PALERMO UNION SCHOOL DISTRICT
TECHNOLOGY ACCEPTABLE USE POLICY FOR STUDENTS

PURPOSE

This policy provides the procedures, rules, guidelines and codes of conduct for the use of the technology and information networks at Palermo Union School District (PUSD). Use of such technology is a necessary, innate element of the PUSD educational mission, but technology is provided to staff and students as a privilege, not a right. PUSD seeks to protect, encourage and enhance the legitimate uses of technology by placing fair limitations on such use and sanctions for those who abuse the privilege. The reduction of computer abuse provides adequate resources for users with legitimate needs.

SUMMARY

Public technology that includes but is not limited to computers, wireless & LAN access, electronic mail, Internet access, Telephone/Voice Mail systems, printing devices and all other forms of instructional, networking and communication tools are provided as a service by PUSD to students. Use of these technologies is a privilege, not a right. Students are expected to observe the following:

- All users are required to be good technology citizens by refraining from activities that annoy others, disrupt the educational experiences of their peers, or can be considered as illegal, immoral and/or unprofessional conduct

The student is ultimately responsible for his/her actions in accessing technology at PUSD. Failure to comply with the guidelines of technology use may result in the loss of access privileges and/or appropriate disciplinary action. Severe violations may result in civil or criminal action under the California Statutes or Federal Law.

GUIDELINES

1. Access to computers, computer systems, information networks, and to the information technology environment within the PUSD system is a privilege and must be treated as such by all students.

2. The PUSD system will be used solely for the purpose of research, education, and school-related business and operations.

3. Any system which requires password access or for which PUSD requires an account, such as the Internet, shall only be used by the authorized user. Account owners are ultimately responsible for all activity under their account and shall abide by this Policy.

4. The District's technological resources are limited. All users must respect the shared use of PUSD resources. The District reserves the right to limit use of such resources if there are insufficient funds, accounts, storage, memory, or for other reasons deemed necessary by the system operators, or if an individual user is determined to be acting in an irresponsible or unlawful manner.

5. All communications and information accessible and accessed via the PUSD system is and shall remain the property of the District.

6. Student use shall be supervised and monitored by system operators and authorized staff. Student use must be related to the school curriculum.

7. Any defects or knowledge of suspected abuse in PUSD systems, networks, security, hardware or software shall be reported to the system operators.

UNACCEPTABLE USE

The Palermo Union School District (PUSD) has the right to take disciplinary action, remove computer and networking privileges, or take legal action or report to proper authorities, any activity characterized as unethical, unacceptable, or unlawful. Unacceptable use activities constitute, but are not limited to, any activity through which any user:

1. Violates such matters as institutional or third party copyright, license agreements or other contracts. The unauthorized use of and/or copying of software is illegal.

2. Interferes with or disrupts other network users, services, or equipment. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of computer viruses or worms, distributing quantities of information that overwhelm the system (chain letters, network games, etc.) and/or using the network to make unauthorized entry into any other resource accessible via the network.

3. Attempts to disable, bypass or otherwise circumvent the PUSD content filter that has been installed in accordance with the federal Children's Internet Protection Act. This includes but is not limited to the use of proxy servers.

4. Seeks to gain or gains unauthorized access to information resources, obtains copies of, or modifies files or other data, or gains and communicates passwords belonging to other users.

5. Uses or knowingly allows another to use any computer, computer network, computer system, program, or software to devise or execute a scheme to defraud or to obtain money, property, services, or other things of value by false pretenses, promises, or representations.

6. Destroys, alters, dismantles, disfigures, prevents rightful access to, or otherwise interferes with the integrity of computer-based information resources, whether on stand-alone or networked computers.

7. Invades the privacy of individuals or entities.

8. Uses the network for commercial or political activity or personal or private gain.

9. Installs unauthorized software or material for use on District computers. This includes, but is not limited to, downloading music, pictures, images, games, and videos from either the Internet or via portable drives.

10. Uses the network to access inappropriate materials.

11. Uses the District system to compromise its integrity (hacking software) or accesses, modifies, obtains copies of or alters restricted or confidential records or files.

12. Submits, publishes, or displays any defamatory, inaccurate, racially offensive, abusive, obscene, profane, sexually oriented, or threatening materials or messages either public or private.

