CORONA-NORCO UNIFIED SCHOOL DISTRICT

AR 8340

INFORMATION TECHNOLOGY SERVICES

ALL EMPLOYEES

PERSONAL DEVICE POLICY

Employee use of personal devices (e.g., laptops, tablets, smart phones, and network connected peripherals) provides opportunities to improve results in regard to student learning, teacher collaboration, administrative effectiveness, and other aspects of the District's mission. When used capably and appropriately, these devices enable our employees to be more effective, efficient, and flexible; which, in turn, improves their capacity to promote educational and operational excellence.

Accordingly, the District will allow employees to use personal devices on the District's facilities and specified networks, in accordance with the Employee Responsible Use Policy (AR 8310) and the following guidelines.

A. General Guidelines

A personal device is a privately owned electronic appliance, which may include laptops, tablets, smart phones, and any current or emerging devices that can be used for word processing, Internet access, recording of images or sound, email, text messages, applications, and other electronic communication.

The District's Bring Your Own Device ("BYOD") network is a wireless data transmission medium created and maintained by the District for the dedicated purpose of supporting secure connection of personal devices to the Internet and selected District information resources.

Any personal device connected to the District's BYOD network will be configured with the District's Enterprise Mobility Management ("EMM") solution. EMM applies management policies to the personal device to establish a safe, secure, and productive environment for students and employees. It is the employee's responsibility to make sure their device meets the minimum requirements and is capable of EMM enrollment. Employees will be held responsible for appropriate use and maintenance of their device.

Personal devices on the District's facilities or BYOD network should be used by employees in an ethical and responsible manner. The use of the District's BYOD network or of a personal device on District facilities is a privilege, not a right; misuse may result in the restriction or cancellation of access. Misuse may also lead to disciplinary and/or legal action for employees, up to and including dismissal from District employment or criminal prosecution by government authorities.

The use of personal devices by employees is optional. Employees who choose not to bring their own device will not be penalized.

B. Employee Responsibilities

Personal devices are the sole responsibility of the employee who assumes the risk for personal devices brought to District facilities. The District accepts no responsibility for either the security of, or the data residing on the personal device and will not support, repair or troubleshoot personal devices. The District shall not be liable for any lost, stolen, or damaged personal devices, including any loss of data or other content from such devices.

The District will not pay any charges or fees from cellular or other service providers incurred as a result of an employee's use of personal devices on District facilities. Any software or hardware related issues that arise while a personal device is connected to the District network are the employee's responsibility.

Employees who access District data, including, but not limited to, student or employee information on personal 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 is use.

Camera, video, or voice recording functionality on personal devices shall not be used in any manner that infringes on the privacy rights of other persons. No recording of any kind is permitted in bathrooms, locker rooms, nurse's office, staff offices, or any other areas where there is an expectation of privacy.

Employees agree to a code of conduct that recognizes the need to use their personal device appropriately when on the District's facilities or BYOD network, as follows:

1. Ensure the security of their personal device.

2. Maintain the configuration, operating system, and applications of the personal device. This includes ensuring that the personal device's security controls are not subverted via "hacks", jailbreaks, roots, security software changes, or changing security settings.

3. Refrain from sharing or lending their personal device to students, parent/guardians, employees, or other persons.

4. Disable the personal device from serving as a hub ("hotspot") for other wireless devices while on the District's facilities.

5. Prevent the storage of inappropriate data on the personal device such as, but not limited to, images or content that may be deemed harmful to minors and sensitive student or staff information that should only reside on District controlled computing resources.

6. Limit personal use of the personal device (i.e., for other than educational or administrative purposes), such that any personal use has no adverse effect on any student's academic performance or on the employee's job performance, imposes

no tangible cost to the District, and does not unduly burden the District's resources.

7. Respect and not abuse the District's limited networking, computing, and security resources. This includes taking reasonable and prudent steps to prevent the personal device from unduly burdening or creating a security risk to the District's resources. Personal devices shall not be connected to any District network via a hardwire (i.e., cabled) connection; connection for personal devices shall exclusively be via the wireless BYOD network.

8. Cooperate with efforts by the District's Information Technology Department to resolve operational or security concerns that they believe may stem from personal devices and the District's BYOD network.

