

SAN MARCOS UNIFIED SCHOOL DISTRICT  
BOARD POLICY

HUMAN RESOURCES AND DEVELOPMENT

---

EMPLOYEE USE OF TECHNOLOGY

4040  
Page 1 of 3

---

The Governing Board recognizes that technological resources enhance employee performance by offering effective tools to assist in providing a quality instructional program; facilitating communications with parents/guardians, students, and the community; supporting District and school operations; and improving access to and exchange of information. The Board expects all employees to learn to use the available technological resources that will assist them in the performance of their job responsibilities. As needed, employees shall receive professional development in the appropriate use of these resources, including the Online Digital Citizenship Professional Development. The use of District Technology is a privilege permitted at the District's discretion and is subject to the conditions and restrictions set forth in applicable Board Policies, Administrative Procedures, and this Responsible Use Agreement.

Employees shall be responsible for the appropriate use of technology and shall use District technology primarily for purposes related to their employment.

District technology includes, but is not limited to, computers, the District's computer network including servers and wireless computer networking technology (Wi-Fi), the Internet, email, USB drives, wireless access points (routers), tablet computers, smartphones and smart devices, telephones, cellular telephones, personal digital assistants, pagers, MP3 players, wearable technology, online collaboration, file storage services, any system or program owned, managed or licensed by the District, any wireless communication device including emergency radios, and/or future technological innovations, whether accessed on or off site or through District-owned or personally owned equipment or devices.

### **Responsible Uses of District Technology**

The Superintendent or designee shall establish a Responsible Use Agreement which outlines employee obligations and responsibilities related to the use of District technology. Upon employment and whenever significant changes are made to the District's Responsible Use Agreement, employees shall be required to acknowledge in writing that they have read and agreed to the Responsible Use Agreement.

Employees shall not use District technology to access, post, submit, publish, or display harmful or inappropriate matter that is threatening, obscene, disruptive, sexually explicit, or unethical or that promotes any activity prohibited by law, Board policy, or administrative regulations.

### **Prohibited Uses of District Technology**

Harmful matter includes matter, taken as a whole, which to the average person, applying contemporary statewide standards, appeals to the prurient interest and is matter which depicts or describes, in a patently offensive way, sexual conduct and which lacks serious literary, artistic, political, or scientific value for minors. (Penal Code 313)

### **Annual Notifications**

The Superintendent or designee shall ensure that all District computers with Internet access have a technology protection measure that protects against access to visual depictions that are obscene, child pornography, or harmful to minors and that the operation of such measures is enforced. The Superintendent or designee may disable the technology protection measure during use by an adult to enable access for bona fide research or other lawful purpose. (20 USC 7131; 47 USC 254)

The Superintendent or designee shall annually notify employees in writing that they have no reasonable expectation of privacy in the use of any equipment or other technological resources provided by or maintained by the District, including, but not limited to, computer files, email, text messages, instant messaging, and other electronic communications, even when provided their own password. To ensure proper use, the Superintendent or designee may monitor employee usage of District technology at any time without advance notice or consent and for any reason allowed by law.

In addition, employees shall be notified that records maintained on any personal device or messages sent or received on a personal device that is being used to conduct District business may be subject to disclosure, pursuant to a subpoena or other lawful request.

Employees shall report any security problem or misuse of District technology to the Superintendent or designee.

Inappropriate use of District technology may result in a cancellation of the employee's user privileges, disciplinary action, and/or legal action in accordance with law, Board policy, and administrative regulation.

#### Legal Reference:

##### EDUCATION CODE:

52295.10-52295.55 Implementation of Enhancing Education Through Technology grant program

##### GOVERNMENT CODE

3543.1 Rights of employee organizations

6250-6270 California Public Records Act

##### PENAL CODE

502 Computer crimes, remedies

632 Eavesdropping on or recording confidential communications

##### VEHICLE CODE

23123 Wireless telephones in vehicles

23123.5 Mobile communication devices; text messaging while driving

23125 Wireless telephones in school buses

##### UNITED STATES CODE, TITLE 20

7101-7122 Student Support and Academic Enrichment Grants

7131 Internet safety

6751-6777 Enhancing Education Through Technology Act, Title II, Part D, especially;

6777 Internet safety

UNITED STATES CODE, TITLE 47

254 Universal service discounts (E-rate)

CODE OF FEDERAL REGULATIONS, TITLE 47

54.520 Internet safety policy and technology protection measures, E-rate discounts

COURT DECISIONS

City of San Jose v. Superior Court (2017) 2 Cal.5th 608

City of Ontario v. Quon et al. (2010) 000 U.S. 08-1332

Management Resources:

WEB SITES

CSBA: <http://www.csba.org>

American Library Association: <http://www.ala.org>

California Department of Education: <http://www.cde.ca.gov>

Federal Communications Commission: <http://www.fcc.gov>

U.S. Department of Education: <http://www.ed.gov>

Adoption History:

