

**EMPLOYEE USE OF TECHNOLOGY/ACCEPTABLE USE POLICY**

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 electronic resources that will assist them in their jobs. As needed, staff shall receive professional development in the appropriate use of these resources.

*(cf. 0440 - District Technology Plan)*  
*(cf. 4032 - Reasonable Accommodation)*  
*(cf. 4131 - Staff Development)*  
*(cf. 4231 - Staff Development)*  
*(cf. 4331 - Staff Development)*  
*(cf. 6162.7 - Use of Technology in Instruction)*  
*(cf. 6163.4 - Student Use of Technology)*

Employees shall be responsible for the appropriate use of technology and shall use the District's electronic resources only for purposes related to their employment. Such use is a privilege which may be revoked at any time.

*(cf. 4119.25/4219.25/4319.25 - Political Activities of Employees)*

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

*(cf. 4119.23/4219.23/4319.23 – Unauthorized Release of Confidential/Privileged Information)*  
*(cf. 5125 – Student Records)*  
*(cf. 5125.1 – Release of Directory Information)*

**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. Wireless access to be the District's network must be approved, configured, and encrypted by District Technology Department staff. All other unauthorized wireless devices are to be considered a potential threat to the security of the District's network. Personal computers or wireless devices that can otherwise be used to bypass the District's web filter and are to be considered a violation of student and work place safety are not to be brought into the school/classroom. (20 USC 7001; 47 USC 254)

## **EMPLOYEE USE OF TECHNOLOGY/ACCEPTABLE USE POLICY**

To ensure proper use, the Superintendent or designee may monitor employee use of technological resources, including e-mail, voice mail systems, and stored files, at any time without advance notice or consent. When passwords are used, they must be made available to the Superintendent or designee upon request 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 may also 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 legal/or action in accordance with law, Board policy and administrative regulations.

*(cf. 4118 - Suspension/Disciplinary Action)*

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

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 annually to acknowledge in writing that they have read and understood the District's Acceptable Use Agreement.

*(cf. 4112.9/4212.9/4312.9 - Employee Notifications)*

*(cf. E. 6162.7 – District Software/Copyright User Agreement)*

### **Use of cellular Phone or Mobile Communications Device**

Any employee that uses a cell phone or mobile communications device in violation of law, Board policy, or administrative regulation shall be subject to discipline and may be referred to law enforcement officials as appropriate.

*(cf. 3542 - School Bus Drivers)*

#### *Legal Reference:*

##### *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*

## **EMPLOYEE USE OF TECHNOLOGY/ACCEPTABLE USE POLICY**

*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 Technology Through Technology Act*

*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*

### *WEB SITES*

*CDE: <http://www.cde.ca.gov>*

*CSBA: <http://www.csba.org>*

*Federal Communications Commission: <http://www.fcc.gov>*

*U.S. Department of Education: <http://www.ed.gov>*

*American Library Association: <http://www.ala.org>*

**EMPLOYEE USE OF TECHNOLOGY/ACCEPTABLE USE POLICY**

**Online/Internet Services: User Obligations and Responsibilities**

Employees are authorized to use the District's equipment to access the Internet or other online services in accordance with Board policy, the District's Acceptable Use Agreement, and the user obligations and responsibilities specified below.

1. The employee in whose name an on-line services account is issued is responsible for its proper use at all times. Employees shall keep account information, home addresses and telephone numbers private. They shall use the system only under their own account number to which they have been assigned.

2. Employees shall use the system safely, responsibly and primarily for work-related purposes.

*(cf. 6162.7 - Use of Technology in Instruction)*

3. Employees shall not access, post, submit, publish or display harmful or inappropriate matter that is threatening, obscene, disruptive or sexually explicit, or that could be construed as harassment or disparagement of others based on their race~~s~~, ethnicity, national origin, gender, sexual orientation, age, disability, religion or political beliefs.

*(cf. 4030 - Nondiscrimination in Employment)*

*(cf. 4031 - Complaints Concerning Discrimination in Employment)*

*(cf. 4119.11/4219.11/4319.11 - Sexual Harassment)*

4. Employees shall not use the system to promote unethical practices or any activity prohibited by law, Board policy or administrative regulations.

*(cf. 4119.11/4219.25/4319.25 - Political Activities of Employees)*

5. Employees shall not use the system to engage in commercial or other for-profit activities without permission of the Superintendent or designee.

6. Copyrighted material shall not be placed on the system without the author's permission. Employees may download copyrighted material only in accordance with applicable copyright laws.

*(cf. 6162.6 - Use of Copyrighted Materials)*

7. Employees shall not attempt to interfere with other users' ability to send or receive email, not shall they attempt to read, delete, copy, modify, or forge other users' email.

8. Employees shall not intentionally upload, download or create computer viruses and/or maliciously attempt to harm or destroy District equipment or materials or the data of any

**EMPLOYEE USE OF TECHNOLOGY/ACCEPTABLE USE POLICY**

other user, including so-call “hacking.”

9. Employees shall not develop any classroom or work-related web sites, blogs, forums, or similar online communications representing the District or using the District equipment or resources without permission of the Superintendent or designee. Such sites shall be subject to rules and guidelines established for District online publishing activities including, but not limited to, copyright laws, privacy rights, and prohibitions against obscene, libelous, and slanderous content. Because of the unfiltered nature of blogs, any such site shall include a disclaimer that the District is not responsible for the content of the messages. The District retains the right to delete material on any such online communications.

