Palo Verde Unified School District
COMPUTER USE POLICY
"POLICY FOR RESPONSIBLE COMPUTING"

SECTION 1. PREAMBLE

With the advent of powerful hardware and software, the Internet and the World Wide Web, computers have become a major communication tool. For example, we now use computers to send E-mail, explore the Web, gather information and offer Distance Learning. While this new computer use can stimulate intellectual, social and cultural growth, it can also facilitate harassment and other irresponsible, destructive behavior. The decentralization power and flexibility a networked computer communication system affords may create situations that are not clearly covered by existing laws or current Palo Verde Unified School District policies, making it mandatory that Palo Verde Unified School District develop and enforce new policies and standards for the responsible use of computers on the campus. These policies defining and governing acceptable and unacceptable use will apply to anyone who uses any computer system, network system, Internet or Intranet web site or other data processing equipment owned by Palo Verde Unified School District as well as remote computer systems when used to access Palo Verde Unified School District computer systems.

As a condition of using the School District's computer resources, all users must sign the written "Acceptable Use Agreement" referred to in this policy. Use of the School District's computer resources in violation of this Policy is prohibited, and can result in revocation of a user's access to the School District's computer resources, student or employee disciplinary action, and a referral for prosecution to other entities for violation of federal, state and/or local laws and regulations.

SECTION 2. DEFINITION OF TERMS

Administrative Officer:	Employee of Palo Verde Unified School District with supervisory responsibility over a unit of the School District which operates Information Resources.
Computer Account:	The combination of a user number, user name, or user ID and a password that allows an individual access to a mainframe computer or some other shared computer or network.
Computer Resources:	The sum total of all computers, workstations, mainframes, software, cabling, peripherals, networks, accounts, passwords, ID numbers, and data owned or leased by Palo Verde Unified School District.
Data Owner:	The individual or department that can authorize access to information, data, or software and that is responsible for the integrity and accuracy of that information, data, or software. The data owner can be the author of the information, data, or software or can be the individual or department that has negotiated a license for the School District's use of the information, data, or software.

on your desk, you may be acting, in whole or in part, as that computer's system administrator.

User: Someone who does not have system administrator responsibilities for a computer system or network but who makes use of that computer system or network. A user is still responsible for his or her use of the computer and for learning proper data management strategies.

SECTION 3. POLICY COVERAGE

Section 3.1 Access

Palo Verde Unified School District is committed to providing access to computing resources to all members of its community: current students, faculty and staff. While providing students and staff limited access to School District computer resources is consistent with the education and service missions of the School District, such access to this valuable and vulnerable school resource is a revocable privilege. Palo Verde Unified School District is responsible for securing its network and computing systems to a reasonable degree against failure, loss of data, and unauthorized access while making them accessible to the largest possible group of authorized and legitimate users and uses.

Section 3.2 Privileges

3.2.1 Computers and networks provide access to resources as well as the ability to communicate with others worldwide. Access to the School District's computer resources is a revocable privilege, which requires that users act responsibly and in a manner consistent with the provisions of this Policy.

3.2.2 Users do not own accounts on Palo Verde Unified School District computers, but rather are granted the use of such accounts. The School District owns the account and grants individuals the privilege of using it.

3.2.3 All enrolled students, faculty, and other School District employees may apply for user ID's to utilize E-mail and Internet and Intranet services offered by the School District. Such an application may be granted only if the applicant signs the Acceptable Use Agreement referred to herein. Users who have had their privileges revoked or suspended may not apply for a user ID during the term of such revocation or suspension.

Section 3.3 Responsibilities

As a condition of the privilege of using the School District's computer resources, each user will be held accountable for his or her own actions which affect such resources. No person shall be permitted access to the School District's computer resources unless and until that person has signed the "Acceptable Use Agreement" provided for in this Policy. By signing that Agreement, each user acknowledges and agrees to abide by the terms of this Policy. A user who violates the terms of this Policy shall be held responsible for his or her actions, and will be subject to discipline for such

Technology"). Users are required to abide by all applicable copyright and trademark laws, and to abide by all licensing agreements and restrictions. Users shall not copy, transfer, or utilize any software or electronic materials in violation of such copyright, trademark, and/or licensing agreements. The copying of software that has not been placed in the public domain and distributed as "freeware" is expressly prohibited by this Policy. Users who access, copy, transfer and/or use "shareware" are expected to abide by the requirements of the shareware licensing agreement. No user may inspect, change, alter, copy, or distribute proprietary data, programs, files, disks, or software without proper authority.

