Paso Robles Joint USD

Exhibit

Student Responsible Use Of Technology

E 6163.4
Instruction

COMPUTER AND NETWORKED INFORMATION RESOURCES

RESPONSIBLE USE AGREEMENT FOR STUDENTS

Paso Robles Joint Unified School District recognizes that access to technology in school gives students greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. We are committed to helping students develop 21st-century technology and communication skills. To that end, we provide access to technologies for student and staff use. This Responsible Use Policy outlines the guidelines and behaviors that users are expected to follow when using school technologies or when using personally-owned devices on the school campus. Before using on-line services, the student and parent/guardian shall sign the district's CIPA (Children's Internet Protection Act) Compliant Responsible Use Policy indicating that the student understands and agrees to abide by specified user obligations and responsibilities.

The Superintendent or designee shall notify students and parents/guardians about authorized uses of district computers, user obligations and responsibilities, and consequences for unauthorized use and/or unlawful activities in accordance with district regulations and the district's Responsible Use Agreement.

(cf. 5125.2 - Withholding Grades, Diploma or Transcripts)
(cf. 5144 - Discipline)
(cf. 5144.1 - Suspension and Expulsion/Due Process)
(cf. 5144.2 - Suspension and Expulsion/Due Process (Students with Disabilities))
(cf. 5145.12 - Search and Seizure)

The Superintendent or designee shall ensure that all district computers with Internet access have a technology protection measure that blocks or filters Internet access to visual depictions that are obscene, child pornography, or harmful to minors and that the operation of such measures is enforced. (20 USC 6777, 47 USC 254)

To reinforce these measures, the Superintendent or designee shall implement rules and procedures designed to restrict students' access to harmful or inappropriate matter on the Internet and to ensure that students do not engage in unauthorized or unlawful online activities. Staff shall supervise students while they are using online services and may have teacher aides, student aides, and volunteers assist in this supervision.

The Superintendent or designee also shall establish regulations to address the safety and security of students and student information when using email, chat rooms, and other forms of direct electronic communication.

The Superintendent or designee shall provide age-appropriate instruction regarding safe and appropriate behavior on social networking sites, chat rooms, and other Internet services. Such instruction shall include, but not be limited to, the dangers of posting personal information online, misrepresentation by online predators, how to report inappropriate or offensive

content or threats, behaviors that constitute cyberbullying, and how to respond when subjected to cyberbullying.

Usage Policies

All technologies provided by the district are intended for education purposes. All users are expected to use good judgment and to follow the specifics of this document as well as the spirit of it: be safe, appropriate, careful and kind; don't try to get around technological protection measures; use good common sense; and students are expected to ask teachers if they don't know.

Technologies Covered

PRJUSD may provide Internet access, desktop computers, mobile computers or devices, videoconferencing capabilities, online collaboration capabilities, message boards, email, and more. As new technologies emerge, PRJUSD will attempt to provide access to them. The policies outlined in this document are intended to cover all available technologies, not just those specifically listed. This includes Personal Electronic Devices when allowed through this policy.

Network and Computer Use Conduct/Acceptable Use

The Paso Robles Joint Unified ~~Public~~ School~~s~~'District's computer system is expected to be shared and available to all approved users. The computer may not be used in such a way as to disrupt or interfere with its use by others. The student, in whose name an on-line services account is issued, is responsible for its proper use at all times. Students shall keep personal account numbers, home addresses and telephone numbers private. They shall use the system only under their own account number. Students shall use the district's system responsibly and solely for educational purposes. Inappropriate conduct in the use of the system includes, but is not limited to:

- Damage, vandalism or theft of equipment
- Theft, piracy, and altering software
- Installation/Downloading/Utilization of unauthorized/unapproved software including file sharing, proxy, network or user monitoring, /remote access software
- Theft of services