*(cf. 1113 – District and School Web Sites)*

10. Users shall report any security problem or misuse of the services to the Superintendent or designee.

*(cf. 6163.4 - Student Use of Technology)*



# Fountain Valley School District

## Acceptable Use Policy (AUP) for District Computer Systems Information for Employees

E 4040(a)

The District's Acceptable Use Policy ("AUP") is to prevent unauthorized access and other unlawful activities by users online, prevent unauthorized disclosure of or access to sensitive information, and to comply with the Children's Internet Protection Act ("CIPA"). As used in this policy, "user" includes anyone using the computers, Internet, e-mail, chat rooms, and other forms of direct electronic communications or equipment provided by the District (the "network"). Only current students or employees are authorized to use the network.

The District will use technology protection measures to block or filter, to the extent practicable, access of visual depictions that are *obscene, pornographic, and harmful to minors* over the network. The District reserves the right to monitor users' online activities and to access, review, copy, and store or delete any electronic communication or files and disclose them to others as it deems necessary. Users should have no expectation of privacy regarding their use of District property, network, and/or Internet access or files, including e-mail.

### Acceptable Uses of the FVSD Computer Network or the Internet

Employees and other users are required to follow this policy. Employees are required to confirm their consent to this policy when they activate their account. Even without this confirmation, all users must follow this policy and report any misuse of the network or Internet to a supervisor or other appropriate District personnel. Access is provided primarily for education and District business. Staff may use the Internet for incidental personal use during duty-free time. By using the network, users have agreed to this policy. If a user is uncertain about whether a particular use is acceptable or appropriate, he or she should consult a supervisor or other appropriate District personnel.

### Unacceptable Uses of the Computer Network or Internet

Examples of inappropriate activity on the District web site are listed below. The District, however, reserves the right to take immediate action regarding activities (1) that create security and/or safety issues for the District, students, employees, schools, network or computer resources; (2) that use District resources to access content the District, in its sole discretion, determines to lack legitimate educational content/purpose; or (3) other activities determined by the District to be inappropriate.

- Violating any state or federal law or municipal ordinance, such as: accessing or transmitting pornography of any kind, obscene depictions, harmful materials, materials that encourage others to violate the law, confidential information, or copyrighted materials;
- Criminal activities that can be punished under law;
- Selling or purchasing illegal items or substances;
- Obtaining and/or using anonymous e-mail sites; spamming; spreading viruses;
- Causing harm to others or damage to their property, such as:
  1. Using profane, abusive, or impolite language; threatening, harassing, or making damaging or false statements about others; or accessing, transmitting, or downloading offensive, harassing, or disparaging materials;
  2. Deleting, copying, modifying, or forging other users' names, e-mails, files, or data; disguising one's identity, impersonating other users, or sending anonymous e-mail;
  3. Damaging computer equipment, files, data, or the network in any way, including intentionally accessing, transmitting, or downloading computer viruses or other harmful files or programs, or disrupting any computer system performance;



# Fountain Valley School District

## Acceptable Use Policy (AUP) for District Computer Systems Information for Employees

E 4040(b)

4. Using any District computer to pursue “hacking,” internal or external to the District, or attempting to access information protected by privacy laws; or
  5. Accessing, transmitting, or downloading large files, including “chain letters” or any type of large “image(s) file(s).”
- Engaging in uses that jeopardize access or lead to unauthorized access into others’ accounts or other computer networks, such as :
    1. Using another’s account password(s) or identifier(s);
    2. Interfering with other users’ ability to access their account(s); or
    3. Disclosing anyone’s password to others or allowing them to use another’s account(s).
  - Using the network or Internet for commercial purposes:
    1. Using the Internet for personal financial gain;
    2. Using the Internet for personal advertising, promotion, or financial gain; or
    3. Conducting for-profit business activities and/or engaging in non-government-related fundraising or public relations activities such as solicitation for religious purposes or lobbying for personal political purposes.

Student Internet Safety

1. Students under the age of eighteen should only access FVSD network accounts outside of school if a parent or legal guardian supervises their use at all times. The student’s parent or guardian is responsible for monitoring the minor’s use;
2. Students shall not reveal on the Internet personal information about themselves or other persons. For example, students should not reveal their name, home address, telephone number, or display photographs of themselves or others;
3. Students shall not meet in person anyone they have met only on the Internet; and
4. Students must abide by all laws, this Acceptable Use Policy, and all District security policies.

Penalties for Improper Use

The use of a District account is a privilege, not a right, and misuse will result in the restriction or cancellation of the account. Misuse may also lead to disciplinary and/or legal action for both students and employees, including suspension, expulsion, dismissal from District employment, or criminal prosecution by government authorities. The District will attempt to tailor any disciplinary action to the specific issues related to each violation.

Disclaimer

The District makes no guarantees about the quality of the services provided and is not responsible for any claims, losses, damages, costs, or other obligations arising from use of the network or accounts. Any additional charges a user accrues due to the use of the District’s network are to be borne by the user. The District also denies any responsibility for the accuracy or quality of the information obtained through user access. Any statement accessible on the computer network or the Internet is understood to be the author’s individual point of view and not that of the District, its affiliates, or employees.

---

Employee Signature

---

Date