

INFORMATION TECHNOLOGY SERVICESALL STUDENTSPERSONAL DEVICE POLICY

The District uses educational technology as one way of enhancing our mission to teach the skills, knowledge and behaviors students will need as responsible citizens in the global community. Students learn collaboration, communication, creativity and critical thinking in a variety of ways throughout the school day. The District strives to provide appropriate and adequate technology to support instructional purposes. The use of personal devices by students is optional, and students who choose to not use a personal device will not be penalized and alternate modes of participation will be available.

The District will allow students to use personal devices on the District's school grounds, other facilities, and specified networks, in accordance with the Student Responsible Use Policy (AR 8510) 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, messages, 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. It is the student's responsibility to make sure their device meets the minimum requirements and is capable of EMM enrollment.

Personal devices on the District's facilities or BYOD network should be used by students 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, and misuse may result in the restriction or cancellation of access. Misuse may also lead to disciplinary and/or legal action for students, including expulsion or criminal prosecution by government authorities.

Students will be held responsible for appropriate use and maintenance of their device, and parents/guardians are encouraged to support such use and care.

## B. Student Responsibilities

Personal devices are the sole responsibility of the student and parent/guardian, who assume the risk for personal devices brought to school grounds and other District facilities. The District accepts no responsibility for either the security of, or the data residing on, the personal device and has no duty to support, repair or troubleshoot personal devices. Under no circumstances, including those when District staff attempt to assist the student (on a “best effort” basis) with their personal device, shall the District be responsible for the personal device’s replacement, repair, configuration or data. 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 a student’s use of personal devices on school grounds or other District facilities. Any software- or hardware-related issues that arise while a personal device is connected to the District network are the student’s and parent/guardian’s responsibility.

Students should bring their devices to school with a fully charged battery. The District is not responsible for providing an opportunity or the necessary power to charge the device during the school day.

Students are to use their devices in locations and at times as permitted by teachers, administrators, or other District employees. Students must use devices as directed by their teacher, and must comply with District and school site rules and regulations regarding use of the personal device.

Camera, video, or voice recording functionality on personal devices shall not be used in any manner which infringes on the privacy rights of any other persons. This includes recording, sending, or posting images or sounds of any person without their permission. No recording of any kind is permitted in a classroom without the express permission of the teacher. No recording of any kind is permitted in bathrooms, locker rooms, nurse’s offices, administrator’s offices, or any other areas where there is an expectation of privacy. Students may not turn on, activate, or utilize a personal device during testing or assignment unless given permission by a teacher.

When a student uses any prohibited device or uses a permitted personal device in a manner inconsistent with District or school site rules and regulations, or for illegal activity, a District employee may confiscate the device. The employee shall store the item in a secure manner until an appropriate time.

The District advises students and parents/guardians that device storage capacity be prioritized for pedagogical practices. Personal applications and content should not compromise the educational purpose of the device when used in the Personal Device program.

Students agree to a general code of conduct that recognizes the need to use their personal device appropriately when on school grounds, other District facilities or the BYOD network, as follows:

1. Ensuring the physical security of their device.
2. Maintaining 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. Refraining from sharing or lending their personal device to students, employees, or other persons.
4. Disabling the personal device from serving as a hub (“hotspot”) for other wireless devices while on school grounds or other District facilities.
5. Preventing the storage of inappropriate data on the personal device. This includes, but is not limited to, images or content that may be deemed harmful to minors.
6. Limiting personal use of the personal device (i.e., for other than educational purposes), such that any personal use has no adverse effect on their or any other student’s academic performance, imposes no tangible cost to the District, and does not unduly burden the District’s resources.
7. Respecting, and not abusing, 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 be exclusively via the wireless BYOD network.
8. Cooperating 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. Removing a personal device from EMM when the student graduates or otherwise departs from the District, transfers ownership or control of the personal device, or decommissions the personal device from regular use.
10. Ensuring use is consistent with District and school site rules and regulations.

#### 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 school grounds, other District’s facilities, or the BYOD network.

#### D. 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 21<sup>st</sup> Century Act. This requires the District to have a filtering system in place that actively monitors and filters inappropriate internet content. Any attempts to bypass the District’s content filtering or security measures are prohibited and may

result in a loss of privileges and disciplinary action.

While on school grounds or other District facilities, students must use the District's BYOD network to connect their personal device. Use of any alternate internet access, including cellular data services, is strictly prohibited.

Despite the District's best efforts, the filtering system is unable to restrict access to all potentially offensive and controversial materials. Any attempts to bypass the District's content filtering or security measures are strictly prohibited and will result in a loss of privileges and may result in disciplinary action.

If a student becomes aware of any security problem with their personal device while on school grounds, other District facilities, or while accessing the BYOD network, they shall immediately report such information to the teacher or other District personnel.

To support the District's CIPA compliance requirements and certify adherence to the Student Responsible Use Policy (AR 8510) while using the District's BYOD network, each student'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 intention of the District to actively manage or access personal devices. In situations where there is a potential violation of the Student Responsible Use Policy (AR 8510), school site or District rules and regulations, or the law, the District reserves the right to investigate activities on the District's network, including personal devices, to determine if any wrongdoing occurred. The District reserves the right to monitor students' Internet use while on school grounds and other District facilities. If a student is found to have violated school site or District rules and regulations, then the student's user privileges may be suspended, revoked, canceled or limited, and the violation may result in disciplinary action.

#### E. Student Personal Device Privacy

The District respects a student'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. Upon request, the District will provide a list of the type of information that is collected from personal devices.

No warrant or subpoena is required for District officials to obtain or to search a personal device in the possession of a student. Education Code section 48901.5 permits the District to regulate use and possession of electronic devices on school premises. Students and parents/guardians who bring a personal device onto school grounds or other District facilities agree they 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 student who elects to possess or use a personal device on school grounds or other District facilities is deemed to have consented to a search of that device by school

authorities if reasonable suspicion of a violation of federal, state, or local law, or school site or District rules and regulations exists, pursuant to all applicable laws and District policies.

F. Applications and Software Used in the Classroom

The District does not require software for personally owned devices. The District reserves the right to send “push” notifications and educational content to the personal device. Any applications the District pushes to devices will be of no cost to the student or parent/guardian.

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 a student accrues due to the use of the District’s network are to be borne by the student. The District also denies any responsibility for the accuracy or quality of the information obtained through student 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 a student to bring a personal device to school grounds and other District facilities, the parent/guardian agrees to not hold the District or any District employees responsible for the failure of any technology protection measures, violations of copyright restrictions, or users’ mistakes or negligence. The parent/guardian agrees to indemnify and hold harmless the District and District personnel for any damages or costs incurred as a result of the student’s use and possession of the device.