# 524 INTERNET USE AND SAFETY

## I. PURPOSE

Electronic information research skills are now fundamental to preparation of citizens and future employees. Access to the school computer system and to the Internet enables students and employees to explore thousands of libraries, databases, bulletin boards, and other resources while exchanging ideas with people around the world. The purpose of this policy is to set forth guidelines for access to the Southside Family Charter School (SFCS) computer system and wireless network, including use of personal electronic devices while at school, and ensure the safe and appropriate use of the Internet by all users.

## II. GENERAL STATEMENT OF POLICY

A. In making decisions regarding student and employee access to the school computer system and the Internet, including electronic communications, the school considers its own stated educational mission, goals, and objectives. Use of the school computer system and use of the internet shall be consistent with school policies and the school mission.

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

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

## III. USER GUIDELINES

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

1. obscene, abusive, defamatory, threatening, disrespectful, violent, or sexually explicit language or material;

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

3. violence or discrimination toward other people (hate literature) or that may constitute harassment or discrimination.

B. Users will not use the school system to engage in any illegal act in violation of any local, state, or federal statute or law.

C. Users will not vandalize, damage, or disable the property or systems of SFCS or another person or organization. Users will not make deliberate attempts to degrade or disrupt equipment, software, or system performance by spreading computer viruses or by any other means. Users will not tamper with, modify, or change the school system software, hardware, or wiring or take any action to violate the school's security system, and will not use the school system in such a way as to disrupt the use of the system by other users.

D. Generally, users will not use anyone else's password, open or use anyone else's files, or log in through another person's account, without the direct permission of that person. Limited exceptions to this apply, including staff users accessing student accounts for educational purposes and School Administrator accessing student or staff accounts for school purposes.

E. Users will not use the school 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.

1. This paragraph does not prohibit the posting of employee contact information on the school webpage 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).

2. Staff users must maintain private, confidential, or proprietary information as required by the Minnesota Data Practices Act and school policies.

F. Users will not attempt to gain unauthorized access to the school system or any other system through the school 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 system may not be encrypted without the permission of appropriate school authorities.

G. Users will not violate copyright laws or usage licensing agreements, or otherwise 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, including work generated through artificial intelligence (AI).

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

I. A student or employee engaging in the foregoing unacceptable uses of the Internet when off school premises also may be in violation of this policy as well as other school policies, including the Bullying and Hazing Prohibition policy (SFCS Policy 514). Examples of such violations include, but are not limited to, situations where the school system is compromised or if a school employee or student is negatively impacted, or if student learning or the school environment is substantially and materially disrupted. If the school receives a report of an unacceptable use originating from a non-school computer or resource, the school 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 computer system and the Internet, and discipline under other appropriate school policies, including suspension, expulsion, exclusion, or termination of employment.

J. If a user inadvertently accesses unacceptable materials or an unacceptable Internet site, the user shall immediately disclose the inadvertent access to an appropriate person. Student users should turn off the computer monitor and immediately inform a teacher. In the case of a school employee, the immediate disclosure shall be to the School. This disclosure may serve as a defense against an allegation that the user has intentionally violated this policy. In certain instances, a user also may access otherwise unacceptable materials if necessary to complete an assignment and, in the case of a student, if done with the prior approval of and with guidance from the appropriate teacher.

IV. FILTER

A. With respect to any of its computers with Internet access, the school employs software filtering technology which restricts Internet access to any visual depictions that are reasonably believed to be obscene or child pornography or material harmful to minors under federal or state law.

B. Software filtering technology shall be narrowly tailored and shall not discriminate based on viewpoints protected under Policy 413.

C. The School Administrator or other person authorized by the School may disable the technology protection measure, during use by an adult, to enable access for bona fide research or other lawful purposes.

V. LIMITED EXPECTATION OF PRIVACY

A. By authorizing use of the school system, the school 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 system.

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

C. An individual investigation or search will be conducted if school authorities have a reasonable suspicion that the search will uncover a violation of law or school policy.

D. Parents have the right at any time to investigate or review the contents of their child's files and email files. Parents have the right to request the termination of their child's individual account at any time.

