EMPLOYEE USE OF TECHNOLOGY

The Governing Board recognizes that technological resources enhance 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 training in the appropriate use of these resources.

(cf. 0440 - District Technology Plan)
(cf. 1100 - Communication with the Public)
(cf. 1113 - District and School Web Sites)
(cf. 1114 - District-Sponsored Social Media)
(cf. 4032 - Reasonable Accommodation)
(cf. 4131 - Staff Development)
(cf. 4231 - Staff Development)
(cf. 4331 - Staff Development)

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

(cf. 0410 - Nondiscrimination in District Programs and Activities)
(cf. 4119.11/4219.11/4319.11 - Sexual Harassment)
(cf. 4119.21/4219.21/4319.21 - Professional Standards)
(cf. 4119.23/4219.23/4319.23 - Unauthorized Release of Confidential/Privileged Information)
(cf. 4119.25/4219.25/4319.25 - Political Activities of Employees)
(cf. 5125 - Student Records)
(cf. 5125.1 - Release of Directory Information)
(cf. 6162.6 - Use of Copyrighted Materials)
(cf. 6163.4 - Student Use of Technology)

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, 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.

The Superintendent or designee shall establish an Acceptable 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 Acceptable Use Agreement, employees shall be required to acknowledge in writing that they have read and agreed to the Acceptable Use Agreement.

EMPLOYEE USE OF TECHNOLOGY (continued)

To qualify for federal universal service discounts for Internet access, Internet services, or internal connections (E-rate discounts), districts are mandated by 47 USC 254 to adopt an Internet safety policy that includes, but is not limited to, provisions addressing access by minors to "inappropriate matter" on the Internet; see BP 6163.4 - Student Use of Technology. Consistent with those requirements, the following paragraph provides that employees shall not use district technology to access inappropriate matter. "Inappropriate matter" is not defined in the law and the determination of what matter is considered inappropriate is a local decision to be made by the district. Penal Code 313 provides a definition of "harmful matter" as specified below. Districts that have adopted their own definition should revise the following paragraphs as appropriate.

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.

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)

Note: 47 USC 254 mandates that the district's Internet safety policy for E-rate discounts include the operation and enforcement of a "technology protection measure" that protects against Internet access to visual depictions that are obscene, child pornography, or harmful to minors. Similarly, as a condition of receiving technology funds under Title II, Part D of the No Child Left Behind Act (20 USC 6751-6777) for the purpose of purchasing computers with Internet access or paying for direct costs associated with Internet access, 20 USC 6777 mandates that districts adopt an Internet safety policy that includes the operation of a technology protection measure that protects against access to visual depictions that are obscene or child pornography. Although these requirements focus on measures designed to protect students using district technology (see BP 6163.4 - Student Use of Technology), they also require policy that affects Internet access by adults.

The following paragraph is for use by districts that desire to use E-rate or federal technology funding sources and may be adapted by other districts that choose to install technology protection measures.

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 6777; 47 USC 254)

EMPLOYEE USE OF TECHNOLOGY (continued)

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.

(cf. 4118 - Suspension/Disciplinary Action)
(cf. 4218 - Dismissal/Suspension/Disciplinary Action)

Legal References: (see next page)

EMPLOYEE USE OF TECHNOLOGY (continued)

Legal Reference:

EDUCATION CODE
51870-51874 Education technology
52295.10-52295.55 Implementation of Enhancing Education Through Technology grant program
GOVERNMENT CODE
3543.1 Rights of employee organizations
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 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 Ontario v. Quon et al. (2010) 000 U.S. 08-1332
Management Resources:

Management Resources:

WEB SITES
CDE: http://www.cde.ca.gov
CSBA: http://www.csba.org
California Department of Education: http://www.cde.ca.ov
Federal Communications Commission: http://www.fcc.gov
U.S. Department of Education: http://www.ed.gov
American Library Association: http://www.ala.org

Policy
Adopted: November 1, 2005
Revised: November 15, 2016
GAMUT UPDATE: 7/15

SAUGUS UNION SCHOOL DISTRICT
Santa Clarita, California

ACCEPTABLE USE AGREEMENT AND RELEASE OF DISTRICT FROM LIABILITY (EMPLOYEES)

Acceptable Use

The district network services are provided for education and educators. The use of your account must be in support of education and research and consistent with the educational objectives of the district. Use by individuals for commercial activities is not acceptable, and use for political lobbying is also prohibited.

