

**EMPLOYEE ACCEPTABLE USE POLICY**

USE OF TECHNOLOGY

Communications and computer technology at SDUHSD are provided and maintained for instructional, educational and administrative purposes only. This Administrative Regulation implements Board Policy 4112.7/4212.7, Employee Acceptable Use Policy, and governs the use of these technologies by employees during the performance of their functions.

A. ACCESS TO TECHNOLOGY EQUIPMENT AND SERVICES

Access to technology is provided to facilitate the instructional and administrative tasks performed by District employees. The level of access provided will coincide with the requirements of each employee's job functions.

Computer files and communications stored or sent over electronic networks, including e-mail, voice mail and Internet access, are not private, and may be monitored and viewed by the District at any time without prior notice. This technology should not be used to divulge confidential information about students, employees, or District business to unauthorized persons.

To ensure proper use, the Superintendent or designee may monitor the District's technological resources, including e-mail, voice mail systems and Internet usage, at any time without advance notice or consent.

B. ACCEPTABLE USE

It is a general policy that computer or network resources are to be used in a responsible, efficient, ethical, and legal manner in support of education, business and/or research and within the educational program and goals of the District. The use of electronic information resources is a privilege, not a right. Each user is personally responsible for this provision at all times when using electronic information services.

The Superintendent, principal, or their designees may set more restrictive guidelines for employees in their area of responsibility.

While electronic information resources offer tremendous opportunities of educational value, they also offer persons with illegal or unethical purposes avenues for reaching students,

EMPLOYEE ACCEPTABLE USE POLICY

teachers, and others, including parents. SDUHSD does not have control of the information on commercial electronic information services or the information on the Internet, although it attempts to provide prudent and available barriers. Sites accessible via the Internet may contain material that is illegal, defamatory, inaccurate or potentially offensive to some people.

Should an employee see any unacceptable materials or inappropriate use, he/she shall notify the site administrator or supervisor immediately, report any instances where the Acceptable Use Policy or security may be violated and report inappropriate Internet web sites to the Information Technology Department so that access to the sites can be blocked in the future.

If there is any doubt as to the appropriate use of a District-provided electronic system, the employee should review the use in advance with a supervisor and/or a member of the Information Technology Department.

C. PROPER USE AND CARE

Before operating any equipment, users will be made familiar with the basics of safety and damage prevention, and trained on proper care and operation. Users will be individually assessed to determine their technical capabilities, and will be properly trained and supported by the Information Technology Department, as systems are issued for their use.

Many users, especially at school sites, will be sharing systems as part-time users. In this scenario, subsequent users will suffer if systems are mis-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.

Equipment abuses are unacceptable whether out of frustration, misuse, negligence or carelessness. Users are responsible for damage to or loss of District equipment. District vandalism policies apply, making users liable for intentionally inflicted damage.

**EMPLOYEE ACCEPTABLE USE POLICY**

Users should not attempt repairs without authorization or support from designated District or school site personnel. Volunteers - students, parents, family members, or friends - are not authorized to attempt repairs on District equipment.

Guidelines for the care and use of computer software are similar to hardware policies. Users are responsible for damage to or loss of District software systems. District vandalism policies apply to software as well, making users liable for intentionally inflicted damage. Employees who are personally-assigned portable technology devices such as laptops, cellular phones, personal digital assistants, etc., shall return those devices to the District upon demand and shall be liable for any costs to repair or replace equipment that is lost or damaged beyond reasonable wear and tear.

Users shall not install or modify applications without approval and support of the Director of Educational Technology. Any unauthorized changes to systems, operating software, application software, or hardware configurations will be uninstalled when discovered by technology or instructional staff. Peer-to-Peer file-sharing software cannot be installed or used on district computers for the purpose of illegally sharing copyrighted materials such as music, images and software.

Users shall not download or install software without proper approval of the Director of Educational Technology. Non-licensed or unapproved software will be deleted.

In order to ensure proper configuration and to safeguard network security and performance, users should not attach computers, printers, network equipment (including wireless access points), web cameras, or other types of hardware to the District's network or telephone systems without prior approval and support of the Director of Educational Technology. Any equipment found to be in violation of this policy will be immediately disconnected.

**D. PERSONAL RESPONSIBILITY**

All technology equipment is District property and is provided for instructional or administrative use only. Personal use is limited in the same manner as other similar District property - telephones, copiers, postage, office supplies and instructional

EMPLOYEE ACCEPTABLE USE POLICY

materials. Supervisors will provide guidance as to the appropriate level of personal use.

The same guidelines that currently apply to magazines, books, videos, or other materials apply equally to Internet use. Board policies on sexual harassment, civility, and commercial activity apply to all technology or electronic activities.

The conduct of personal business, including buying and selling products or promoting services, using District resources is not allowed. In addition, District electronic resources cannot be used to conduct political or religious activities. District e-mail cannot be used to advertise or solicit for non-district sponsored events.

The District maintains a public Internet site and an in-house Intranet site. All materials published on these sites must follow the same Board Policies and Education Code Sections that apply to printed material. These policies include restrictions on the content, nature, purpose, and volume of information to be published. Intranet pages are provided for District employees only. Any information to be posted on the public Web site or in-house Intranet site must meet the District's Web Guidelines and Publishing Standards. Restrictions apply to links to other sites that may not be appropriate and to personal information or pictures of students without parental consent. Specific Web site guidelines are established and available through the Information Technology Department.

Do not store personal files or applications on District media.

E. SECURITY AND PASSWORDS

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

1. Do not use another user's passwords.
2. Do not write down a password where others can see it.

EMPLOYEE ACCEPTABLE USE POLICY

3. Change passwords regularly.
4. Never demonstrate a security problem to other users.
5. Never use another individual's account. All use of the system must be under your own account.
6. Users shall not bypass filters or firewalls, use proxy servers, gain access to sites or networks without authorization, or otherwise attempt to defeat network security protocols.
7. Users may not physically attach personally-owned devices to an SDUHSD network.
8. Users may not load any software or executable programs on any SDUHSD computer/network.

To maintain the integrity of the student information system (grades, attendance, curriculum), do not permit any student to use your staff computer or your staff User ID at any time. Any user identified as a security risk will be denied access to the information system.

F. PENALTIES FOR VIOLATIONS

Violation of the Acceptable Use Policy may result in a reduction or loss of access privileges. In many cases, access privileges may be essential to job functions. Additionally, those failing to follow the guidelines contained in this regulation may face disciplinary action in accordance with collective bargaining agreements, Personnel Commission Rules and Regulations for the Classified Service, state law, and Board policy.

G. EMPLOYEE ACKNOWLEDGEMENT

All employees of SDUHSD who have access to District technology will be required to annually acknowledge that they have received this administrative regulation, read it and accepted the guidelines.

**EMPLOYEE**

**ACCEPTABLE USE CONTRACT**

I have received, read and accept the guidelines in the Employee Acceptable Use Policy.

\_\_\_\_\_  
Print Name

\_\_\_\_\_  
Dept./Site

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date