9. Remove a personal device from EMM when the employee exits the District, transfers ownership or control of the personal device, or decommissions the personal device from regular use.

10. Ensure use is ethical and responsible.

C. Device Recommendations

The District will provide a list of minimum specifications that the personal device must meet to be connected to the District's BYOD network. Personal devices that do not meet the minimum requirements or are not listed as recommended devices cannot be used on the District's BYOD network. The District may provide a list of devices that are disallowed on the District's facilities or BYOD network.

D. Use of Enterprise Mobility Management (EMM)

To use the District's BYOD network, personal devices will be enrolled in EMM, which will apply management policies that establish a safe, secure, and productive environment for students and employees. The District may send notifications or workplace appropriate content to the personal device from EMM. The District will be responsible for all licensing costs relating to this content.

E. Monitored Use

The District participates in and receives funding from the Federal FCC E-rate program, which mandates that the District be compliant with the Federal Children's Internet Protection Act ("CIPA") as amended by the Protecting Children in the 21st Century Act. This requires the District to have a filtering system that actively monitors and filters inappropriate Internet content. Any attempts to bypass the District's content filtering or security measures are prohibited and will result in a loss of privileges.

When using a personal device that is not connected to the District's BYOD network (e.g., by using a cellular data plan), the employee must remain aware that the Internet content received on that personal device is not protected by the District's filtering system. The employee will be responsible for ensuring that any content that is available for students on that personal device meets the District's policies for content filtering (AR 8320, AR 8520). The District recommends employees use devices connected to a District network when engaged in District related activities. If an employee becomes aware of any security problem with their personal device while on the District's facilities or BYOD network, they shall immediately report such information to the Information Technology Help Desk.

To comply with CIPA requirements and certify adherence to the Employee Responsible Use Policy (AR 8310) while using the District's BYOD network, each employee's personal device will be subject to protection and monitoring systems. Any inappropriate material and/or unauthorized configuration changes will be monitored, and appropriate disciplinary procedures will be enforced. Removal of EMM components from a personal device will result in the device losing access to the District's BYOD network.

Upon enrollment of a personal device into EMM, basic information such as, but not limited to, make, model, operating system version, installed applications, and device serial number will be logged. It is not the District's intention to actively manage or access personal devices. In situations where there is a potential violation of the Employee Responsible Use Policy (AR 8310), the District reserves the right to investigate activities on the District's network, including BYOD devices, to determine if any wrongdoing occurred. The District reserves the right to monitor employees' Internet use. If an employee is found to have violated Board policies or administrative regulations, then the employee's user privileges may be suspended, revoked, canceled or limited, and the violation may result in disciplinary action.

F. Employee Personal Device Privacy

1. Employees should be aware that the contents of the personal device and any communications sent or received on the device may be subject to disclosure:

   - According to the California Public Records Act (CPRA), when an employee conducts public business using private email or personal devices, those communications may be subject to disclosure.

   - Employees who bring a personal device onto District facilities or connect it to the District's BYOD network are considered the "authorized possessors" or owners of personal devices within the meaning of the California Electronic Communications Privacy Act (Penal Code section 1546 et seq.) to the extent, if any, the Act applies.

Accordingly, any employee who elects to possess or use a personal device on the District's BYOD network is deemed to have consented to a search of that device by District authorities if reasonable suspicion of a violation of District rules or federal, state or local law exists, pursuant to all applicable laws and District policies.

2. The District respects an employee's privacy in regard to their personal device. The District will monitor information about the device only as necessary to provide a safe and secure environment for our students and employees. Upon request, the District will provide a list of the type of information that is collected from personal devices.

G. 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 an employee accrues due to the use of the District's network are to be borne by the employee. The District also denies any responsibility for the accuracy or quality of the information obtained through employee 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.

By permitting an employee to bring a personal device to District facilities, the employee agrees to not hold the District or any District staff responsible for the failure of any technology protection measures, violations of copyright restrictions, or users' mistakes or negligence. The employee agrees to indemnify and hold harmless the District and District personnel for any damages or costs incurred as a result of the employee's use and possession of the device.

Legal Reference: CSEA code of ethics, NEA code of ethics, CPSEL Administrative Standards

Administrative Regulation Dated: September 3, 2019