Initial Review: 9/18/18

Approved: 10/16/18

SAN MARCOS UNIFIED SCHOOL DISTRICT  
EXHIBIT  
HUMAN RESOURCES AND DEVELOPMENT

---

EMPLOYEE USE OF TECHNOLOGY

4040  
Page 1 of 5

---

**RESPONSIBLE USE AGREEMENT AND RELEASE OF DISTRICT FROM LIABILITY  
(EMPLOYEES)**

The San Marcos Unified School District authorizes District employees to use technology owned or otherwise provided by the District as necessary to fulfill the requirements of their position. The use of District technology is a privilege permitted at the District's discretion and is subject to the conditions and restrictions set forth in applicable Board policies, administrative procedures, and this Responsible Use Agreement. The District reserves the right to suspend access at any time, without notice, for any reason.

The District expects all employees to use technology responsibly in order to avoid potential problems and liability. The District may place reasonable restrictions on the sites, material, and/or information that employees may access through the system.

The District makes no guarantee that the functions or services provided by or through the District will be without defect. In addition, the District is not responsible for financial obligations arising from unauthorized use of the system.

Each employee who is authorized to use District technology shall sign this Responsible Use Agreement at least once as an indication that he/she has read and understands the agreement, and will acknowledge each year in the Annual Notification Packet.

**Definitions**

District technology includes, but is not limited to, computers, the District's computer network including servers and wireless computer networking technology (Wi-Fi), the Internet, email, USB drives, wireless access points (routers), tablet computers, Smartphones, telephones, cellular telephones, personal digital assistants, pagers, MP3 players, wearable technology, any wireless communication device including emergency radios, and/or future technological innovations, whether accessed on or off site or through District-owned or personally owned equipment or devices.

**Employee Obligations and Responsibilities**

Employees are expected to use District technology safely, responsibly, and primarily for work-related purposes. Any incidental personal use of District technology shall not interfere with District business and operations, the work and productivity of any District employee, or the safety and security of District technology. The District is not responsible for any loss or damage incurred by an employee as a result of his/her personal use of District technology.

The employee in whose name District technology is issued is responsible for its proper care and use at all times. Employees shall not share their assigned online services account information, passwords, or other information used for identification and authorization purposes, and shall use the system only under the account to which they have been assigned to ensure the

confidentiality of both staff and students. Password should be changed regularly to ensure proper security. Employees shall not gain unauthorized access to the files or equipment of others, access electronic resources by using another person's name or electronic identification, or send anonymous electronic communications. Furthermore, employees shall not attempt to access any data, documents, emails or programs in the District's system for which they do not have authorization.

Employees are prohibited from using District technology for improper purposes, including, but not limited to, use of District technology to:

1. Access, post, display, or otherwise use material that is discriminatory, defamatory, obscene, sexually explicit, harassing, intimidating, threatening, or disruptive or that could be construed as harassment or disparagement of others based on their race, ethnicity, national origin, sex, gender, sexual orientation, age, disability, religion, or political beliefs.
2. Disclose or in any way cause to be disclosed confidential or sensitive District, employee, or student information without prior authorization from a supervisor.
3. Send/transmit, download, upload, or post messages that may be considered physically, sexually, or verbally threatening or harassing via text, email, comment, or post.
4. Engage in personal commercial or other for-profit activities without permission of the Superintendent or designee.
5. Engage in unlawful use of District technology for political lobbying.
6. Infringe on copyright, license, trademark, patent, or other intellectual property rights.
7. Intentionally disrupt or harm District technology or other District operations (such as destroying District equipment, placing a virus on District computers, adding or removing a computer program without permission, changing settings on shared computers).
8. Install unauthorized software.
9. Engage in or promote unethical practices or violate any law or Board policy, administrative regulation, or District practice.
10. Degrade or disrupt equipment or system performance (including, but not limited to, inappropriate downloads, streaming, or other activities).
11. Invade the privacy of another.
12. Access, create, post, submit, publish, display, transmit, or otherwise use material that could be used in the production of destructive devices.
13. Develop any classroom or work-related web sites, blogs, forums, or similar online communications representing the District or using District equipment or resources without permission of the Superintendent or designee. Such sites shall be subject to rules and guidelines established for District online publishing activities including, but not limited to, copyright laws, privacy rights, and prohibitions against obscene, libelous, and slanderous content. Because of the unfiltered nature of blogs, any such site shall include a disclaimer that the District is not responsible for the content of the messages. The District retains the right to delete material on any such online communications.

### **Privacy**

Since the use of District technology is intended for use in conducting District business, no employee should have any expectation of privacy in any use of District technology.

The District reserves the right to monitor and record all use of District technology in accordance with applicable law, including, but not limited to, access to the Internet or social media, communications sent or received from District technology, or other uses within the jurisdiction of the District. Such monitoring/recording may occur at any time without prior notice for any legal purposes including, but not limited to, record retention and distribution and/or investigation of improper, illegal, or prohibited activity. Employees should be aware that, in most instances, their use of District technology (such as web searches or emails) cannot be erased or deleted.