E. School employees should be aware that the school retains the right at any time to investigate or review the contents of their files and email files. In addition, school employees should be aware that data and other materials in files maintained on the school system may be subject to review, disclosure or discovery under Minn. Stat. Ch. 13 (the Minnesota Government Data Practices Act).

F. The school will cooperate fully with local, state and federal authorities in any investigation concerning or related to any illegal activities or activities not in compliance with school policies conducted through the school system.

## VI. 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 school.

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 will be reviewed by each classroom teacher with their students at the beginning of the school year. All students and classroom teachers will sign the agreement, and it will be kept on file at the school.

D. A separate Internet Use Agreement will be sent to parents before the beginning of the school year, to be signed and returned with the beginning of school year forms. This form shall include an option for parents to indicate a preference that their child not use the Internet, in which case alternative arrangements must be made by the school.

E. The Internet Use Agreement form for employees must be signed by the employee upon hiring. The form must then be filed at the school.

## VII. LIMITATION ON SCHOOL LIABILITY

Use of the school system is at the user's own risk. The system is provided on an "as is, as available" basis. The school will not be responsible for any damage users may suffer, including, but not limited to, loss, damage, or unavailability of data stored on school diskettes, tapes, hard drives, or servers, or for delays or changes in or interruptions of service or misdeliveries or nondeliveries of information or materials, regardless of the cause. The school is not responsible for the accuracy or quality of any advice or information obtained through or stored on the school system. The school will not be responsible for financial obligations arising through unauthorized use of the school system or the Internet.

VIII. RESPONSIBILITY

A. The school expects that faculty will blend thoughtful use of the school computer system and the Internet throughout the curriculum and will provide guidance and instruction to students in their use.

B. School staff and parents have the shared responsibility to work together to help students develop the critical thinking skills needed to identify information appropriate to their age and development levels, and access the Internet safely and responsibly.

C. Students are responsible for following all internet use guidelines referenced in this policy and in the Internet Use Agreement Form.

D. Parents are responsible for supervision of student use of school-provided and personally-owned electronic devices used at home or through other remote locations.

E. This policy shall be posted on the school website, and available upon request from the school office.

F. . Because of the rapid changes in the development of the Internet, the board shall conduct an annual review of this policy and agreement forms.

**XIII. NOTIFICATION REGARDING TECHNOLOGY PROVIDERS**

A. "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.

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 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 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.

C. The school district or a technology provider may only engage in activities prohibited by paragraph B 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.031; or

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

D. If the school 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 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.

## XV. 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.

Legal References: 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. 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)
*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, 89 S.Ct. 733, 21 L.Ed.2d 731 (1969)
United States v. Amer. Library Assoc., 539 U.S. 194, 123 S.Ct. 2297, 56 L.Ed.2d 221 (2003)
*Sagehorn v. Indep. Sch. Dist. No. 728*, 122 F.Supp.2d 842 (D. Minn. 2015)
R.S. v. Minnewaska Area Sch. Dist. No. 2149, No. 12-588, 2012 WL 3870868 (D. Minn. 2012)
Tatro v. Univ. of Minnesota, 800 N.W.2d 811 (Minn. App. 2011), aff'd on other grounds 816 N.W.2d 509 (Minn. 2012)
S.J.W. v. Lee's Summit R-7 Sch. Dist., 696 F.3d 771 (8th Cir. 2012)
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: Southside Family Charter School Policy 403 (Discipline, Suspension, and Dismissal of School Employees)
Southside Family Charter School Policy 406 (Public and Private Personnel Data)
Southside Family Charter School Policy 413 (Harassment and Violence Prohibition: Protected Classes)
Southside Family Charter School Policy 506 (Student Behavior Intervention)
Southside Family Charter School Policy 514 (Bullying and Hazing Prohibition Policy)
Southside Family Charter School Policy 515 (Protection and Privacy of Pupil Records)
Southside Family Charter School Policy 521 (Student Disability Nondiscrimination)
Southside Family Charter School Policy 522 (Student Sex Nondiscrimination)
Southside Family Charter School Policy 525 (Social Media Use)