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

*Saint Paul Public Schools provides access to district technology resources to support learning, enhance instruction, and support school district operations.*

**Employees, contractors, and Board Members must read and comply with Saint Paul Public Schools policies, procedures and guidelines regarding the use of district technology resources, including Board of Education Policy 520.00 *Technology Usage and Safety*, Procedure 520.00.1 *Technology Usage and Safety,* and *Guidelines for Acceptable Use of Technology by Employees, Contractors, and Board Members.***

**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. Communication systems and devices: Telephones, cellular phones, Voice over Internet Protocol (VoIP) phones; voicemail facilities; TelePresence; electronic mail (e-mail); facsimile (fax) machines
   c. 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, and communication and collaboration systems
   d. 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 application (apps) software
   e. Data: Information including text, data files, email, images, video, and audio files that are stored, accessed, or transmitted using district technology
   f. 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.

## ACCESS

### Usage Guidelines

Saint Paul Public Schools (SPPS) provides employees and other authorized individuals access to a variety of district technology resources. When an employee is terminated or leaves the district, their access to district technology resources, including accounts, is terminated. Employees and other authorized users are expected to use the district technology resources to deliver instruction, conduct business, and support district operations. Personal use of district technology resources should be minimal and incidental. The use of district technology resources and access to the Internet is a privilege, not a right. Unacceptable uses of district technology resources may result in one or more of the following consequences: suspension or revocation of use or access privileges; discipline under applicable district policies and procedures; or civil or criminal liability under applicable laws.

### District Property, Privacy, and Terms of Agreement

In Saint Paul Public Schools, district technology resources are the property of the school district. The District reserves all rights to control its technology resources, and maintains the right to monitor or restrict a user's access to or use of district technology resources, including but not limited to, the Internet; to search any computer or device that is assigned to a user or used on any district computer or network; and retrieve, alter and delete any data created, received or maintained by any user using district technology resources. By authorizing use of the district technology resources, the school district does not relinquish control over materials on the system, or materials contained in files on the system. Data and other materials in files maintained on district technology resources may be subject to review, disclosure, or discovery under various laws. Routine maintenance or monitoring of district technology resources may lead to a discovery that a user has violated Policy 520.00, these Guidelines, or the law. An individual search will be conducted if district authorities have a reasonable suspicion that the search will uncover a violation of law or school district policy. The school 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.

Any work prepared by an employee on or with the assistance of district technology resources is considered work for hire under the United States copyright law and is the property of Saint Paul Public Schools. It cannot be licensed or sold for the benefit of any individual employee or user.

### Limitations on School District Liability

Use of the school district technology resources is at the individual's own 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: loss, damage, or unavailability of data stored on or transmitted through district technology resources; delays, changes, or interruptions of service; and missed or non-delivery of information or materials. The school district shall not be responsible for unauthorized financial obligations or consequential damages arising from the use of district technology resources.

### Permission to Use Networks

The District is required to comply with the Children's Internet Protection Act (CIPA) and employ technology protection measures. With respect to 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. The technology protection measures utilized will block or filter Internet access to any visual depictions that:

- Are obscene;
- Contain child pornography; or
- Are harmful to minors.

Employees who inadvertently access an unacceptable site on the Internet or employees who believe that another employee is using district technology resources inappropriately, such as for illegal use, should immediately

notify their supervisor. If there is a reason to believe that there has been misuse of district resources, user accounts may be accessed and searched by network administrators.

**High-Level Filter Access**
The Technology Services Department has enabled a technology measure that will allow SPPS employees to gain authorized high-level filter access to instructional websites such as YouTube. Employees are to use sound judgment when accessing these websites; are expected to comply with all district policies; and must comply with the conditions and terms of service for any external website. High-level filter access is tracked and monitored for compliance. Any misuse or abuse of high-level filter access is a violation of district policy, and 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. Employees should not share high-level filter access with anyone. During periods of high network demand, such as online testing, the District reserves the right to suspend high-level filter access for all users.

The use of any means, including other websites, https, and anonymous proxies, to circumvent the content filter is strictly prohibited, and is a direct violation of Policy 520 and these Guidelines.

