Superintendent Policy 4040: Acceptable Use Of Technology

Status: ADOPTED

Original Adopted Date: 04/16/2016 | **Last Reviewed Date:** 04/16/2016

The County Superintendent of Schools 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 COE 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 COE technology primarily for purposes related to their employment.

COE technology includes, but is not limited to, computers, the COE'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 COE-owned or personally owned equipment or devices.

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

Employees shall not use COE 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 County Superintendent of Schools or designee shall ensure that all COE 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 County Superintendent of Schools 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 County Superintendent of Schools 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 County Office of Education (COE), 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 County Superintendent of Schools or designee may monitor employee usage of COE 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 COE business may be subject to disclosure, pursuant to a subpoena or other lawful request.

Employees shall report any security problem or misuse of COE technology to the County Superintendent of Schools or designee.

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

Federal	**Description**
20 USC 7101-7122	Student Support and Academic Enrichment Grants
20 USC 7131	Internet Safety
47 CFR 54.520	Internet safety policy and technology protection measures, E-rate discounts

Management Resources	**Description**
Court Decision	City of San Jose v. Superior Court (2017) 2 Cal.5th 608
Court Decision	City of Ontario v. Quon et al. (2010) 000 U.S. 08-1332
Website	U.S. Department of Education
Website	Federal Communications Commission
Website	CSBA
Website	California Department of Education
Website	American Library Association

State	**Description**
Gov. Code 3543.1	Rights of employee organizations
Gov. Code 6250-6270	California Public Records Act
Pen. Code 502	Computer Crimes, remedies
Pen. Code 632	Eavesdropping on or recording confidential communications
Veh. Code 23123	Wireless telephones in vehicles
Veh. Code 23123.5	Mobile communication devices; text messaging while driving
Veh. Code 23125	Wireless telephones in school buses

Exhibit 4040-E(1): Acceptable Use Of Technology

Status: ADOPTED

Original Adopted Date: 04/16/2016 **| Last Reviewed Date:** 04/16/2016

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

The San Luis Obispo County Office of education authorizes County Office of Education (COE) employees to use technology owned or otherwise provided by the COE as necessary to fulfill the requirements of their position. The use of COE technology is a privilege permitted at the COE'S discretion and is subject to the conditions and restrictions set forth in applicable Superintendent policies, administrative regulations, and this Acceptable Use Agreement. The COE reserves the right to suspend access at any time, without notice, for any reason.

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

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

Each employee who is authorized to use COE technology shall sign this Acceptable Use Agreement as an indication that he/she has read and understands the agreement.

Definitions

COE technology includes, but is not limited to, computers, the COE'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 COE-owned or personally owned equipment or devices.

Employee Obligations and Responsibilities

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

The employee in whose name COE technology is issued is responsible for its proper 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. 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 COE's system for which they do not have authorization.

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

1. Access, post, display, or otherwise use material that is discriminatory, defamatory, obscene, sexually explicit, harassing, intimidating, threatening, or disruptive

2. Disclose or in any way cause to be disclosed confidential or sensitive COE, employee, or student information without prior authorization from a supervisor

3. Engage in personal commercial or other for-profit activities without permission of the Superintendent or designee

4. Engage in unlawful use of COE technology for political lobbying

5. Infringe on copyright, license, trademark, patent, or other intellectual property rights

6. Intentionally disrupt or harm COE technology or other COE operations (such as destroying COE equipment, placing a virus on COE computers, adding or removing a computer program without permission, changing settings on shared computers)

7. Install unauthorized software

8. Engage in or promote unethical practices or violate any aw or Superintendent/Board policy, administrative regulation, or COE practice

Privacy

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

The COE reserves the right to monitor and record all use of COE technology, including, but not limited to, access to the Internet or social media, communications sent or received from COE technology, or other uses within the jurisdiction of the COE. 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 COE technology (such as web searches or emails) cannot be erased or deleted.

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

Personally Owned Devices

If an employee uses a personally owned device to access COE technology or conduct COE business, he/she shall abide by all applicable Superintendent/Board policies, administrative regulations, and this Acceptable 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 or public records request.

Records

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

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 COE technology, he/she shall immediately report such information to the County Superintendent of Schools or designee.

Consequences for Violation

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

Employee Acknowledgment

I have received, read, understand, and agree to abide by this Acceptable 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 COE technology or when my personal electronic devices use COE 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 COE and its personnel from any and all claims and damages arising from my use of COE technology or from the failure of any technology protection measures employed by the district.

Name: _____ Position: _____
(Please print)

School/Work Site: _____

Federal References	Description
20 USC 7101-7122	Student Support and Academic Enrichment Grants
20 USC 7131	Internet Safety
47 CFR 54.520	Internet safety policy and technology protection measures, E-rate discounts

Management Resources References	Description
Court Decision	City of San Jose v. Superior Court (2017) 2 Cal.5th 608
Court Decision	City of Ontario v. Quon et al. (2010) 000 U.S. 08-1332
Website	U.S. Department of Education - https://simbli.eboardsolutions.com/SU/XcSsJimoslsh3XhJKy4tplus7wplusA==
Website	Federal Communications Commission - https://simbli.eboardsolutions.com/SU/rFmFn0jtplusslshkbdn8jDPcIlg==
Website	CSBA - https://simbli.eboardsolutions.com/SU/W3QxkK2FPsDsQBnMIENxGg==
Website	California Department of Education - https://simbli.eboardsolutions.com/SU/os2jq5DcA2RawmY2VZ5FZQ==
Website	American Library Association - https://simbli.eboardsolutions.com/SU/ziXdKiQzPM5ZnufeaKplus7jQ==

State References	Description
Gov. Code 3543.1	Rights of employee organizations
Gov. Code 6250-6270	California Public Records Act
Pen. Code 502	Computer Crimes, remedies
Pen. Code 632	Eavesdropping on or recording confidential communications
Veh. Code 23123	Wireless telephones in vehicles
Veh. Code 23123.5	Mobile communication devices; text messaging while driving
Veh. Code 23125	Wireless telephones in school buses