3.3.5 Users should remember that information distributed on Palo Verde Unified School District computers and networks use School resources and this reflects upon Palo Verde Unified School District and not just an individual. Even with appropriate disclaimers, the School District is represented by its students, faculty and staff, and so appropriate decorum is warranted.

The principles of academic freedom apply in full to electronic communication. The conventions of courtesy and etiquette, which govern vocal and written communications, shall extend to electronic communications as well. Fraudulent, harassing, threatening, or obscene messages (as those terms are defined in Section 3.4.2.1.1 of this Policy) and/or other material must not be transmitted through the School District's computer resources.

3.3.6 Expected Privacy

The School District's computer resources and all users' accounts are the property of the School District. There is no right to privacy in the use of the computer resources or users' accounts, and the School District reserves the right to monitor and access information on the system and in users' accounts for the purpose of determining whether a violation of this Policy has occurred. The School District will remove any information on the system, which it determines to be in violation of this Policy.

Users must understand the weak privacy afforded by electronic data storage and electronic mail in general, and apply appropriate security to protect private and confidential information from unintended disclosure. Electronic data, including E-mail, which is transmitted over the School District's computer resources and/or the Internet is more analogous to an open postcard than to a letter in a sealed envelope. Under such conditions, the transfer of information, which is intended to be confidential, should not be sent through the School District's computer resources.

In addition, users should be aware that the School District may access information contained on its computer resources under numerous circumstances, including, but not limited to, the following circumstances:

3.4.1.1 Users agree to represent themselves according to their true and accurate identities in all electronic messages, files and transactions at all times.

3.4.1.2 While using School computing facilities and systems, users agree to behave within the standards described in the School's Code of Conduct, especially those standards describing academic honesty and campus safety. Those standards regarding plagiarism or collusion on assignments apply to course work completed with computers just as they do to other types of course work.

3.4.2 Respecting Rights of Others

3.4.2.1 Students, faculty, staff and administrators.

3.4.2.1.1 Legal and ethical limitations on the use of School District computer resources.

In using the School District's computer resources, users must communicate in the same manner as is expected in the classroom or on campus. The distance provided by electronic communications does not create a forum in which there are no ethical or legal limitations. Users shall not use School District computer resources in any unlawful manner including, but not limited to, attempting to defraud another, threatening physical harm to another, procuring or distributing obscene material in any form, or unlawfully harassing another.

While the School District recognizes and respects users' rights to freedom of speech, such rights are not absolute. Speech, which is fraudulent, libelous, obscene, harassing, or threatening, is not permitted under state or federal law. Users are expressly prohibited from using the School District's computer resources to engage in such conduct. Users violating this section will be subject to revocation of their user accounts, and will be further subject to student/staff disciplinary action, and, in appropriate circumstances, a referral for prosecution for the violation of criminal laws.

For purposes of this Policy, the terms fraud and libel are given their legal meaning as developed by the courts of this State and the United States. "Obscenity" means words, images or sounds which a reasonable person, applying contemporary community standards, when considering the contents as a whole, would conclude that they appeal to prurient sexual/physical interests or violently subordinating behavior rather than an intellectual or communicative purpose, and materials that, taken as a whole regarding their content and their particular usage or application, lack any redeeming literary, scientific, political, artistic or social value. "Threatening" means communications, which result in

4.1.1.2 Authorized access to lab and campus networks to perform and complete required course work for Palo Verde Unified School District course in which the user is currently enrolled.

4.1.1.3 User access to authorized Palo Verde Unified School District student E-mail accounts.

4.1.1.4 Independent study and research.

4.1.1.5 Users agree to follow acceptable use policies established by individual computing labs and network systems and to obey directives issued by authorized School District personnel supervising such labs and systems.