- Use of the system to communicate unlawful information or to transmit computer viruses/trojan/back door software.
- Accessing information which is pornographic, obscene, sexist, racist or abusive
- Plagiarism of ideas or information
- Violation of copyright
- Use of the system for commercial purposes or for political campaigning
- Assuming another person's identity on the network (e.g. using a login/password that is not the user's)
- Attempting to gain and/or Subvert/Bypass PR~~P~~JUSD's computer security/file management system
- Not using the PR~~P~~JUSD's assigned login/password during any computer use
- Attempting to gain unauthorized access to the PR~~P~~JUSD Network and/or computer workstations
- Making deliberate attempts to disrupt computer system or network, destroy computer data or student assessment/grade/progress data, or physically modify, harm, or destroy any computer or network hardware
- Utilization of file sharing software to obtain copy protected/copyrighted/ inappropriate files.
- Attempting to vandalize equipment and/or harass other users. Vandalism is defined as any malicious attempt to harm, modify, or destroy data of another user, which includes, but is not limited to, the loading or creating of computer viruses. Harassment/Cyberbullying is defined as the persistent annoyance of other users, or the interference of another user's work. Harassment includes, but is not limited to, the sending of unwanted e-mail Cyberbullying is defined as unwelcomed verbal, written or physical conduct, but is not limited to the following misuses of technology: harassing, teasing, intimidating, threatening, or terrorizing another student or staff member by way of any technological tool, such as sending or posting inappropriate or derogatory email messages, instant messages, text messages, digital pictures or images, or website postings (including blogs) directed at a student by another student that has the effect of:

    1. Physically, emotionally or mentally harming a student;
    2. Damaging, extorting or taking a student's personal property;
    3. Placing a student in reasonable fear of physical, emotional or mental harm;

4. Placing a student in reasonable fear of damage to or loss of personal property; or

5. Creating an intimidating or hostile environment that substantially interferes with a student's educational opportunities.

- Other conduct deemed objectionable by the Paso Robles Joint Unified ~~Public~~ School~~s~~Distrtict

- Any violations of the classroom rules, school conduct code, Educational Code or Penal Code

Netiquette

Users are expected to always use the Internet, network resources, and online sites in a courteous and respectful manner. Users are also expected to recognize that among the valuable content online is unverified, incorrect, or inappropriate content. Users are expected to use trusted sources when conducting research via the Internet. Users should also remember not to post anything online that they wouldn't want parents, teachers, or future colleges or employers to see. Once something is online, it's out there—and can sometimes be shared and spread in ways never intended.

Security

Users are expected to take reasonable safeguards against the transmission of security threats over the school network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin. Students are expected not to attempt to remove viruses' themselves or download any programs to help remove the virus. The Paso Robles ~~Public~~ Joint Unified School~~s~~'District's computer system is intended for the exclusive use of its registered users who are responsible for their password and their accounts. Any problems that arise from the use of the account are the responsibility of the account holder. Any misuse of the account or system will result in disciplinary action and/or the suspension or cancellation of privileges. Use of the account by someone other than the registered user will be grounds for cancellation and will result in disciplinary action. Any user identified as a security risk for having a history of discipline/appropriate use problems with other computer systems will be denied access to PRJU~~P~~SD Workstations and the Internet by the Paso Robles Joint Unified ~~Public~~ School~~s~~District.

Personal Safety

Users should never share personal information, including phone number, address, social security number, birthday, or financial information, over the Internet without adult

permission. Users are expected to recognize that communicating over the Internet brings anonymity and associated risks, and should carefully safeguard the personal information of themselves and others. Users should never agree to meet someone they meet online in real life without parental permission. If students see a message, comment, image, or anything else online

that effects personal safety, bring it to the attention of an adult immediately.

Plagiarism

Users are expected not plagiarize (or use as their own, without citing the original creator) content, including words or images, from the Internet. Users are expected not to take credit for things they didn't create themselves, or misrepresent themselves as an author or creator of something found online. Research conducted via the Internet should be appropriately cited, giving credit to the original author.

Email

PRJUSD may provide users with email accounts for the purpose of school-related communication. Availability and use may be restricted based on school policies. If users are provided with email accounts, they are expected to be used with care. Users should not send personal information; should not attempt to open files or follow links from unknown or untrusted origin; should use appropriate language; and should only communicate with other people as allowed by the district policy or the teacher. Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Email usage may be monitored and archived.

Social/Web 2.0 / Collaborative Content

Recognizing the benefits collaboration brings to education, PRJUSD may provide users with access to web sites or tools that allow communication, collaboration, sharing, and messaging among users. Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Posts, chats, sharing, and messaging may be monitored. Users should be careful not to share personally-identifying information online.

Cyberbullying

Cyberbullying will not be tolerated. Harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyberstalking are all examples of cyberbullying. Don't be mean. Don't send emails or post comments with the intent of scaring, hurting, or intimidating someone else. Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges. In some cases, cyberbullying can be a crime. Remember that all student network activities are monitored and retained.

