LODI UNIFIED SCHOOL DISTRICT

Policy 4040

Personnel

Employee Use of Technology

The Board of Education 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 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, 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.

Employees shall be notified that computer files and electronic communications, including email and voice mail, are not private. Technological resources shall not be used to transmit confidential information about students, employees, or district operations without authority.

Online/Internet Services

The Superintendent or designee shall ensure that all district computers with Internet access have a technology protection measure that prevents access to visual depictions that are obscene or child pornography 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.

To ensure proper use, the Superintendent or designee may monitor employee usage of technological resources, including the accessing of email and stored files. Monitoring may occur at any time without advance notice or consent. When passwords are used, they may be changed by the Superintendent or designee so that he/she may have system access.

The Superintendent or designee shall establish administrative regulations and an Acceptable Use Agreement which outline employee obligations and responsibilities related to the use of district technology. He/she also may establish guidelines and limits on the use of technological resources. Inappropriate use 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.

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.

The Superintendent or designee shall provide copies of related policies, regulations, and guidelines to all employees who use the district's technological resources. Employees shall be required to acknowledge in writing that they have read and understood the district's Acceptable Use Agreement.

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. The district discourages the use of personal devices and/or personal email accounts as being used for district business. An employee shall not transmit student or staff

personal identifiable information to personal devices and/or personal email accounts.

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

Legal References: EDUCATION CODE
51870-51874 Education technology
52270-52272 Education technology and professional development grants
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 20
6751-6777 Enhancing Education Through Technology Act, Especially
Title II, Part D
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
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

Policy
adopted: 05/21/02
revised: 11/19/02
revised: 11/04/03
revised: 01/15/08
revised: 02/16/10
revised: 12/12/17