SECTION 4.127.1 Employee Internet Safety and Responsible Use

Communications and computer technology at Poway Unified are provided and maintained for instructional, educational, and administrative purposes. This administrative procedure implements Board Policy 4.127 Employee Use of Technology, and governs the use of all District technology by employees and other authorized users during the performance of their duties.

Personal Responsibility

District technology equipment and resources are provided for instructional or administrative use. The need for occasional personal use is recognized. It is understood that such use shall not interfere with an employee's duties and responsibilities. Staff shall use the District technology in a responsible, ethical, and legal manner.

The use of District technology for a commercial business such as buying or selling products or promoting services for personal gain and/or profit is prohibited.

District electronic resources cannot be used to communicate, advertise, or solicit for non-district sponsored events or political/religious activities. It is not the intent of this provision to limit otherwise legal communication by bargaining units or employee organizations.

The District maintains a public-access Internet site and an Intranet site. All materials published on these sites must follow the same board policies that apply to printed material (Administrative Procedure 6.70.7).

Acceptable Use

Communication and Internet Access

It is a general policy that computer or network resources are to be used in a responsible, ethical, and legal manner in support of education, business, and goals of the District.

Each user is responsible for adherence to this policy at all times when using electronic information services. Violation of this policy and/or misuse of network resources may result in disciplinary action which may include, but not be limited to, loss of privileges.

Web sites accessible via the Internet may contain material that is illegal, defamatory, inaccurate, or potentially offensive to some people. The District provides filtering and blocking barriers to identified Internet sites, resources, and content. Should an employee see any unacceptable materials, he/she is encouraged to notify the Information Technology Department.

Proper Use and Care of Equipment

Many users, especially at school sites, will be sharing systems as part-time users. In this scenario, subsequent users will suffer if systems are improperly configured or damaged by previous users. In some cases, special software is used to protect essential system

configurations, requiring each user to log-on individually and enabling only the services for which the user is authorized.

Users are responsible for damage to or loss of District equipment per board guidelines (Administrative Procedure 6.84.1). District vandalism policies apply, making users liable for intentionally inflicted damage. Employees who are personally assigned portable technology devices such as laptops, cellular phones, electronic tablet devices, etc., shall return those devices to the District upon demand.

Applications on Local Machines

Users are not authorized to attempt repairs or installation of software on District equipment. All installation or repairs should be requested in the District work order system. Prior to installing or modifying applications on a desktop machine, users shall seek approval from and work with the site Local Area Network (LAN) or the IT Department. Any unauthorized changes to systems, operating software, application software, or hardware configurations will be uninstalled when discovered by technology or instructional staff.

Applications and Devices on Network Servers

The District Information Technology Department is responsible for acquisition and installation of applications and ensuring the proper configuration and safeguarding network security and performance by authorizing the use of all peripheral devices, including but not limited to, desktop/laptop computers, printers, network equipment, wireless access points, web cameras, or other types of hardware to the District's network or telephone systems. Any equipment found to be in violation of this policy will be immediately disconnected.

The District takes no responsibility for lost, damaged, or stolen personal devices. Upon employee request, the District may provide the use of District-owned applications installed by District IT personnel on personal devices. The District takes no responsibility for personal device performance if the District-owned application is installed on a personal device. The employee agrees to bring in their personal device upon the request of the District, or upon separation from the District, to remove the District-owned and provided application for redistribution.

All the rules and regulations stated in the District Technology Use Agreement are applicable to wireless connectivity, as well as all network connections.

Data Security and Confidentiality

Employees and other authorized users will keep all student information confidential. Printing, posting, sharing, and/or displaying of student information in a public area, even without the student name, violates Federal confidentiality laws. Employees and authorized users will keep employee information confidential as required by law.

Security and Passwords

Security on any computer system is a high priority. A breach of security compromises the integrity of our student records, curriculum, attendance accounting, business records, confidential student and employee data, and communications. To maintain security, users are issued unique passwords to enable their access. All users are informed and understand that the District maintains the right, with cause, to access at any time, without advance notice or consent, all applications and files on the District-provided computer and electronic systems without use of the individual user ID and password.

Users should always:

- **Maintain confidentiality of their password, never giving it out**
- **Access the system under their own account**
- **Adhere to the established security rights and privileges assigned to their account or equipment**
- **Logout of a computer prior to allowing use by another person**

Expected Privacy

The District's computer resources and all user accounts are the property of the District. There is no right to privacy in the use of the computer resources or user accounts, and the District reserves the right to monitor and access information on the system and in user accounts for purposes of determining whether a violation of state or federal law, Board policy, or District Administrative Procedures has occurred. The District will remove any information on the system which it determines to be in violation of state or federal law, Board policy, or District Administrative Procedures.

Electronic data, including email which is transmitted over the District's computer resources and/or through the Internet, is not confidential. The transfer of information which is intended to be confidential should not be sent through the District's computer resources.

Employee Acknowledgement

All employees of Poway Unified and authorized users who have access to District technology will be required to acknowledge that they have received, read, and accepted the guidelines of this administrative procedure during their first login of a new school year.