Privileges

The use of SUSD WAN is a privilege, not a right, inappropriate use will result in a cancellation of the privilege to use these resources through the district. The district administration reserves the right to deny, revoke, or suspend specific user accounts at any time it is deemed necessary.

Network Etiquette

You are expected to abide by the generally accepted rules of network etiquette. These include (but are not limited to) the following:

- Be polite. Never send, or encourage others to send, abusive messages.

- Use Appropriate Language. Remember that you are a representative of yourself and the district on a publicly accessible system. You may be alone with your computer, but what you write is seen globally! Never swear or use vulgarities or any other inappropriate language.

- Privacy. Remember that revealing your own phone number and address is like listing them in a public telephone directory, and may result in unwanted intrusions of your privacy. Do not reveal your telephone number or address.

- Electronic Mail. Electronic mail (e-mail) is not guaranteed to be private. Messages relating to or in support of illegal or unethical activities must be reported to the district administration.

Unacceptable Use

The SUSD WAN may not be used for any purpose which conflicts with the SUSD goals or for illegal or unethical purposes. Appropriateness of use will be determined by the district. The following are examples of use that is inappropriate and, therefore, unacceptable.

EMPLOYEE ACKNOWLEDGMENT INTERNET USE TERMS AND CONDITIONS
(continued)

- Use without having a written acceptance of these terms and conditions on file.

- Sending or receiving messages that have content or purpose which is likely to be illegal or unethical. The district reserves the right to set standards determining the likely illegality or unethical nature of any information residing on the system.

- Transmitting unacceptable content which includes but is not limited to material which is likely to be pornographic, unethical, or contain illegal solicitations, or to be racist or sexist, or to contain inappropriate language for a K-12 environment.

- Transmitting a message with someone else's name as author or using someone else's account.

- Transmitting any material in violation of any United States or California law regulation. This includes copyrighted or trademarked material, threatening or obscene material, or material protected by trade secret.

- Use that impairs or damages the district system operation or these of the district system by another account holder.

- Sharing of an individual account or password. These accounts are not family accounts and are for the use of the employee only.

- The district accounts are not designed for simultaneous use. If the ISP administration determines that an account is being used by more than one person, your account will be suspended to protect your account and e-mail security.

Penalty for Inappropriate Use of the SUSD System

Inappropriate use of the district system may result in a cancellation of the offending account. Each situation which requires review will be handled individually with the dual intent of educating account holders concerning appropriate use and conforming to the district policies and terms and conditions of use.

Services

The district makes no warranties of any kind, whether expressed or implied, for the service it is providing and will not be responsible for any damages suffered while on this system. These damages include lass of data as a result of delays, non-deliveries, or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the Internet is at your own risk. The district specifically disclaims any responsibility for the accuracy of information obtained through its Network Services.

EMPLOYEE ACKNOWLEDGMENT INTERNET USE TERMS AND CONDITIONS
(continued)

Security

Security on any computer system is a high priority. If you identify a security problem, notify the system administrator at once. Never demonstrate the problem to other users. Never use another individual's user ID and password. Any user identified as a security risk due to behavior on the district system or any other system will be denied access to the system.

Vandalism

Vandalism is defined as any malicious attempt to observe information intended to be private or to change data created or owned by another user or any other agency or network that is accessible from the district system or to make any unauthorized changes to the appearance or operational characteristics of the district system. This includes, but is not limited to, the uploading of computer viruses and the changing of any file not owned by the user on the district system. Any vandalism will result in the loss of the account and possible legal referral.

Updating

The district may occasionally require review and update of your account information to continue service. You must notify the district of any changes in your account information.

I hereby accept and understand the above terms and conditions

_____ _____

Employee Signature Date