4.1.2 Instructional use (faculty)

4.1.2.1 Use in classroom instruction.

4.1.2.2 Development of instructional materials.

4.1.2.3 Research connected to academic and instructional concerns and interests.

4.1.2.4 Communication with colleagues and professional organizations and institutions.

4.1.3 Administrative use (administrators, classified staff, departments)

4.1.3.1 School District administrative and business communications and transactions.

4.1.3.2 Communications with colleagues and professional organizations and institutions.

4.1.3.3 Research tied to School concerns and interests.

Section 4.2 Inappropriate Use

Use of School District's computer resources for purposes other than those identified in Section 4.1 is not permitted. Users are specifically prohibited from using the School District's computer resources in any manner identified in this section, as discussed in the following subsections.

In addition, users should be aware of the provisions of Penal Code section 313.1, which requires criminal sanctions for any person who, with knowledge that a person is a minor, or who fails to exercise reasonable care in ascertaining the true age of a minor, knowingly sells, rents, distributes, sends, causes to be sent, exhibits, or offers to distribute or exhibit by any means any **harmful matter** to the minor. Any action in violation of Section 313.1 shall be referred to the appropriate police agency for prosecution.

4.2.8.1 Impersonation of any person or communication under a false or unauthorized name.

4.2.8.2 Transmission of any unsolicited advertising, promotional materials or other forms of solicitation.

4.2.8.3 Using School District resources for commercial purposes or personal financial gain.

4.2.8.4 Sending or storing messages and/or materials with the intent to defraud, harass, defame, or threaten.

4.2.8.5 Inappropriate mass mailing "spamming" or "mail bombing."

4.2.8.6 Tampering with any software protections or restrictions placed on computer applications or files.

4.2.8.7 Knowingly or carelessly introducing any invasive or destructive programs (i.e., viruses, worms, Trojan Horses) into School District computers or networks.

4.2.8.8 Attempting to circumvent local or network system security measures.

4.2.8.9 Altering or attempting to alter system software or hardware configurations on either network systems or local computing devices.

4.2.8.10 Installing unauthorized software programs on School local computing devises or network systems and/or using such programs.

4.2.8.11 Ignoring or disobeying policies and procedures established for specific computer labs or network systems.

4.2.8.12 Copying system files, utilities and applications that expressly belong to the School.

SECTION 5. INAPPROPRIATE USES OF SCHOOL DISTRICT COMPUTER RESOURCES: REPORTING AND CONSEQUENCES

Section 5.1 Reporting Violations

Authorized computer system supervisors may informally resolve unintentional or isolated minor violations of use policies through E-mail or face-to-face discussion and education with the user or users concerned.

5.1.1 Student Violations

activities or the computer files of an individual, they have the obligation to pursue any or all of the following steps to protect the user community:

- Take action to protect the system(s), user jobs, and user files from damage. Palo Verde Unified School District reserves the right to immediately suspend a user's privilege of access to District's computer resources if District has any reason to believe that the user has committed a violation of this Policy.

- Notify the alleged abuser's supervisor, project director, instructor, academic advisor, or administrative officer, as appropriate, of the investigation.

- Refer the matter for processing through the appropriate School District disciplinary process if the user's actions are deemed to be in violation of standards of conduct for students or employees, respectively.

- Suspend or restrict the alleged abuser's computing privileges during the investigation and administrative processing.

- Inspect the alleged abuser's files, diskettes, magnetic media, optical media, and/or tapes.

- Minor infractions of this Policy or those that appear accidental in nature are typically handled internally by the System Administrator in an informal manner by electronic mail or in-person discussions. More serious infractions are handled via the procedures outlined above.

- Infractions such as harassment, or repeated minor infractions as described in this Policy may result in the temporary or permanent loss of access privileges, notification of a student's academic advisor and/or site administrator, or the appropriate supervisor or administrator in the case of a faculty or a staff member.

- More serious infractions, such as unauthorized use, attempts to steal passwords or data, unauthorized use or copying of licensed software, violations of the School District's policies, or repeated violations of minor infractions may result in the temporary or permanent loss of access privileges, and referral for discipline under applicable existing School District student or employee disciplinary processes.

- Offenses which are in violation of local, state, or federal laws will result in the immediate loss of computing privileges, student or employee discipline, and will be reported to the appropriate law enforcement authorities.

Abuse of computing privileges is subject to disciplinary action as well as loss of computing privileges. An abuser of the School District's computing resources may also be liable for civil or criminal prosecution. It should be