

Adopted: 3/16/1999 Saint Paul Public Schools Policy 520.00
Revised: 6/17/2008; 6/19/2012; 10/21/2023
Reviewed: 2/21/2023

520.00 TECHNOLOGY USAGE AND SAFETY

I. POLICY PURPOSE

The Technology Usage & Safety Policy (Policy 520.00) establishes proper use guidelines for the district's technology resources. Its core purpose is to ensure the effective and safe utilization of these resources by students, parents/guardians, and employees. This shared responsibility is crucial for maximizing the educational value and maintaining the integrity of the technology infrastructure.

II. GENERAL STATEMENT OF POLICY

The Technology Usage & Safety Policy (Policy 520.00) outlines the proper use of the district's technology resources, and encompasses a wide array of items, including network infrastructure, internet services, communication systems (e.g., phones, email), information systems (e.g., websites, learning management systems, data repositories), and various hardware and software devices. Access to these resources is considered a privilege, not a right, and any misuse can lead to consequences ranging from suspension of access to legal liability

Users of district technology resources have specific responsibilities, including:

- Complying with all relevant policies.
- Respecting the privacy of other users and maintaining security.
- Recognizing and honoring intellectual property rights.
- Avoiding prohibited activities such as unauthorized access, interfering with network services, distributing harmful content, engaging in illegal acts, violating copyrights, and sharing private information.

There is a limited expectation of privacy for files and activities on district technology resources, as they are subject to monitoring for compliance. The Technology Services department enforces technology protection measures—such as content filtering, multi-factor authentication (MFA), and strong password practices—to uphold the safety and security of users and systems. Parents/guardians have the right to review their child's files and request termination of their child's account access. The district commits to educating students annually on appropriate online behavior, including cyberbullying awareness and response.

III. DEFINITIONS

1. District Technology Resources

These include but are not limited to the following items that are provided or paid for in whole or in part by the District:

- a. **Infrastructure:** Networks including fiber, cables, and other hardware; Internet services and access; content filters
- b. **Cybersecurity:** Software tools to monitor and enforce student and staff data protection, access control, incident response, and legal compliance, maintaining the confidentiality, integrity, and availability of information within the district.
- c. **Communication systems and devices:** Telephones, cellular phones, Voice over Internet Protocol (VoIP) phones; voicemail facilities; TelePresence; electronic mail (e-mail); cloud fax services
- d. **Information systems and services:** Applications and databases that are internally or externally hosted and accessed via an internal or external connection, including websites, information systems, electronic resources, learning management systems, and communication and collaboration systems
- e. **Hardware, software, and devices:** Desktop and laptop computers; mobile and tablet devices; servers; portable hard drives and storage devices; printers and scanners; mice, keyboards, cameras, and other peripheral devices; software including operating systems, applications, and mobile applications (apps) software
- f. **Data:** Information including text, data files, email, images, video, and audio files that are stored, accessed, or transmitted using district technology
- g. **Other:** New technologies as they become available

2. Harmful to Minors

Any material or picture, image, graphic image file, or other visual depiction that:

- a. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion
- b. 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
- c. Taken as a whole, lacks serious literary, artistic, political, or scientific value to minors

3. User

All employees, contractors, Board members, students, volunteers, parents/guardians, and other individuals when they are using district technology resources.

IV. ACCESS, USE AND SAFETY

1. Access

The District offers users access to a variety of district technology resources

2. Use as a Privilege

The use of the district technology resources is a privilege, not a right. Unacceptable uses of district technology resources may result in one or more of the following consequences: suspension or cancellation of authorized use or access privileges; discipline under applicable district policies and procedures; or civil or criminal liability under applicable laws.

3. Safety Education

The District will educate students about appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms, and cyberbullying awareness and response.

V. USER RESPONSIBILITY

1. Appropriate Use

Individual users of district technology resources have the responsibility to:

- a. Comply with all policies as they may be interpreted to apply to technology resources
- b. Find, evaluate, and effectively use information and resources
- c. Respect the privacy of other users
- d. Maintain the security of the district technology resources
- e. Recognize and honor the intellectual property rights of others
- f. Disclose inadvertent access of unacceptable materials or an unacceptable Internet site to an appropriate district administrator

2. Acceptable Use of technology resources includes the following:

- a. Support instructional, administrative, and business uses consistent with the mission of the district
- b. Encourage efficient, cooperative, and creative methods to perform the user's job duties or educational tasks
- c. Exercise authorized and appropriate access to voice, audio, video, and data systems, software or data, both locally and at and from other sites, and
- d. Administer, support, or maintain district technology resources as appropriate.

