

**TECHNOLOGY ACCEPTABLE USE**

The district's Governing Board believes the use of technology (computers, document cameras, PDA's, email services, software applications, the Internet and data network, mobile devices, and other electronic communication support devices) supports learning; enhances instruction; and improves overall district business and personnel efficiency and communication.

The effective performance of the district technology resources (including computer equipment, data network, email services and Internet access) relies upon users adhering to established standards of proper conduct and use.

This Technology Acceptable Use Policy defines the responsibilities of district staff while using the district computer equipment, including mobile devices, and/or connecting to the district data network, email and voice mail systems, and Internet access. In general, this policy requires the appropriate, efficient, ethical, safe, and legal utilization of the district technology resources. The district declares unethical, unsafe, and unacceptable behavior as just cause for taking disciplinary action, revoking information network access privileges, and/or initiating legal action.

**Acceptable Use**

The district technology provides a powerful resource which allows staff to communicate both locally and globally; to access data and to share information. This resource demands that those entrusted with the privilege of its use be accountable. Therefore, use of the district technology equipment and services must be in direct support of district assigned duties and responsibilities of the user.

By using the district's technology hardware, software, network services (Internet, email, and voice mail) and web services district staff assumes personal responsibility for their appropriate use and agrees to comply with this policy and all applicable district policies.

In order to use district technology, employees must sign the E 4040 Title Staff Member Consent and Waiver for Internet/District Network Access and Use of District Technology Equipment" form.

Technology platforms are changing rapidly in the 21<sup>st</sup> century. Therefore, the district has the right to authorize consistent use of electronic platforms as needed to support the optimum educational and operational use of technology for instruction and/or staff support. Currently, the district's main platform includes: PC workstations, laptops/tablets, cellular and Smart phones, and thin clients. Purchase of different electronic platforms, or supplements, can be authorized by the district when a consideration for the following is included in the decision:

- Cost effectiveness,
- Ability for personnel to technically support platform use,
- Equipment can be integrated within the current facility infrastructure, and
- Its use will provide the most effective support and applicability for student learning.

## **TECHNOLOGY ACCEPTABLE USE (continued)**

### **Technology Functions**

The district network and the Internet are communication and research tools to be used by district staff in accordance with generally accepted business practices.

This policy sets forth guidelines and procedures for the proper use of the district's data network and Internet access.

### **Internet and District Network Access Policy and Procedures**

It is the policy of the district that Internet use over the district's data network shall be limited to appropriate educational or business purposes. All district staff shall comply with this policy and related administrative regulations.

### **Network Resources and Security**

While the Internet connection offers an abundance of benefits, it can also open the district's network infrastructure and data system to significant risks.

1. The internet is one of the most popular means for the transmission and spread of computer viruses. Beware of viruses: a file that is downloaded must be scanned for viruses before it is run or accessed. Caution must be used when copying files coming from unknown sources. Staff must not open or copy files from sources they do not know or trust.
2. The district's network is a shared resource. Unnecessary or unauthorized internet usage causes network congestion, resulting in slower responses from other networked resources like shared applications, data, and printers. Communication-intensive operations such as large file transfers, mass emailing and the like should be scheduled for off-peak times, and/or coordinated through appropriate administrative channels or through the Technology Department.
3. Caution should be used with downloaded browser extensions and interactive web programs. They may accidentally or purposefully damage a district system, or access and connect with private data without the user's knowledge. These sources also utilize additional bandwidth and cause network congestion.

### **Prohibited Use of District Data Network and Internet Access**

Prohibited use of the district data network and Internet access includes and is not limited to, the following:

**TECHNOLOGY ACCEPTABLE USE** (continued)

1. Personal activities that incur additional costs to the district or interfere with staffs work performance;
2. Profit-making activities that accrue to the employee;
3. Unlawful activities, including sending and receiving copyrighted materials in violation of copyright laws or licensing agreements;
4. Creating, viewing or communicating sexually explicit or offensive material or messages, cartoons, jokes, ethnic slurs or racial epithets, and any statement or images that might be construed as harassment, disparagement or libel of any person;
5. Religious, political, charitable, social or personal purposes and activities;
6. Obtaining or accessing files or communication for unlawful purposes;
7. Using the information network for illegal, inappropriate, or obscene purposes, or in support of such activities. Illegal activities shall be defined as those which violate local, state, and/or foreign laws. Inappropriate use shall be defined as a violation of the intended use of the network, and/or purpose and goal. Obscene activities shall be defined as a violation of generally accepted social standards for use of a publicly-owned and operated communication vehicle;
8. Stealing data, equipment, or intellectual property;
9. Gaining unauthorized access to the files of others, or vandalizing the data or files of another user;
10. Forging electronic mail messages, or uses an account owned by another user;
11. Invading the privacy of individuals (both inter- and intra-district);
12. Posting anonymous messages;
13. Downloading entertainment software or games that are not used for instructional or training purposes, including participation in Internet gaming;
14. Actions that degrade or disrupt the performance of the district's data network;
15. Actions that intentionally compromise the security of the district's technology systems.

## **TECHNOLOGY ACCEPTABLE USE (continued)**

### Use of Cellular Phones or Mobile Communications Devices

An employee shall not use a cellular phone or other mobile communications device in violation of law, Board policy, or administrative regulation, and such violation shall be subject to discipline and may be referred to law enforcement officials as appropriate.

### Privacy and Disclosure

The district staff using the district Internet access, ~~and~~ data network, and district issued technology devices shall not expect or assume that they are provided any degree of privacy.

The district reserves the right to monitor all traffic on the network and restrict access, if necessary, to assure that the network continues to function properly for all users.

The district reserves the right to automatically prohibit, remove, constrain, or disable problematic applications and plug-ins from desktops and also place access restrictions on specific websites or devices.

The district reserves the right to intervene and access web sites of the user at any time if and when a user is suspected of one of the above named violations. The district reserves the right to intervene and access email, voice mail, as well as other Internet communication information if there is suspicion of a violation of district policy.

### **Consequences of Violation**

Internet usage and access through the district data network is a privilege, not a right. The district reserves the right to restrict, suspend or terminate this privilege without prior notice. Consequences of violations include but are not limited to:

- Suspension of information network access;
- Revocation of information network access;
- Suspension of network privileges;
- Revocation of network privileges;
- Suspension of computer access;
- Revocation of computer access or use of district provided technology device;
- Legal action and prosecution by the authorities;

Anyone accused of any of the violations has all the rights that would normally apply if such person were accused of any illegal activity.

The district has the right to restrict or terminate information network access at any time for any reason. The district further has the right to monitor network activity in any form that it sees fit to maintain the integrity of the information network.

**TECHNOLOGY ACCEPTABLE USE (continued)**

**Copyright Act 1976**

According to the Copyright Act of 1976, Fair Use” means that a person may freely use any information they legally find on the Internet as long as they do so only for scholarly purposes. According to this law, no one may plagiarize or sell what is found on the Internet.

*Legal Reference:*

EDUCATION CODE

51870-51874 Education technology

52270-52272 Education technology and professional development grants

52295.10-52295.55 Implementation of Enhancing Education Through Technology grant program

GOVERNMENT CODE

3543.1 Rights of employee organizations

PENAL CODE

502 Computer crimes, remedies

632 Eavesdropping on or recording confidential communications

VEHICLE CODE

23123 Wireless telephones in vehicles

23123.5 Mobile communication devices; text messaging while driving

23125 Wireless telephones in school buses

UNITED STATES CODE, TITLE 20

6751-6777 Enhancing Education Through Technology Act, Title II, Part D, especially:

6777 Internet safety

UNITED STATES CODE, TITLE 47

254 Universal service discounts (E-rate)

CODE OF FEDERAL REGULATIONS, TITLE 47

54.520 Internet safety policy and technology protection measures, E-rate discounts

*Management Resources:*

WEB SITES

CSBA: <http://www.csba.org>

American Library Association: <http://www.ala.org>

California Department of Education: <http://www.cde.ca.gov>

Federal Communications Commission: <http://www.fcc.gov>

U.S. Department of Education: <http://www.ed.gov>

Policy  
adopted: March 4, 1997  
amended: June 19, 2007  
reviewed: May 5, 2009  
amended: March 6, 2012

**SANTEE SCHOOL DISTRICT**  
Santee, California