Internet Access / Monitoring

It is possible that students) may find material on the Internet that would be considered objectionable. Although student's use of the Internet will be supervised by staff, and Internet firewalls and filters are employed, Paso Robles Public Schools cannot guarantee that students will not gain access to inappropriate material. Staff members of the Paso Robles ~~Public~~ Joint Unified School District will determine what is appropriate use of technology resources. The

District reserves the rights to any materials stored in files which are generally accessible to others and will remove any material that is believed to be unlawful, obscene, pornographic, abusive, or otherwise objectionable. The system may not be used to obtain, view, download, or otherwise gain or provide access to such materials. The District staff will refer for disciplinary action any individual who does not comply with the provisions of this agreement. Cancellation of user privileges will be at the discretion of the staff after application of due process.

Mobile Devices Policy

PRJUSD may provide users with mobile computers or other devices to promote learning outside of the classroom. Users are expected to abide by the same acceptable use policies when using school devices off the school network as on the school network. Users are expected to treat these devices with extreme care and caution; these are expensive devices that the school is entrusting to student care. Users are expected to report any loss, damage, or malfunction to district IT staff immediately. Users may be financially accountable for any damage resulting from negligence or misuse. Use of school-issued mobile devices off the school network may be monitored.

Personal Electronic Devices (PED)

PED Introduction and Definition

This policy relates to any personal electronic device (PED) that could be used for communications or data storage and retrieval. This includes, but is not exclusive of mobile phones, USB drives, MP3 players, PDAs, laptop computers, tablet computers, DVD players, and calculators. PRJUSD embraces emerging digital technologies and encourages its teachers and students to look for ways of using them to enhance teaching and learning. The technology of mobile phones and other electronic devices to facilitate the recording of sound, take photographs and video images is open to abuse that can lead to an invasion of a person's privacy. The availability and appropriate use of these resources provide opportunities that can help students develop spiritually, academically, socially and physically. Their inappropriate use can be detrimental to the teaching / learning process, anti-social, and even harmful. PRJUSD will be providing wireless network access for PEDs to some of our educational and school sites. Network access for PED equipment will only be allowed via wireless Ethernet technology, not via direct Ethernet structured cabling in district facilities.

As sites become online, we'll inform staff and students on wireless connecting procedures. PRJUSD will not be held responsible for the loss, theft or destruction of any personal electronic devices. PRJUSD reserves the right to review files on any mobile device brought into a school. The Computer and Network Information Resources Acceptable Use Agreement for Students also applies to all personally-owned electronic devices. Any violation of these rules will result in the loss of the student's privilege to bring mobile electronic devices to school.

PED Policy for Non-wireless Sites

Students (9-12) are expected to keep PED (including laptops, tablets, smart phones, and cell phones) turned off and put away during (instructional, 9-12) (school, TK-8) ~~school~~ hours~~Â~~

unless in the event of an emergency or as instructed by a teacher or staff for educational purposes, or unless approved by school site policies. Because of security concerns, when PED are used on campus, they should not be used over the school network without express permission from district IT staff.

PED Policy for District Wireless Sites

Students are expected to keep PEDs turned off and put away during classroom instructional hours - unless in the event of an emergency or as instructed by a teacher or staff for educational purposes, or unless approved by school site policies. For PEDs that connect to the school wireless network:

- Students are expected to use PEDs for positive purposes: for learning, and for legitimate communication.
- PEDs must not be used to harass or victimize other students or staff, or to abuse a person's right to privacy (for example, taking, storing and then using a digital photo/video without a person's permission).
- The device is to be running the latest Virus Protection software including the latest weekly virus definition files.
- The device is to be running the latest Security Patches for its Operating Systems.
- The device is to be free of spyware, adware, worms, viruses, trojan horses, and peer-to-peer software that could disrupt the network.
- The device is not to be used for any illegal activity, peer to peer file sharing (including Kazaa, Limewire, Gnutella, Napster, Bit Torrent, etc...), hacking or cracking this network or any other, downloading large files, or viewing (or listening to) streaming media.
- The device is not to be running any Internet or web hosting services and ~~is~~does not have Internet Connection Sharing services turned on.
- School staff who suspect a PED may being used inappropriately or has been used inappropriately may inspect any PED brought onto the school campus by a student.
- During school operation hours, the internet may only be accessed through the school site wireless network, not through any other Internet access
- In using their PEDs students are expected to comply with the Computer and Networked Information Resources Acceptable Use Agreement for Students.

