Palo Pinto Independent School District

Student Acceptable Use Policy

Palo Pinto Independent School District (PPISD) makes a variety of communications and information technologies available to students through computers, networks, internet, e-mail, enterprise systems, and other means. These technologies, when properly used, promote educational excellence by facilitating resource sharing, innovation, and communication within the district. Illegal, unethical or inappropriate use of these technologies can have dramatic consequences, harming the district, its students and its employees.

PPISD takes the digital and cyber safety of students seriously and does our best to keep them safe and to make their technology use age appropriate. In accordance with the Children's Internet Protection Act (CIPA), PPISD educates students regarding appropriate online behavior, including interacting with other individuals on social networking websites (including chat rooms). PPISD also educates students on cyber bullying awareness to ensure Internet safety, including use of email and Web 2.0 resources, and has deployed filtering technology and protection measures to restrict access to inappropriate content such as those that are illegal, harmful, or contain potentially offensive information. While every effort is made to provide the most secure and optimal learning environment by monitoring online activities, it is not possible to absolutely prevent access (accidental or otherwise) to inappropriate content. It is possible that you may run across areas of inappropriate content and some material you (or your parents) might find objectionable. While the district will take reasonable steps to restrict access to such material, it is not possible to absolutely prevent such access. If you encounter a web site that you believe should be blocked, please notify a teacher or school administrator.

The district firmly believes that the valuable information and interaction available through the appropriate use of technology far outweighs the possibility that users may procure material that is not consistent with the district's educational goals. In a 21st Century school system, technology, the Internet, and Web 2.0 tools are essential to prepare students for their future.

It is each student's responsibility to read district policy, regulations and agreement forms and ask questions if you need help in understanding and following the guidelines for appropriate and acceptable use.

Access to the network or other technology resources or systems is a privilege—not a right—and it may be revoked by the District at any time.

Mandatory Review -. All district students shall be required to acknowledge receipt and understanding in writing of this acceptable use agreement each year.

Scope of this agreement – This acceptable use agreement applies to any technology provided or managed by the District, including, but not limited to, computer systems, networks, internet, phones, servers, files, data, enterprise systems, mobile technologies, online resources, cloud storage, and software.

Subject to Monitoring - All district technology system usage shall not be considered confidential and is subject to monitoring by designated staff at any time to ensure appropriate use. System users should not use the computer system to send, receive or store any

information, including e-mail messages, that they consider personal or confidential and wish to keep private. All electronic files, including e-mail messages, transmitted through or stored in the computer system will be treated no differently than any other electronic file. The district reserves the right to access, review, copy, modify, delete or disclose such files for any purpose. Users should treat the computer system like a shared or common file system with the expectation that electronic files, sent, received or stored anywhere in the computer system will be available for review by any authorized representative of the district for any purpose.

Inappropriate Use

Inappropriate use includes, but is not limited to, those uses that violate the law, that are specifically named as violations in this document, that violate the rules of network etiquette, or that hamper the integrity or security of any components that are connected to the district's electronic communication systems. Electronically posting messages or accessing materials that are abusive, obscene, sexually oriented, threatening, harassing, illegal, cyberbullying, or damaging to another's reputation are prohibited.

The following actions are also considered inappropriate uses and are prohibited:

- Violations of law including improper use of copyrighted materials, plagiarism, or other protected materials.
- Cheating, altering records, or otherwise accessing information or systems that the student has not been given access to.
- Tampering with or theft of components from district systems may be regarded as criminal activity under applicable state and federal laws.
- Modifying or changing computer settings and/or internal or external configurations without appropriate permission is prohibited.
- Use of the system for any type of income-generating activity is prohibited. Advertising the sale of products, whether commercial or personal is prohibited.
- Use of the system for promoting activities or events for individuals or organizations not directly affiliated with or sanctioned by the district is prohibited.
- Vandalism, abuse of school owned equipment, deliberate attempts to degrade or disrupt equipment or systems.
- Attempts to circumvent District security measures or to compromise security.
- Sharing usernames and passwords with others; and/or borrowing someone else's username, password, or account access.
- Purposefully opening, viewing, using or deleting files or other electronic resources belonging to another system user without permission.
- Other actions commonly viewed as inappropriate technology use or illegal.
- Wireless hotspots, including those created on a cell phone, are prohibited on PPISD property unless they are specifically issued by the district.