All passwords created for or used on any District technology are the sole property of the District. The creation or use of a password by an employee on District technology does not create a reasonable expectation of privacy.

### **Personally Owned Devices**

If an employee uses a personally owned device to access District technology or conduct District business, he/she shall abide by all applicable Board policies, administrative regulations, and this Responsible Use Agreement. Any such use of a personally owned device may subject the contents of the device and any communications sent or received on the device to disclosure pursuant to a lawful subpoena, public records request, or other lawful request.

### **Records**

Any electronically stored information generated or received by an employee which constitutes a District or student record shall be classified, retained, and destroyed in accordance with BP/AR 3580 - District Records, BP/AR 5125 - Student Records, and/or other applicable policies and regulations addressing the retention of District or student records.

### **Appropriate Use of Digital Tools and Resources**

Employees whose duties include supervision of students are expected to provide reasonable supervision and instruction to students under their authority when the students are using District Technology per Board policies, administrative regulations, and other authorities, to monitor students' compliance with their responsibilities under the Student Responsible Use Agreement.

Teachers who are engaged with students in electronic forms of communication are encouraged to follow standard District guidelines for professional conduct as outlined in the SMUSD Employee Handbook in the Employee Conduct section. When communicating with students, keep in mind that the time of day, cultural differences, use of informal language or acronyms all can contribute to the interpretation of appropriate contact. Obtaining parental permission for contact, copying parents on messages, and setting hours of contact can all contribute to professional standards for communication with students. It is recommended that staff utilize

District-owned accounts for electronic communications with students, such as a District-issued email account.

Copyrighted software or data may not be placed on any system connected to the District's system(s) without permission from the holder of the copyright. Only the owner(s) or individuals specifically authorized may upload copyrighted material to the system(s). No teacher/staff member is authorized to perform maintenance or software installations on any District equipment without permission. Staff members wishing to use personal computers on campus, must verify that equipment is running appropriate and updated virus protection. Equipment not running up-to-date anti-virus software may be blocked from the network until it complies. The school district will not provide technical support for personal property, nor will the District install any District-owned software on personal property, or be responsible for problems related to such use.

### **Responsible Use of District Mobile Devices and Loaner Equipment**

Staff members are expected to uphold reasonable standards of care and security to ensure the safety of loaner equipment. This would entail protecting it from damage from food or drink; and securing the equipment in a locked cabinet or desk when not in use. Staff are allowed to use mobile devices off campus, however, they may be responsible for replacement should the equipment be lost, damaged, or stolen when off campus. If transported, it is the employee's responsibility to keep equipment safe and free from damage. This includes locking devices out of sight, in the trunk of your vehicle and not leaving equipment in environments that can cause damage (e.g. hot vehicles, direct sun, moisture, etc.) Equipment is not to be loaned to another staff member, student or family member.

Repairs are to be done by certified District personnel only. Replacements are to be obtained through the District by contacting the Director of Educational Technology.

Loaned equipment remains the property of the San Marcos Unified School District. Equipment does not become the property of staff to which it is assigned.

### **Reporting**

If an employee becomes aware of any security problem (such as any compromise of the confidentiality of any login or account information) or misuse of District technology, he/she shall immediately report such information to the Superintendent or designee.

### **Consequences for Violation**

Violations of the law, Board policy, or this Responsible Use Agreement may result in revocation of an employee's access to District technology and/or discipline, up to and including termination. In addition, violations of the law, Board policy, or this agreement may be reported to law enforcement agencies as appropriate.

Any malicious attempts to harm or destroy District equipment or materials, data of another user of the District's system(s), or any of the agencies or other networks that are connected to the



Internet is prohibited. Deliberate attempts to compromise, degrade, or disrupt system performance may be viewed as violations of District policies and administrative regulations and, possibly, as criminal activity under applicable state and federal laws.

Unauthorized equipment as well as additions/deletions to the network, network equipment, or software are strictly prohibited. Noncompliance with applicable regulations may result in a) disciplinary action consistent with District policies and regulations; b) revocation of account; c) suspension of access to District technology. Violations of law may result in disciplinary action by the District and/or referral to law enforcement.

### **Employee Acknowledgment**

I have received, read, understand, and agree to abide by this Responsible Use Agreement, BP 4040 - Employee Use of Technology, and other applicable laws and District policies and regulations governing the use of District technology. I understand that there is no expectation of privacy when using District technology or when my personal electronic devices use District technology. I further understand that any violation may result in revocation of user privileges, disciplinary action, and/or appropriate legal action.

I hereby release the District and its personnel from any and all claims and damages arising from my use of District technology or from the failure of any technology protection measures employed by the District.

Name: \_\_\_\_\_ Position: Sub Teacher  
(Please print)

School/Work Site: DO/SUBS

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

#### Adoption History:

Initial Review: 9/18/18

Approved: 10/16/18