**All Personnel**

## TECHNOLOGY ACCEPTABLE USE

### Technology Hardware and Software

The district provides staff with technology resources for administrative use and for enhancing educational experiences. Technology resources include networking equipment, desktop/notebook computer, desktop telephone, mobile phone, personal digital assistants (PDA), projectors, document cameras, and other instructional technology equipment.

This administrative regulation contains the following sections:

1. Technology Hardware and Software
2. Mobile Computer Equipment
3. Email Services
4. Internet Blocking
5. Social Networking Sites

### Technology Hardware and Software Use Guidelines

Technology resources (equipment, software and data) are considered valuable property of the district. All hardware and software acquired for, or on behalf of, the district or developed by district staff or contract personnel is and shall be deemed as district property.

All district staff authorized to use district technology resources shall adhere to the following:

1. Staff shall use the resources in the manner and to the extent that the user is authorized.
2. Staff shall comply with district policies and practices regarding physical security and safety of the resource.
3. Staff shall not use district technology resources in support of or for illegal activities or personal gain.
4. Staff shall not use district technology resources in a manner that violates other district policies.
5. Staff shall not abuse district technology resources including and not limited to any actions that endanger or damage the resources.
6. The district technology resources shall not be used for recreational purposes, unless the purpose is related to a district project, I.E. field trips, professional training, etc.

**Technology Hardware**

In order for Technology and Communication Services (TCS) staff to effectively support and service the district's computer hardware, staff assigned with Technology Hardware (computer, tablet PC, document cameras, projectors, etc.) shall adhere to the following guidelines:

1. Computer equipment shall not be moved, relocated, or taken home without prior consent from the site Principal and TCS Department;

2. System settings shall not be altered on the equipment;

3. Components shall not be removed or added to the equipment without prior approval from the TCS Department;

4. Repairing or servicing the equipment without prior approval from the TCS Department is prohibited (Exceptions include minor repair learned in District authorized training sessions.);

5. Staff shall not install applications/software without prior approval; and

6. Staff shall use the equipment as required in this and other related policies.

No other computer, peripherals or networking equipment may be connected (wire or wireless) into the district network without Technology and Communication Service's (TCS) prior permission.

**Technology Software**

Only software purchased or developed by the district can be installed on the district computer. This is to ensure compliance with software licensing requirements.

Internet downloadable Shareware, Freeware and Demo Versions of software/programs are not to be installed on any district computer without prior approval from the Technology and Communication Services (TCS) Department. Often such software can cause undesirable consequences to the individual computer and to the data network operations in general.

Backup copies of software are allowed and recommended. Backup copies are necessary to protect the software in the event the original fails. However, it is not permitted to use the backup copy software simultaneously on another computer.

Unless the district or school has a "network license," network sharing of applications and software is strictly prohibited. "Network Licenses" enable the software/application to be used simultaneously by multiple computers over the data network.

Software such as port scanner, network penetrations tester, and network mapping/discovery software are considered "hacking tools" and are not permitted on the district network without prior approval from the Technology and Communication Services (TCS) Department. Such

software packages generate network traffic and are deemed a threat to the district data network well being.

The district owned software/applications (purchased or created) are not to be installed on home (personal) computers. If district staff is required or wishes to work from home and such installation is required, prior authorization must be given by the District Administration.

**Copyrights and License Agreement**

The district and its staff are legally bound to comply with all proprietary software licensing agreements. Each staff member is individually responsible for reading, understanding, and following all applicable licenses, notices, contracts and agreements for software that he or she uses on district computers. Duplication of copyrighted software may be a violation of federal and state law. In addition to violation of such laws, unauthorized duplication of software is a violation of this policy

**Mobile Computer Equipment**

District Office and school staffs are allowed to use the district's mobile computer equipment (notebook and tablet PC) inside and outside the schools in order to enhance, enrich and facilitate teaching and administrative duties as well as school communications.

**Mobile Computer Usage and Guidelines**

All notebook, tablet PC, and related equipment and accessories are district property and are provided to staff members for a period of time as deemed appropriate by the school administration.

All staff/teachers that are issued district owned equipment must adhere to the following:

1. Equipment is issued for school related business, curriculum enhancement, research, and communication.

2. District owned notebooks/tablet PC's may be used for limited personal purposes subject to the district's policies.

3. No attempt shall be made to install, download software and/or applications without prior consultation with Technology Communication Services staff.

