The Board of Trustees recognizes that technological resources can 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.

Employees shall be responsible for the appropriate use of technology and shall use the district's technological resources 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, web resources, email, USB drives, wireless access points (routers), tablet computers, smartphones and smart devices, cameras, copiers, 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.
District technology is that which is owned or provided by the district.

Personal technology is non-district technology.

Impersonating includes knowingly and without consent creating or accessing an account under another person’s name for purposes of harming, intimidating, threatening, or defrauding an individual or entity. (Penal Code § 528.5)

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 district's Acceptable 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.

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)

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)

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.

Employee(s) shall be prohibited against impersonating other user accounts.

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 Reference:
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
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

Policy ALUM ROCK UNION ELEMENTARY SCHOOL DISTRICT
adopted: July 2, 2013 San Jose, California
Revised: October 10, 2019