3. Unacceptable Use

- a. Providing, assisting or gaining unauthorized or inappropriate access to the district's technology resources, including any type of voice, video, or data network or system
- b. Interfering with the ability of others to effectively use the district's technology resources or network services
- c. Gaining unauthorized access to or compromising another user's account, file, work, or data
- d. Distributing any material to intentionally cause congestion of the voice, audio, video, and data networks
- e. Accessing, reviewing, uploading, downloading, storing, printing, posting, receiving, transmitting, or distributing:
 - i. Pornographic, obscene, or sexually explicit material or other material or visual depictions that are harmful to minors
 - ii. Abusive or threatening materials, including hate mail, or harassing or discriminatory materials that violate school district policies
- f. Publishing materials or otherwise distributing content without the author's permission
- g. Using technology resources for a commercial, political, or profit making purpose, except as specifically approved or agreed to by the district
- h. Using technology resources to engage in any illegal act or violate any local, state, or federal statute or law 3 of 30 254
- i. Violating copyright laws or usage licensing agreements, or otherwise using another person's intellectual property without the person's prior approval or proper citation
- j. Disclosing, using, posting or otherwise disseminating private information about another person, or posting personal contact information about oneself or others
- k. Using someone else's digital signature without authorization

- l. Monitoring another user's information, attempting security breaches, or disrupting communication
- m. Utilizing unauthorized systems and applications not reviewed, approved or in compliance with district technology and security standards.

4. Guidelines for Acceptable Use

The publications Guidelines for Acceptable Use by Employees, Contractors, and Board Members, Guidelines for Acceptable Use by Students and The Rights and Responsibilities Handbook contain additional information further describing acceptable use of district technology resources.

VI. LIMITED EXPECTATION OF PRIVACY

1. Limited Privacy:

By authorizing use of district technology resources, the District does not relinquish control over materials on the system or contained in files on the system. Users should expect only limited privacy for the contents of personal files stored on, or activity conducted through, district technology resources.

2. Data Privacy:

Data and other materials in files maintained on district technology resources may be subject to review, disclosure, or discovery under various laws.

3. Investigative Uses:

The District will cooperate fully with local, state, and federal authorities in any investigation concerning or related to any activities not in compliance with law or school district policies and conducted using district technology resources

4. Violations:

Routine maintenance and monitoring of the district technology resources may find that a user has violated this policy, another school district policy, or the law. A search of the individual's system content and use will be conducted if school authorities have a reasonable suspicion that the search will uncover a violation of law or school district policy.

5. Parent/Guardian Rights:

Parents or guardians have the right at any time to review the contents of their student's files, including email files, stored on district

technology resources. Parents or guardians have the right to request the termination of their student's individual account at any time.

6. School District's Rights:

The District reserves all rights to control its technology resources, and may:

- a. Monitor or restrict a user's access to district technology resources
- b. Search any computer or electronic data storage devices that are assigned to a user or used on any district computer or network
- c. Retrieve, alter, post, remove or delete any data created, received, transmitted, stored, or maintained by any user on or through district technology resources to the extent consistent with law and District policy.
- d. Remove, replace or disable SPPS hardware or software designated as obsolete, out of compliance or dangerous.

VII. LIMITATIONS ON SCHOOL DISTRICT LIABILITY

1. Use of district technology resources is at the user's risk. The system is provided on an "as is, as available" basis. Regardless of the cause, the District will not be responsible for any damage users may suffer, including but not limited to the following:
 - a. Loss, damage, or unavailability of data stored on or transmitted through district technology resources
 - b. Delays, changes, or interruptions of service
 - c. Missed or non-delivery of information or materials
2. The school district shall not be responsible for unauthorized financial obligations or consequential damages arising from the use of district technology resources.

VIII. PROTECTION MEASURES

1. Monitoring of on-line activities

With respect to any computers or devices with Internet access, the district will monitor the online activities of both minors and adults and employ technology protection measures during any use of such devices by minors and adults.

2. Filtering content

The district's technology protection measures shall be designed to address the safety and security of minors when using direct electronic communications and to block or filter Internet access to inappropriate materials including, but not limited to, any visual depictions that:

- a. Are obscene

- b. Contain child pornography, or
- c. Are harmful to minors

3. Authorized exceptions:

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

IX. TECHNOLOGY USE AGREEMENT

As a condition of access to the district technology resources, users must agree to, accept, and abide by the Technology Usage and Safety Policy and the Guidelines for Acceptable Use, as they may be amended from time to time.

LEGAL REFERENCES:

47 U.S.C. §254 - *Children's Internet Protection Act of 2000 (CIPA)*

47 C.F.R. § 54.520 - *FCC rules implementing CIPA*

20 U.S.C. §6751 et seq. - *Enhancing Education Through Technology Act of 2001*

20 U.S.C. 1232g - *FERPA*

Minn. Stat. § 125B.15 - *Internet Access for Students*

Minn. Stat. §125B.26 - *Telecommunications/Internet Access Equity Act*

Minn. Stat. Chapter 13 - *Minnesota Government Data Practices Act*

CROSS REFERENCES:

Student Rights and Responsibilities Handbook

**Guidelines for Acceptable Use of Technology by Employees,
Contractors, and Board Members**

Guidelines for Acceptable Use of Technology by Students - Page 6 of 6
Policy 520.00