4. Equipment must be protected from theft and damages.

5. Staff shall be held responsible for any problem caused by their negligence.

6. Staff shall not attempt to repair or service the equipment. All repair/service must be performed by Technology staff.

7. Staff shall not remove, alter, or replace any hardware/components and/or software on the machine.

8. Staff shall not change the system configuration including network settings.

9. Computer equipment must not be loaned to a third party including family members.

10. Staff shall use the equipment in accordance with the district's BP 4040 "Technology Acceptable Use" even when using the machine on a network outside of the school district.

**Avoid Mobile Computer Theft and Damage**

Because of its size and portability, mobile computers are extremely vulnerable to theft and damage. Staff shall exercise care to ensure that mobile computers and other district technology equipment assigned to them are not stolen or damaged.

If staff wishes to take a mobile computer home, staff must complete and file with TCS the "Equipment Loan Form" (Form 64-686) at the beginning of the school year and/or prior to taking equipment from the district and agree to adhere to the following guidelines to protect the mobile computer from being stolen and/or damaged:

1. Do not leave a mobile computer in an unlocked vehicle.

2. Avoid storing the mobile computer in extreme temperature.

3. Do not leave a conference room without your mobile computer.

4. Never check a mobile computer as luggage at the airport.

5. Lock the mobile computer in your office or classroom during off-hours or in a locked cabinet or desk when possible.

6. Do not place drinks or food in close proximity of your mobile equipment.

7. Make sure your hands are free from lotions before using the equipment. (Hand lotion is a major contributing factor to dust and dirt on the keyboard).

8. Use your mobile computer on a flat, solid surface so that there is air circulation. Using your mobile computer on a bed can cause damage due to overheating.

9. Always use a surge protector when you are charging the battery.

10. Remember to put the Tablet PC Digitizer Pen back into the pen slot after use.

If theft or damage occurs, immediately notify the District/School Administration and District Technology Department.

Each staff member is responsible for any hardware and/or software that are assigned to him/her. In the event of damage or loss, staff will be monetarily responsible if the

damage/loss is due to staffs' negligence. If multiple losses or damages occur, the district reserves the right to revoke a staff member's use of the electronic equipment.

**Privacy and Disclosure**

Staff shall not expect or assume any privacy or data protection for personal data stored on the district assigned mobile computer.

District staff must provide access to any equipment and/or accessories that they have been assigned upon request by the district office.

**Email Services**

The district utilizes Microsoft Exchange for its electronic mail services. Although email is an effective communication tool, it also presents a significant opportunity for abuse, loss of staff productivity, and potential liability for the district and the district staff.

**Permissible Uses of Electronic Mail**

1. Authorized Users — District staff and other persons who have received permission under the appropriate authority are "Authorized Users" of the District email system and resources

2. Purpose of Use — Use of the District email system and resources must be related to district business, including academic pursuits. Incidental and occasional personal use of the system may occur when such use does not generate a direct cost for the School District.

**Email Use Guidelines**

Email communication should be for district related business, performance of work related duties, and for professional training and education

Inappropriate use of the district email system includes, but is not limited to, the following activities:

1. Creating, viewing, or communicating offensive material or messages,

2. Creating and communicating hoax messages and electronic chain letters, and

3. Creating, viewing or communicating material or messages that contain cartoons, jokes, ethnic slurs or racial epithets, and/or any statement or images that might be construed as harassment, disparagement, or libel of any person.

**Best Practice or Email Etiquette**

Email is a communication tool. As with all forms of communication, it is appropriate that we follow proper etiquette. Here are some best practices when communicating through email:

1. Avoid “Spamming”. Email should never be mass-mailed to unsuspecting audiences,

2. Tag each email with your name, your email address and your telephone number, and

3. Do not send a message that you would not want published. It is common for an innocent note to be misconstrued, especially if inadequate thoughts are given to how it will be interpreted by an outsider, causing embarrassment or liability to the user and/or the district.

**Record Management**

The district’s email system is not designed for long term storage. It is to be used for the communication of transitory information only. Any information, which is either required or intended to be separately preserved, must be moved by the user to a separate file category that is subject to an approved retention schedule.

**Privacy and Disclosure**

All email messages transmitted over the district’s email system are considered to be property of the district and can be accessed through the district server.

Transmissions over the district email service are not secure and staff using the system shall not assume or expect any privacy for their messages that are sent over the service.

The district reserves the right to:

1. Access and view any messages sent over the district email system.

2. Inspect and disclose the content:

    a. In the course of an investigation (misconduct or misuse),

    b. As needed to protect health and safety of District staff and students, and

    c. As needed to prevent interference with District goals and objectives.