Cyberbullying

Cyberbulling is strictly prohibited and will be subject to strong disciplinary action in accordance with the student handbook. Cyberbullying is defined as the use of any Internet-connected device for the purpose of bullying, harassing, or intimidating another student. This includes, but may not be limited to:

- Sending abusive text messages to cell phones, computers, or Internet-connected game consoles.
- Posting abusive comments on someone's blog or social networking site (e.g., Twitter or Facebook).

- Creating a social networking site or web page that masquerades as the victim's personal site and using it to embarrass him or her.
- Making it appear that the victim is posting malicious comments about friends to isolate him or her from friends.
- Posting the victim's personally identifiable information on a site to put them at greater risk of contact by predators.
- Sending abusive comments while playing interactive games.
- Recording and distributing media with the intent to manipulate or embarrass others.

Improper Care of District Equipment – Students will treat district owned computers and other equipment with respect, including taking reasonable precautions or care to prevent damage. Any abuse or intentional breaking of district technology equipment will be handled as a disciplinary situation in accordance with the student handbook. Students will also be held financially responsible for repairs or replacement due to physical abuse or intentional damage to technology equipment.

Reporting Security Problems - If knowledge of inappropriate material or a security problem on the District's technology systems is identified; the user should immediately notify the district's Technology Department. The security problem should not be shared with others.

Students under 13

The Children's Online Privacy Protection Act (COPPA) is a federal law that regulates the online collection of personal information from children under the age of 13. The law generally requires website operators to provide parental notification and obtain parental consent before collecting personal information from these students. However, COPPA also authorizes school districts to provide this consent when the collection of information is for the use and benefit of the school and for no other commercial purpose. Parents can obtain more information regarding COPPA via the Federal Trade Commission website at www.ftc.gov.

PPISD recommends and/or manages certain web-based applications that have been vetted for appropriateness, compliance with federal privacy laws (FERPA), and educational value to enhance the learning experience of students. In compliance with COPPA, PPISD manages student accounts and logons for these resources. Managing these accounts may require the disclosure of certain basic information about students such as name and school name. These may include tools such as Google G Suite for Education, Canvas, iStation, or others.

Disclaimer

The District's technology systems are provided on an "as is, as available" basis. The District does not make any warranties, whether express or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The District does not warrant that the functions or services performed by, or that the information or software contained on the system will meet the system user's requirements, or that the system will be uninterrupted or error free, or that defects will be corrected.

PPISD shall not be liable for a student's inappropriate use of the district's technology infrastructure or violations of copyright restrictions or other laws, a student's mistakes or negligence, and for any costs incurred by a student through the use of technology systems.

Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third-party individuals in the system are those of the providers and not the District.

The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's electronic communications system.

Elastic Clause

The school and administration reserve the right to establish fair and reasonable rules and regulations for circumstances that may arise requiring actions that are not covered under these guidelines. In all cases, rules, regulations, and possible consequences shall be as consistent as possible with previously established rules, regulations, and consequences for similar incidents.

Matters omitted from these guidelines should not be interpreted as a limitation to the scope of the District's responsibility and, therefore, the District's authority in dealing with any type of infraction that may not be in the best interest of the safety and welfare of the students or staff.

Consequences for violations

If a violation of the Acceptable Use Policy occurs, students will be subject to one or more of the following actions:

1. Revocation of access;
2. Disciplinary action in accordance with the *Student Handbook*;
3. Financial responsibility for damages;
4. Appropriate legal action.