Student Responsible Use Agreement
EC 48901.5 (PSD BP 6163.4)

Instruction
The Palmdale School District ("District") authorizes students to use District technology for educational purposes only. The use of District technology is a privilege, not a right. All use of District is subject to the restrictions set forth in federal and state law, Board policies, administrative regulations, and this Responsible Use Agreement. The District reserves the right to suspend or limit access at any time, without notice, for any reason.

The District expects all students to use technology, the District's or others', responsibly at all times. The District may place restrictions on the sites, material, and/or information that students may access through District technology.

All aspects of this Responsible Use Agreement apply equally whether District technology is accessed on or off site or through District-owned or personally-owned equipment or devices.

Definitions
District technology includes, but is not limited to, District-owned devices (e.g., District owned computers, smart phones, smart devices, tablet computers, telephones, cellular phones, USB drives, wireless access points (routers), personal digital, wearable technology, any wireless communication device (emergency radios, etc.); the District's email system computer network, servers, wireless computer networking technology (Wi-Fi), online collaboration, file storage services; any system or program owned, managed or licensed by the District; peripherals; interactive projection systems; access to network information sources (e.g., the Internet); and future technological innovations.

Privacy
Students have no reasonable expectation of privacy in any use of District technology or accounts, whether at school or at home. The District may access, monitor, and record all student use of District technology without specific advanced notice, including, but not limited to, any and all student email and other District provisioned accounts, access to the Internet or social media, communications sent or received from District technology or accounts, or other uses. Students should be aware that, in most cases, their use of District technology and accounts (such as web searches and Drive storage) cannot be erased or deleted and can be monitored.

The district may create online accounts (Google, Apple, etc.) for students to be used for educational purposes. The district reserves the right, but is not obligated, to monitor, suspend, restrict access, and/or delete student accounts. All passwords/accounts created for or used on any District technology belong to the District. The creation or use of a password by a student using District technology does not create a reasonable expectation of privacy. In the creation of student accounts the District will perform due diligence to ensure that student data is protected, both by the vendor and the District. The data that students create, store, and/or transmit using District technology is not private and is considered the property of the District.

By using District technology and/or accounts, whether from personally or District-owned devices, students and parents grant specific consent, as defined by the California Electronic Communications Privacy Act ("CalECPA"), also known as Senate Bill 178, to the District searching and monitoring all use of District

Technology, including, but not limited to, electronic communication information and electronic device information created, stored, or transmitted via District technology.

Use Restrictions
The use of personal electronic devices and/or District technology on campuses is permitted. Please refer to school site policies regarding limitations of use on campus.

Electronic devices/technology may not be used at any time in locker rooms, restrooms, the nurse's office, and/or any area where individuals have an expectation of privacy.

Students are prohibited from photographing, video and/or audio recording, or posting any content online, without express permission from a District faculty member. Recording a teacher at any time without consent is illegal according to California Education Code Section 51512.

Reporting
If a student becomes aware of any security problem, unauthorized log in, or misuse of District technology, he/she shall immediately report such information to the teacher or other District personnel. If a student unintentionally gains access to another student's account, he/she should immediately notify a teacher or District personnel and log-out of that account.

District-Owned Devices
Upon receipt of a District-owned device, the student and the student's parents are the authorized possessor as defined in CalECPA. As an authorized possessor of a District-owned device, students are responsible for using the device appropriately for educational purposes and in accordance with the Responsible Use Agreement. The District may confiscate any District-owned device at any time and without cause. If the District confiscates a District-owned device, the student is no longer the authorized possessor of the device.

Personally Owned Devices
If a student uses a personally owned device to access District technology, he/she shall abide by Board policies, administrative regulations, this Responsible Use Agreement, and the Student Code of Conduct/Student Handbook. The student is fully responsible, at all times, for the personally-owned device brought to school.

Students using personally-owned devices on District property must use the District's filtered network by authenticating and logging. **The use of private (3G/4G/5G/LTE Data) network access on District property is strictly prohibited.** Violators may have their devices inspected, their right to use personally-owned devices on District property restricted or terminated, and/or be subject to other disciplinary action.

Participation in this program is not required. Students who utilize their own devices on campus will be deemed an authorized user of the device by the District and will be required to grant the District access to the device in the event there is a reasonable suspicion of wrongdoing and/or for the teacher to access student work product in conjunction with curriculum and instruction. Students' personally owned devices may be searched if there is a reasonable suspicion, under the circumstances, that the student is violating law, District policy, or school rules. (New Jersey v. T.L.O)

Student Obligations and Responsibilities

Students are expected to use District technology safely, responsibly, and for educational uses only. The student is responsible for proper use of account(s) and/or District technology issued to him/her at all times. Students must keep private and not share their account information, passwords, or other information at any time. Students shall only use their assigned account(s).

The following list is meant to provide families with examples of prohibited conduct but is not intended to serve as a comprehensive list.

- Access, share, post, or otherwise use material that is discriminatory, obscene, profane, abusive, threatening, disruptive, defamatory, inaccurate, sexually explicit, offensive, illegal, or damaging to another's reputation.
- Access, share, transmit, post, display, publish or otherwise use material that could be construed as harassing or disparaging of other based on their race/ethnicity, national origin, sex, gender, sexual orientation, age, disability, religion, or political beliefs.
- Harass, intimidate, or threaten students, staff, or other individuals (cyberbullying)
- Share, use, or distribute personal identification information (such as name, address, phone number, or other information) about themselves or others.
- Visit social networking sites (including Facebook, Instagram, Twitter, Tik Tok, etc.) without the express permission of a District faculty member.
- Encourage or engage in the use or sale of drugs, alcohol, tobacco, or banned substances.
- Search for and/or visit inappropriate websites (such as websites containing lewd, sexually suggestive, or graphically violent images or demeaning, derogatory, or hateful speech).
- Record video or audio, or take photographs of other students or staff; transmit, post, or share images, videos, and/or audio files created without express permission from a District faculty member.
- Infringe on copyright, trademark, patent, or other intellectual property rights, including, but not limited to using others' intellectual property without citation or expressed permission.
- Intentionally harm District technology or other District operations (such as destroying District equipment; uploading, downloading, or creating a virus on District computers; adding or removing a computer program; changing settings on shared computers; etc.), or "hack" into District technology to change or use data of the District or other users.
- Create alternate (fake) accounts, login information, or passwords..
- Engage in or promote commercial and/or for-profit activities.
- Engage in or promote unethical practices or any activity prohibited by law, Board policy, administrative regulations, or Student Code of Conduct/Handbook.

Academic and behavioral policies and expectations are applicable to all technology use on and off campus that may cause a serious disruption on campus. The District reserves the right, but is not obligated, to intervene when off campus issues are brought to its attention.

Consequences for Violation

Violations of the law, Board policy, administrative regulations, or this Responsible Use Agreement may result in a student's loss of access to District technology and/or discipline, up to and including suspension or expulsion. In addition, violations of the law, Board policies, administrative regulations, or this Responsible Use Agreement may be reported to law enforcement agencies as appropriate.