTENCY WITH OTHER SCHOOL POLICIES

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

VIII. LIMITED EXPECTATION OF PRIVACY

A. By authorizing use of the education district system, the education 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 education district system.

B. Routine maintenance and monitoring of the education district system may lead to a discovery that a user has violated this policy, another education 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 education district policy.

D. 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.

E. Education district employees should be aware that the education district retains the right at any time to investigate or review the contents of their files and e-mail files. In addition, education district employees should be aware that data and other materials in files maintained on the education district system may be subject

to review, disclosure or discovery under Minnesota Statutes Chapter 13 (Minnesota Government Data Practices Act).

F. The education 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 education district policies conducted through the education 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, and employees of the education district.

B. This policy requires the permission of and supervision by the school's designated professional staff before a student may use a school account or resource to access the Internet.

C. The Internet Use Agreement form for students must be read and signed by the user, the parent or guardian, and the supervising teacher. The 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.

X. LIMITATION ON EDUCATION DISTRICT LIABILITY

Use of the education district system is at the user's own risk. The system is provided on an "as is, as available" basis. The education district will not be responsible for any damage users may suffer, including, but not limited to, loss, damage, or unavailability of data stored on education 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 education district is not responsible for the accuracy or quality of any advice or information obtained through or stored on the education district system. The education district will not be responsible for financial obligations arising through unauthorized use of the education district system or the Internet.

XI. USER NOTIFICATION

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

B. This notification shall include the following:

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

2. Disclaimers limiting the education district's liability relative to:

a. Information stored on education district diskettes, hard drives, or servers.

b. Information retrieved through education district computers, networks, or online resources.

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

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

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

4. Notification that, even though the education district may use technical means to limit student Internet access, these limits do not provide a foolproof means for enforcing the provisions of this acceptable use policy.

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

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

7. Notification that, should the user violate the education 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' RESPONSIBILITY; NOTIFICATION OF STUDENT INTERNET USE

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

B. Parents will be notified that their students will be using education district resources/accounts to access the Internet and that the education district will provide parents 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 notification that the parents have the option to request alternative educational activities not requiring Internet access and the material to exercise this option.

4. 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.

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

XIII. NOTIFICATION REGARDING TECHNOLOGY PROVIDERS

A. "Technology provider" means a person who:

1. contracts with the education district, as part of a one-to-one program or otherwise, to provide a school-issues device for student use; and

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

B. "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.

C. Within 30 days of the start of the 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:

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 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.

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

E. 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.

F. 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.

XIV. SCHOOL-ISSUED DEVICES

A. "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.

B. Except as provided in paragraph C, the education 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.

C. If the education district or a technology provider interacts with a school-issued device as provided in paragraph C, 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 and provide a written description of the interaction, including which features of the device were accessed and a description of the threat. This notice in 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.

XV. LIMIT ON SCREEN TIME FOR CHILDREN IN PRESCHOOL AND KINDERGARTEN

A child is 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 individualized family service plan, in individualized education program, or a 504 plan in effect.

XVI. IMPLEMENTATION; POLICY REVIEW

A. The education district administration may develop appropriate user notification forms, guidelines, and procedures necessary to implement this policy for submission to the school board for approval. Upon approval by the school board, such guidelines, forms, and procedures shall be an addendum to this policy.

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

C. The education 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 conduct an annual review of this policy.

Legal References:
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)
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)
Mahanoy Area Sch. Dist. 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. 1942003)
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: 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)