**Supervision and Monitoring**
The District expects staff to provide thoughtful student use of the Internet and other electronic resources for classroom assignments, educational research, and college and career planning. Teachers and other district staff who use collaborative online learning spaces, including, but not limited to, Moodle and SPPS Apps, are responsible for monitoring the online communication and collaboration activities of students in these online spaces. When no longer actively using an online class or discussion forum in a learning management system, it is recommended that the employee disable access to the course or discussion forum to prevent unauthorized and unsupervised access to the collaborative discussion space.

**Safety Education**
Under the federal Children's Internet Protection Act (CIPA), the district is required to educate students about appropriate online behavior, online interactions, and cyberbullying awareness and response. School district employees and authorized individuals who work with students are expected to provide students with guidance and instruction in appropriate use and online safety, as well as monitor and supervise student use of the Internet and district technology resources. The district will develop and communicate a plan for delivering the online safety curriculum and identify the teachers and staff responsible for delivering the training. Identified teachers and staff will use the district-provided online safety curriculum and will deliver the instruction in the time frame and manner defined by the district. In addition, teachers and staff will review the *Guidelines for Acceptable Use of Technology by Students* on an annual basis. Teachers and identified staff will complete and submit the requested documentation to certify that they have taught the online safety curriculum.

**USE**

**Unauthorized or Illegal Activities**
Use of district technology resources for unauthorized or illegal activities is prohibited. Unauthorized activities include, but are not limited to:

- Vandalizing, destroying, or tampering with computer hardware, software, and networks;
- Pirating software, music, and/or movies;
- Using or accessing a network, file, or an account owned by another user without their permission;
- Maliciously attempting to harm or destroy another user's data, school or district networks, or the Internet, including uploading or creating viruses;
- Violating copyright laws and licensing agreements;

- Accessing, reviewing, downloading, storing, or printing files or messages that are obscene, vulgar or sexually explicit, or uses language that degrades others.

**Online Etiquette**
All network and email users are expected to abide by school and district policies and guidelines. Be professional, polite, and use appropriate language in all electronic communications.

**Do NOT**
- Swear, use vulgarities, send inappropriate jokes or cartoons;
- Use email or the Internet to harass, bully, mistreat, hurt, or intimidate students, staff or others;
- Send fraudulent, intimidating, or anonymous messages;
- Use email or district networks for commercial, profit-making, political campaign purposes, or illegal activities;
- Distribute materials in such a manner that it might cause congestion of the voice, video, and data networks;
- Use technology resources to access, review, upload, download, store, print, post, receive, transmit, or distribute:
    - Pornographic, obscene, or sexually explicit material or other material or visual depictions that are harmful to minors; or
    - Abusive or threatening materials, including hate mail, or harassing or discriminatory materials that violate school district policies;
- Use technology resources to access another user's file or account without permission;
- Use technology resources to engage in any illegal act or violate any local, state, or federal statute or law.

**Caution Regarding Use of Internet and Email**
Be aware that the Internet and other electronic resources are not private. Your postings may be visible for years. Use common sense, and do not post anything online or in an email that you would not feel comfortable saying in a face-to-face environment. Remember, what you post today may have negative repercussions.

**Email**
Email is an official means of District communication. The district provides employees with an spps.org email account, which is to be used for all official district business and communications. Email communications should be professional in nature, and include appropriate tone, word choice, grammar, and subject matter. All parent and student communications must be conducted via the district-provided email account. Use of a personal email account for parent / student communication and official district business is not authorized.

Email is not confidential or private. Just as a postcard could be intercepted and viewed, electronic communications have the potential for being intercepted and viewed by other individuals. Employees should take into account the level of sensitivity / confidentiality of information being shared via email; the likelihood of inadvertent disclosure to someone other than the intended recipient; and the consequences of inadvertent disclosure to someone other than the intended recipient, before sending sensitive information via email. Confidential information should not be shared in the subject line of an email.

All emails sent from a staff email address are subject to *Policy 520* and the *Guidelines for Acceptable Use.* Employees who deliberately request, save, or forward inappropriate emails, except to promptly report violations to the appropriate supervisor, are in direct violation of Policy 520 and may be subject to disciplinary action.

The email servers and email application are the property of the school district. As school district property, email is subject to record retention laws, and data contained in emails may be requested under the Minnesota Government Data Practices Act.