3. Restrict, suspend or terminate email privileges without prior notice.

Although the district will not monitor email transmission as a routine matter, it reserves the right to do so as deemed necessary by the district for the purposes of maintaining the integrity and effectiveness of the system.

**Internet Blocking**

The Internet is an ever expanding resource of information. Large amounts of information are added to the Internet on a daily basis. It is used constantly by the district staff and students as a research tool to enhance learning and educational opportunities.

TECHNOLOGY ACCEPTABLE USE

Because of the vast amount of information on the Internet, there will be content that is inappropriate for students and staff. There will also be materials that are harmful to health, safety and welfare.

The district believes in providing a safe environment for staff and students when they are using the Internet.

This policy is established to limit access to undesirable websites and material. The district will rely on an "Internet filtering device/application" to manage access to the Internet.

**Blocked Web Categories**

Presently, the following web categories are blocked:

| | | |
|---|---|---|
| Adware | Alcohol | Child Pornography |
| Criminal Skills | Cults | Dating/Personals |
| Dubious/Unsavory | Explicit Art | Gambling |
| Hacking | Hate/Discrimination | Malicious CodeNirus |
| Obscene/Tasteless | Peer-to-Peer/File Sharing | Phishing |
| Pornography/Adults | R-Rated | School Cheating |
| Spy ware | Terrorist/Militant | Tobacco |
| Violence/Profanity | Weapons | |

Internet filtering and blocking is not considered a comprehensive method to prevent access to inappropriate material on the Internet. New websites and categories are inserted into the "World Wide Web" daily and it is not feasible to monitor all content on the Internet. There will be instances where an unsuitable site is not covered by the filter.

If a URL (Uniform Resource Locator) that is not appropriate is not being blocked by the filtering device, it is the responsible of the staff to report it to Technology. Technology will take immediate action to add the website (URL) to the blocked categories.

In the event that a website (URL) with educational value is being blocked, staff will notify Technology and the site will be allowed through the filter after it is approved by District Administration.

**SOCIAL NETWORKING SITES**

**Introduction**

"Social Networking Sites" is used to describe community-based web sites, online discussion forums, chat-rooms and other online social spaces. Such sites include blogging, micro-blogging (twitter, plurk), photo-sharing (Flickr, twitpic), video-sharing (YouTube, Vimeo), life-casting (blogtv, qik), and professional and social networking (LinkedIn, Plaxo, Facebook, MySpace).

The absence of, or lack of explicit reference to a specific social website does not limit the extent of the application of this policy.

**Social Networking Guidelines**

The District understands district staff's right to participate in social network sites outside of the district workplace, using personal computers and communication devices, but because participation in social networking sites can be associated with the District, district staff shall adhere to the following:

a. Personal blogs should have clear disclaimers that the view expressed in the blog is the author's and does not represent the views of the School District. Be clear and write in the first person and make your writing clear that you are speaking for yourself and not on behalf of the District.
b. Information and material published on personal blog or social sites/forums should comply with the District's confidentiality and privacy policies. Posting on personal social networking sites should not disclose confidential student information and/or photographs.
c. When posting to personal blog or social sites, be respectful of the district, district employees, students and parents.
d. Employee presence on social sites reflects the district. Employees should be aware of public perception of images, posts, or comments placed on social sites.
e. Social networking account should not be used to harass, threaten, libel, malign, defame, disparage or discriminate against district employees, students and parents.
f. Personal social sites must not provide links to the district's website.
g. Prohibit posting of content that is likely to disrupt school activities.
h. Any violations will be subject to disciplinary actions, up to and including termination. In addition, employee online presence, depending on what is posted, can violate other district policies.

**Privacy and Disclosure**

There is no assumption of privacy when voluntarily posting information to a social networking site.

The District reserves the right to reprimand and discipline staff when social networking sites are used to:

a. Disrupt school activities
b. Disclose confidential information of students, parents and staffs
c. Disrespect the district and its employees, students and parents
d. Make disparaging remarks about students, parents or the district

Regulation
approved: March 4 1997
amended: June 19, 2007
reviewed: May 5, 2009
reviewed: February 8, 2011

**SANTEE SCHOOL DISTRICT**
Santee, California

TECHNOLOGY ACCEPTABLE USE

By signing this agreement, I acknowledge that I have read the District Internet/Network Access and Use of District Technology Equipment Consent and Waiver form, acknowledge District authority and responsibility for electronics and Internet use, and agree to follow the District guidelines and restrictions set forth in BP 4040 and AR 4040.

Employee Name: _____ Site: _____
(Please Print)

Employee Signature: _____ Date: _____