AR 4040 Employee Use of Technology

Electronic Information Resources

Employees who use District Electronic Information Resources, whether such resources are accessed on District property or remotely, must do so in accordance with this Administrative Regulation, Board Policy 4540 (Employee Use of Technology), Board Policy and Administrative Regulation 1114 (Social Media), and the Employee Acceptable Use Agreement.

District Electronic Information Resources include all computer and information technology hardware, software, data and other resources owned, operated, or leased by the Etiwanda School District including, but not limited to, computers, electronic communication devices, network gear, servers, cloud-based solutions, accounts, passwords, identification numbers, and applications. Electronic communication devices are any non-stationary electronic apparatus capable of recording, storing, processing, and/or transmitting data, video/photo images, or sounds. Examples of such devices include laptops, netbooks, Chromebooks, smartphones, tablets, media players, flash drives, and devices with network access capabilities, whether used on or off campus.

Employees must use District Electronic Information Resources responsibly and for the purpose of learning and District-related communication, instruction, business and administrative activities. An employee who violates this Administrative Regulation or applicable policy, regulation, or Agreement, may lose the privilege of using District Electronic Information Resources and may be subject to discipline, up to and including dismissal, and applicable civil and criminal penalties.

No Expectation of Privacy in Electronic Information Resources

Users have no right of privacy in the use of District Electronic Information Resources. The District may access, monitor, and review any electronic information (such as data associated with Internet use, email, text messages, and voicemail) that is transmitted through District Electronic Information Resources. Information intended to be confidential or personal should not be stored or transmitted using District Electronic Information Resources.

User Obligations and Responsibilities

1. The employee in whose name an online services account is issued is responsible for its proper use at all times. Employees must keep account information and other confidential information, such as student data, home addresses, and telephone numbers, secure. Each employee may use the system only under the employee's assigned user account.

2. Employees shall use the system responsibly and for only work-related purposes.

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/ethnicity, national origin, gender, sexual orientation, age, disability, religion or political beliefs.

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

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

AR 4040 Employee Use of Technology (continued)

6. Employees shall not upload, download or create computer viruses or maliciously attempt to harm or destroy District equipment or materials or the data of any other user, including so-called "hacking."

7. Employees shall not read other users' electronic mail or files. They shall not attempt to interfere with other users' ability to send or receive electronic mail, or read, delete, copy, modify or forge other users' mail.

8. Employees shall not develop any classroom or work-related websites, blogs, forums, or similar online social media communications representing the District or using District equipment or resources without the prior written authorization of the Superintendent or designee. Any online use of the name or logo of the District or its schools must be authorized by the Superintendent or designee. Such site shall be subject to the rules and guidelines established for District online publishing activities, including but not limited to: Board Policy and Administrative Regulation 1114 (Social Media) and federal and state laws.

9. Users shall report any security problem or misuse of Electronic Information Resources to the Superintendent or designee.

District Owned Electronic Devices Policy

All District-owned fixed and portable electronic devices and related equipment and accessories are the property of the District. Such devices may be issued to users at the sole discretion of, and for a duration determined by, the District.

District Rights Regarding District Owned Devices

The District has the right to:

1. Monitor all activity, including but not limited to the content of files and messages, Internet browsing history, and social media connections made from the device.

2. Determine whether specific uses of the device are consistent with the District's acceptable use policies.

3. Deem what is appropriate and disconnect access to the network with or without notice at any time the District Technology Department determines such action is warranted.

Using District-owned Devices on the District Network

1. The Etiwanda School District network is a shared resource. While connected to the District network, employees may not use District-owned devices in any way that compromises the performance, security, or integrity of the District network.

2. Employees may not allow a District-owned device to be directly or indirectly accessed from outside the District network, by use of a modem, wireless connection, or other means.

3. Employees must not attempt to circumvent or defeat any mechanism put in place by the District to manage or secure the network.

AR 4040 Employee Use of Technology (continued)

4. Peripheral equipment such as hubs, routers, switches, bridges, wireless access points, printers or other equipment may not be connected to the District network unless approved in writing by the District Technology Department.

Copyright Policy

District-owned devices connecting to the District network must not be used to access, copy, or store illegal or unauthorized copyrighted materials. Such materials include, but are not limited to: copyrighted music, digitized video from copyrighted motion pictures, copyrighted software, photographs, artwork, and books.

Privately Owned Computing Devices Policy

With prior authorization from the District Information Technology department, employees may use personal electronic devices for District business and educational purposes, including to stay connected to colleagues and the workplace, access and use work-related data, or complete tasks related to their employment. Approval to use a personally owned device for these purposes must be obtained in advance from the system administrator and the employee's site administrator or manager. Employees may not use personally owned electronic devices for personal business or communication while on duty, except in emergency situations or during scheduled work breaks.

User Responsibilities

Employees are responsible for the maintenance and repair of their own devices and related equipment. Any software or hardware related issues that arise while a privately owned device is connected to the District network is the employee's responsibility.

Employees who access District data, including but not limited student or employee information, on privately owned devices are responsible for safeguarding that data with appropriate security measures. Such measures include, but are not limited to, use of passwords, care in the handling and transportation of the device, and secure storage of the device when unattended or not in use.

Network Access

Privately owned devices may access the District network only via the guest wireless network(s). Access to the District network using an unauthorized wired or wireless connection is prohibited. Devices using an unauthorized connection will be disconnected without notice.

1. The District network is a shared resource. While connected to the District network, employees may not use privately owned devices in any way that compromises the performance, security, or integrity of the District network.

2. Employees may not allow privately owned devices that are connected to the District's network to be directly or indirectly accessed from outside of the District network.

3. Employees must not attempt to circumvent or defeat any mechanism put in place by the District to manage or secure the network.

4. Peripheral equipment such as hubs, routers, switches, bridges, wireless access points, printers or other equipment may not be connected to the District network unless approved in writing by the District Technology Department.

AR 4040 Employee Use of Technology (continued)

District Rights Regarding Privately Owned Devices

Privately owned devices used in District facilities or to access the District's network or data are subject to District monitoring to determine whether such use is consistent with applicable laws, policies, and regulations. The District may disconnect or discontinue a user's access to the network with or without notice at any time the District Technology Department determines such action is warranted.

Copyright Policy

Privately owned devices connecting to the District network must not be used to download, copy, or store illegal or unauthorized copyrighted materials.

Board Approved:
October 10, 2018
July 22, 2015
July 17, 2014
April 10, 2008
August 19, 2004
Effective Date: August 19, 2004