**SPPS Apps**
Saint Paul Public Schools provides students and staff with access to SPPS Apps, which is a suite of applications provided by Google Apps for Education with the Saint Paul Public Schools brand. SPPS Apps is managed by the district, and is totally separate from a personal Google Apps / Gmail account. SPPS Apps accounts are bound by different terms of service and a contractual agreement with Google. This contract protects the privacy and confidentiality of data in the SPPS Apps domain, and covers email, Google Docs, Calendar, and Sites. SPPS Apps provides authorized users with access to email, Google Docs, Google Calendar, and Google Sites, which may be used for communication and collaboration with students and colleagues. SPPS Apps users may invite Google Apps users, both within and outside the SPPS domain, to view and collaborate on documents. Users must be aware that documents (docs, spreadsheets, presentations) shared outside the SPPS domain are not bound by the same Google terms of service and may be vulnerable to external sharing or data mining. It is the responsibility of each SPPS Apps user to ensure that appropriate sharing controls are used in order to prevent accidental file sharing or publishing of private or confidential information. **Documents with private or confidential student or staff information must not be shared outside of the SPPS Apps domain** (@stpaul.k12.mn.us) **or be published or made public on the Internet**.

**SPPS Apps and Email Forwarding**
While SPPS Apps provides access to email, Lotus Notes is the official district email application for employees. To ensure compliance with record retention laws and efficient operations, employees are required to set up their SPPS Apps email to automatically forward to their Lotus Notes email address (@spps.org). By setting up email forwarding, the employee is only responsible for monitoring a single email account, and all messages sent to the SPPS Apps account will appear in their Lotus Notes email account.

**SPPS Apps and Data Privacy**
The federal Family Educational Rights and Privacy Act (FERPA) protects student education records. Private or confidential student data should never be made publicly accessible, and may only be shared within the SPPS Apps domain with the student and SPPS employees who have a legitimate educational reason for viewing the data.

**Plagiarism / Copyright / Licensing**
Recognize the intellectual property of others, and do not plagiarize. Content on the Internet is considered intellectual property, and is subject to the copyright laws of the United States. Copyrighted material must not be placed on any district, school, classroom, or student web page or online learning space without the permission of the copyright owner. In instances where the copyright owner has granted permission for use, the employee must include a clear citation of the source and list the permission granted by the copyright owner. Any graphics, movies, images, music, or text quoted, paraphrased, or used in presentations, course materials, or other documents under the guidelines of Fair Use must be properly cited using a widely recognized citation format such as MLA, APA, or Chicago style. Employees must make every attempt to request and obtain permission to use copyrighted material, and keep a copy of permissions for your records. Employees must also cite and comply with the guidelines regarding the use of material licensed under a Creative Commons license, where the author or artist denotes the conditions under which the material may be shared, remixed, or reused.

Software and "app"/ application license agreement terms must be strictly followed. Duplicating copyrighted software or apps, without fully complying with license agreement terms, is a serious federal offense and will not be tolerated. Installing unlicensed software on district technology resources is not permitted.

**Back-ups**
A back-up, or the process of making a copy of files and data, is used to restore the original in the event of a disaster or data loss. The district is responsible for creating a backup of data from district-wide applications such as Campus, Moodle, network Travel Folders, and email and other data stored on the servers. It is the ***user's***

responsibility to frequently back up, or make a copy of, his/her own files (word processing documents, presentations, etc.).

**District-owned Portable Electronic Devices**
District-owned portable electronic devices contain sensitive data, which could pose a security risk to both individuals and the school district. These devices are also at an increased risk of being stolen, misplaced, or left unattended. All district technology resources should be handled and stored carefully so that they are not damaged, stolen or lost. For example, electronic devices should not be left inside a vehicle where temperature extremes can permanently damage the equipment or its components, and should not be left unattended in any unlocked area (i.e. classroom, instructional area, office, vehicle, or common area). Laptop computers and personal devices (e.g., iPads, cell phones) should be locked in or on desks, cabinets, or other secured spaces, and should not be left visible while not in the user's possession. Password protection is required on all district-owned portable electronic devices. If a device is stolen, the employee is required to immediately notify the Service Desk and provide the following information: Employee Name, Work Location, Item Description and Property Control Tag Number, and other information regarding the date, time, and location of the theft.