No Warranties

The Paso Robles ~~Public~~Joint Unified School~~s~~ District will not be held responsible for the loss of

data resulting from delays, non-deliveries, or service interruptions sustained or incurred in connection with the use, operation, or inability to use the system. The District specifically denies any responsibility for the accuracy or quality of information obtained electronically. Use of any information obtained electronically is at the risk of the user. While PRJUSD employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness. PRJUSD will not be responsible, financially or otherwise, for unauthorized transactions conducted over the school network.

Encounter of Controversial Material

One of the services available through the District computer system at the school site is telecommunication, including the Internet. The Internet, a community of network systems, is not governed by any entity. The District does not have control over the kind or quality of information that is accessible to Internet users. Although the District does utilize Internet content filtering technologies to provide an academic computing environment, it is the responsibility of the user to utilize networking technologies solely for obtaining academic content.

No Expectation of Privacy

The computer system provided by Paso Robles Joint Unified ~~Public~~ School~~s~~ District is the property of the schools. No person using the system has a right to expect privacy with respect to any material stored on that system, including email and material downloaded from the Internet, and activity while using a district computer. The District reserves the right to monitor and access all such material and activity.

Penalties for Improper Use

Any user violating rules, applicable to state and federal laws, or posted classroom and District rules, is subject to loss of network privileges and other disciplinary actions. In addition, pertaining to State and Federal laws, any unauthorized access, attempted access, or use of any state computing and/or network system is a violation of Section 502 of the California Penal Code or applicable federal laws and is subject to criminal prosecution.

Violations

One of the critical factors that contributes to a business-like learning environment is student conduct. To help assure a positive computing experience, Paso Robles Joint Unified ~~Public~~ School~~s~~ District defines acceptable and unacceptable behavior for student computer use. Students not following the Network Guidelines will be handled on a case-by-case basis, nevertheless the following consequences are in place:

First Offense:

~~Three - Five Day suspension from school, with a disciplinary hearing/conference upon the student's return.~~ Depending on the offense, there is a possibility of 40 hours of community service work. Any non-computer/network security violation will place the student on computer

probation which limits the student to using PR~~PS~~JUSD Computers under direct adult/teacher supervision. Any computer/network security violation will result in the student's computer privileges being removed for one calendar year.

Second Offense:

~~Five Day suspension from school pending an expulsion hearing before the Paso Robles Board of Trustees pursuant to E.C. 48900 (k).~~
Lunch detention assigned. Administrator parent phone call. Device returned to students after school. Parents may contact the Discipline Office if extenuating circumstances exist.

Third Offense:

After school detention assigned. Administrator parent phone call. Device returned to student after 24 hours/next school day or same day parent pick up. Parents may contact the Discipline Office if extenuating circumstances exist.

Fourth Offense:

Saturday school assigned. Administrator parent phone call. Device returned to parent/guardian after 24 hours/next school day with a warning that their child will be suspended for defiance if they commit another violation.

Fifth Offense:

One day suspension from school or other means of correction.

PLEASE RETAIN THIS PAGE FOR YOUR FILES

PASO ROBLES JOINT UNIFIED ~~PUBLIC~~ SCHOOL~~S~~ DISTRICT
COMPUTER and NETWORKED INFORMATION RESOURCES
REQUIRED SIGNATURES

USER: I understand and will abide by the above conditions and rules contained in the Acceptable Use Policy. I further understand that any violation of the above conditions, rules and Acceptable Use Policy is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked and disciplinary action and/or appropriate legal action may be taken.

PARENT OR GUARDIAN: (If you are the parent or guardian of a student under the age of 18, you must also read and sign this agreement.) As the parent or guardian of this student, I have read the Acceptable Use Policy and will instruct my child(ren) regarding any restrictions against accessing materials and will emphasize to my child(ren) the importance of following the Networked Information Policies. I understand that this access is designed for educational purposes. I also recognize that it is impossible for the Paso Robles Public Schools to restrict access to controversial materials, and I will not hold them responsible for materials acquired on

the network. Further, I accept full responsibility for supervision if and when my child's use is not in a school setting. I hereby give permission to issue an account to my child and certify that the information contained on this form is correct.

Please sign and acknowledge acceptance on the student's Emergency Card, located on the back side of the card.

Exhibit__PASO ROBLES ~~PUBLIC~~JOINT UNIFIED SCHOOL~~S~~DISTRICT
~~Revised version: May 8, 2012~~ approved May 26, 2020 Paso Robles, California
~~Initially Board Approved 2-22-00; Approved revisions 6-29-2004, 8-19-2008, 3-8-2011~~