

## Tulare Jt. Union HSD | BP 4040 Personnel

**Employee Use Of Technology**

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.

(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 the district's technological resources primarily for purposes related to their employment.

(cf. 0410 - Nondiscrimination in District Programs and Activities)

(cf. 4119.11/4319.11/4319.11 - 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 outline 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.

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 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. (20 USC 6777; 47 USC 254)

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)

Employees should have no expectation that any communications made using the District's information and communication systems and equipment are exempt from monitoring or access by the District.

## Public Records and Retention

1. Information stored on the District's system and equipment, including email, email attachments, Web postings, and voice mail messages may become records of the District. District records pertaining to the District's business, whether stored in hard copy or electronically, may be considered public records and, therefore, subject to the Public Records Act ("PRA") and Title 5, section 16020, et seq., of the California Code of Regulations, pertaining to the retention and destruction of school records.

2. A District email account is not intended for permanent storage of email. It is each employee's responsibility to save and/or file email that he or she wishes to access, or that are District records and required to be retained by law. "District records" means all records, maps, books, papers, and documents prepared or retained as necessary or convenient to the discharge of official duty and includes any writing containing information related to the conduct of the public's business prepared, School District Email Retention owned, used, or retained by the District regardless of physical characteristics. District records shall be either: (1) saved to an electronic system other than the District email account, (2) electronically archived, or (3) printed on paper and filed as appropriate. Email and other electronic files that are classified pursuant to the District's administrative regulation regarding retention of documents - AR 3580 shall be preserved in one of the three manners described above.

3. The District may access and, to the extent required or allowed by law, disclose any email received, sent, or stored in a District email account. The District may retain or dispose of an employee's email, whether an employee is currently or formerly employed by the District. Email account in-boxes and out-boxes may be purged of email older than five years by the District's information technology department. Email trash folders may be purged as often as every 30 days by the District's information technology department. Staff must notify superintendent or designee of litigation or anticipated litigation in order to preserve related electronic communication.

#### Legal Reference:

#### EDUCATION CODE

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, 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 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>

Policy TULARE JOINT UNION HIGH SCHOOL DISTRICT

adopted: July 15, 2009 Tulare, California

revised: November 5, 2015

revised: January 19, 2017

Tulare Jt. Union HSD | E 4040 Personnel

## **Employee Use Of Technology**

### ACCEPTABLE USE AGREEMENT

#### AND RELEASE OF DISTRICT FROM LIABILITY (EMPLOYEES)

The Tulare Joint Union High 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 regulations, and this Acceptable 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 Acceptable Use Agreement as an indication that he/she has read and understands the agreement.

#### 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 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.

#### 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 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 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

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. Engage in personal commercial or other for-profit activities without permission of the Superintendent or designee
4. Engage in unlawful use of district technology for political lobbying
5. Infringe on copyright, license, trademark, patent, or other intellectual property rights
6. 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)
7. Install unauthorized software
8. Engage in or promote unethical practices or violate any law or Board policy, administrative regulation, or district practice

### 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, 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 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 district 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 district 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 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 Acceptable 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.

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 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: \_\_\_\_\_

(Please print)

School/Work Site: \_\_\_\_\_

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

Exhibit TULARE JOINT UNION HIGH SCHOOL DISTRICT

version: July 2015 Tulare, California

revised: November 5, 2015