13. Uses the District systems for illegal, harassing, vandalizing, inappropriate, or obscene purposes, or in support of such activities is prohibited. Illegal activities are defined as a violation of local, state, and/or federal laws. Cyber-bullying and harassment are slurs, comments, jokes, innuendos, unwelcome comments, cartoons, pranks, and/or other verbal conduct relating to an individual which: has the purpose or effect of unreasonably interfering with an individual's work or school performance;(b) interferes with school operations; (c) has the purpose or effect to cause undue emotional stress or fear in an individual.

14. Vandalism is defined as any attempt to harm or destroy the operating system, application software, or data. Inappropriate use shall be defined as a violation of the purpose and goal of the network. Obscene activities shall be defined as a violation of generally accepted social standards in the community for use of a publicly owned and operated communication device.

15. Violates the District Acceptable Use Policy.

SCHOOL DISTRICT'S RIGHTS AND RESPONSIBILITIES

1. Monitor all activity on the District's system.

2. Determine whether specific uses of the network are consistent with this Acceptable Use Policy.

1. Remove a user's access to the network at any time it is determined that the user is engaged in unauthorized activity or violating this Acceptable Use Policy.

3. Respect the privacy of individual user electronic data. The District will secure the consent of users before accessing their data, unless required to do so by law or policies of PUSD.

4. Take prudent steps to develop, implement, and maintain security procedures to ensure the integrity of individual and PUSD files. However, information on any computer system cannot be guaranteed to be inaccessible by other users.

5. Attempt to provide error-free and dependable access to technology resources associated with the District system. However, the district cannot be held liable for any information that may be lost, damaged, or unavailable due to technical or other difficulties.

6. Ensure that all student users complete and sign an agreement to abide by the District's acceptable use policy and administrative regulation. All such agreements will be maintained on file in the school office.

VIOLATIONS/CONSEQUENCES

Students who violate this Policy will be subject to revocation of PUSD system access up to and including permanent loss of privileges, and discipline up to and including expulsion.

Violations of law will be reported to law enforcement officials.

Disciplinary action may be appealed by parents and/or students in accordance with existing PUSD procedures for suspension or revocation of student privileges.

<u>UNACCEPTABLE USE</u> OF THE DISTRICT'S COMPUTER SYSTEMS INCLUDE, BUT ARE NOT LIMITED TO, THE FOLLOWING:

1. **Altering any computer configuration including screensavers, desktop settings, network settings, passwords, etc.**
2. **Installing or downloading any executable files from the Internet or portable drives.**
3. **Using chat rooms or social web sites except for teacher-directed educational purposes.**
4. **Installing or using instant messenger programs.**
5. **Downloading MP3s or other music files.**
6. **Accessing online radio stations and television programs.**
7. **Writing, downloading, or printing files or messages that contain inappropriate language.**
8. **Accessing or transmitting pornographic or other inappropriate material.**
9. **Violating the rights to privacy of students and employees of the District.**
10. **Reposting personal communications without the author's prior consent.**
11. **Copying commercial software in violation of copyright law.**
12. **Attempting to hack, crack, or otherwise degrade or breach the security of the District'snetwork, other networks, or individual computers.**
13. **Attempting to bypass the district's content filter, including the use of proxy servers.**
14. **Developing or passing on programs that damage a computer system or network, such as viruses.**
15. **Plagiarism.**
16. **Modifying or copying files of other users without their consent.**
17. **Giving out personal information such as address and phone numbers over the Internet without staff permission.**
18. **Accessing or transmitting material which promotes violence or advocates the destruction of property including information concerning the manufacture of destructive devices (explosives, bombs, fireworks, incendiary devices, etc.).**
19. **Accessing or transmitting material which advocates or promotes violence or hatred against particular individuals or groups of individuals.**
20. **Accessing or transmitting material which advocates or promotes the use, purchase, or sale of illegal drugs.**
21. **Conducting or participating in any illegal activity.**
22. **Any act that is determined as Cyber-bullying, harassment, or a violation of good DigitalCitizenship.**
23. **Any inappropriate use as determined by the Superintendent, Director of Technology and/or building administrators.**