**Non-District-owned Electronic Devices:**
The District assumes no responsibility for loss or damage to personal property, including personal electronic devices. Any damage or theft of the personal property is the responsibility of the owner.

Software, applications, music, and movies residing on personal devices must be privately owned and properly licensed. All devices must include up-to-date anti-virus software. The District retains the right to determine where and when privately owned equipment may connect wirelessly to its network and resources.

District technicians and/or school-based personnel will not service or repair hardware or software owned by the employee. No internal components, software, or applications belonging to the district shall be placed in or on any personal equipment, whether as enhancements, upgrades, or replacements.

Employees shall not use non-district owned electronic devices in any way that would violate any other District policies, including those regarding data privacy, copyright, plagiarism, acceptable use, or bullying and harassment.

**Digital Images, Video, and Audio**
Employees who use personal electronic devices or district-owned electronic devices while at school or school-sponsored activities shall respect the privacy of all individuals. The use of an electronic device to take photographs or record audio or video during the school day is limited to instructional and operational use and to activities that are considered to be in the public arena such as sporting events or public performances. Employees and other authorized users shall not email, post to the Internet, or otherwise electronically transmit images, videos, or audio recordings of other individuals taken at school without their written consent and a signed media release form from a student's parent/guardian.

The possession, use, and sharing of portable electronic devices, including cellular phones, in locker rooms, restrooms, or other uses which constitute an invasion of a person's reasonable expectation of privacy, is strictly prohibited.

**Social Media**
The District may use social media networks and other communication technologies to communicate with the general public. Social media networks include, but are not limited to, web sites, weblogs (blogs), wikis, social networks, online forums, Nings, virtual worlds, and any other social media sites that are available to the general public, but may be blocked on the District network (e.g. Facebook, MySpace, YouTube, Flickr, Twitter, etc.). Employees should not access social media for personal use during District time or via district technology resources.

**Cloud Storage**
Saint Paul Public Schools employees should only use district-approved cloud storage services and applications.

**SAFETY**

**Safety**
When using SPPS Apps, Moodle, or other Web 2.0 tools, users should not post or distribute personally identifiable information that could help someone locate or contact the user or another person. Personal information includes such things as pictures, user names, passwords, email addresses, last name, home address, telephone number, parent/guardian names, or school name and address. The posting of an employee's work-related contact information on the school or classroom website is acceptable. Parent/guardian permission is required to post or publish student work online.

**Passwords**
Passwords are for personal use and must remain confidential. All users are required to change the default password assigned when the account is created. Never share a user name or password with other staff or students, and do not log in to a system and allow another user to access the system. An employee is responsible for all activity performed using the employee's credentials, and many systems record all actions performed under a user's log in and access credentials. Do not steal or use another person's user name and/or password. If a password is compromised, it must be changed immediately. To preserve the integrity of district systems and resources, the District reserves the right to employ technologies to lock an account or log a user out of a system after a period of inactivity.

**Workstation Security Standards**
District computers require users to log in with their Active Directory user name and a secure password before granting local access to the computer or network files. Users should not use a local or generic account to access their workstation, as it does not provide adequate security. A computer or mobile device should be secured whenever it is not in use by logging off or locking access. Leaving a computer or mobile device open and logged in while you are away provides the opportunity for anyone to access your e-mail, grade book, and other sensitive files. Make sure you have completely closed all applications and have logged off of or locked access to the computer or mobile device at the end of the work session, work day, or before leaving your desk / work area.

**Acceptable Use of Technology Agreement for Employees, Contractors, and Board Members**
Employees, contractors, and Board members are required to read and review Policy 520 *Technology Usage and Safety*; Procedure 520.00.1 *Technology Usage and Safety*; *Guidelines for Acceptable Use of Technology by Employees, Contractors, and Board Members*; and read and complete the *Acceptable Use of Technology Agreement for Employees, Contractors, and Board Members*.

**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 REFERENCE:**
Policy 520.00 *Technology Usage and Safety Policy*
Procedure 520.00.1 *Technology Usage and Safety*