Series 4000 – Personnel **SP/AR 4040**

ALL PERSONNEL

Part 1 – Acceptable Use Policy

I. Responsibilities:

It is the responsibility of all Sutter County Superintendent of Schools (SCSOS) employees who use county provided technology to understand and follow these policies. All school districts or other agencies connecting to the SCSOS office network (SutterNet) must develop their own Acceptable Use Policy (AUP) that meets or exceeds the principles contained in this document.

It is not the intent of the SCSOS to substitute for or replace district acceptable use policies. However, in matters pertaining to the use of SutterNet, SCSOS must meet the requirements set by our Internet provider, the Digital California Project (DCP), administered by the Corporation for Education Network Initiatives in California (CENIC). In matters pertaining to use of the DCP, DCP AUP supersedes local AUPs. This SCSOS AUP meets or exceeds the DCP AUP.

II. Core Concepts:

A. Rights and Responsibilities: Technology can provide access to resources in and outside the county computer system, as well as the ability to communicate with other users worldwide. Such open access is a privilege and requires that individual users act responsibly.

B. All existing laws (federal and state) and SCSOS regulations and policies apply, including not only those laws and regulations that are specific to technology, but also those that may apply generally to personal conduct. Relevant laws include, but are not limited to: Education Code Section 49073 et seq.; the Public Records Act (Gov. Code Section 6250 et seq.); the Information Practices Act of 1977 (Civil Code Section 1798 et seq.); Penal Code Section 502; the Electronic Communications Privacy Act of 1986; and the Privacy Act of 1974; and the Family Educational Rights and Privacy Act of 1974 (20 U.S.C. Section 1232g), as they may be amended from time to time.

C. Users do not own accounts on SCSOS computers, but are granted the privilege of use. Subject to applicable laws, SCSOS staff may access user data in the normal course of their employment when necessary to protect the integrity of SCSOS technology or rights. For example, staff may review and copy data to investigate suspected misuse. User data may be subject to search by law enforcement agencies under court order.

D. Student data maintained or accessed using SCSOS technology may be considered "educational" or "pupil" records, and may be subject to laws governing its protection. Staff will provide training regarding requirements relating to student data, as necessary.

E. Misuse of technology may result in discipline, penalties under applicable laws, and/or the loss of technology. Users may be held accountable for their conduct under any applicable SCSOS policy or collective bargaining agreement. Illegal production or distribution of software and other intellectual property protected by U.S. copyright law is subject to civil damages and criminal punishment including fines and imprisonment.

F. When other organizations access SCSOS resources, users are responsible for obeying both the policies set forth in this AUP and the policies of their own organizations.

G. SCSOS technology users must respect the privacy of other users and the integrity of the technology. For example, users shall not: seek information on, obtain copies of, or modify data or passwords belonging to other users unless explicitly authorized to do so by those users; intentionally develop technology that harasses other users; infiltrate and/or damage technology.

H. The following warning is in effect for all SCSOS technology:

This technology is the property of the Sutter County Superintendent of Schools Office. Any unauthorized access or use of this technology is prohibited and could be subject to criminal and civil penalties. To help protect the technology from unauthorized use and to assist in problem diagnosis and repair, activities on this technology are monitored, recorded, and subject to audit. Use of this technology implies consent to such monitoring and recording.

I. Employees and other users have no expectation of privacy while using SCSOS technology. All data on SCSOS technology is subject to examination without notice. To the extent employees conduct SCSOS business on personal devices, employees are advised that that records maintained on any personal device or messages sent or received on a personal device that is being used to conduct SCSOS business may be subject to disclosure pursuant to a subpoena, a request made pursuant to the California Public Records Act, or other lawful request.

J. Social media:

SCSOS staff are advised to be mindful with social media use, which is often public information and taken out of context. Social media use by SCSOS staff should not interfere with SCSOS duties or technology use. Any Social Media account created by an SCSOS employee for student or parent communication related to SCSOS business should:

- Conform to applicable state and federal data privacy laws
- Follow copyright or intellectual property laws
- Secure the consent of all involved parties for the right to distribute or publish content

K. Unacceptable Uses:

- Any use of SCSOS technology that violates or supports a violation of local, state, and/or federal law is prohibited. This includes, but is not limited to, the following: stalking others; transmitting or originating any unlawful, fraudulent or defamatory communications; distributing copyrighted material beyond the scope of fair use without permission; or any communications where the message or its distribution would encourage a crime.
- Activities that interfere with or disrupt technology or users. Such interference or disruption includes, but is not limited to: distribution of unsolicited advertising or mass mailings; "spamming;" propagation of computer worms or viruses; and using SCSOS technology to make or attempt to make unauthorized entry to other technology.
- Use in furtherance of outside business activities (e.g., consulting for pay, sales or distribution of products or services for personal profit, etc.), unless specifically authorized by SCSOS.
- Use in support of partisan political activities.
- Viewing or distributing pornographic, racist, or otherwise objectionable materials.
- Any other use that is unacceptable or not in keeping with role, mission, or goals of SCSOS.

Part 2 – Specific Policies and Examples for SCSOS Employees

I. Computer Assignment

A. Computers are assigned to positions, not individuals. As a rule, when an individual changes position, their assigned computer will remain in the old

location. A change in work location may or may not necessitate moving their computer equipment. The individual's supervisor will determine, after consultation with the Technology Department, if the computer will be moved with the individual.

B. Under no circumstances will computers or other peripherals connected to the network be moved without the Technology Department's prior approval.

II. Computer Acquisition

A. No computer or computer peripheral will be acquired by any county department unless said equipment meets the minimum specifications contained in the SCSOS Office Technical Specifications for Networks and Computer Systems.

B. All computer and computer peripheral purchases must be reviewed and approved by the department head.

III. General Computer Configuration/Policies

A. Minimum Equipment Levels.

The SCSOS Office Technology Department specifies minimum equipment levels. Any equipment the employee desires in excess of job-related needs will be purchased and supported at the employee's expense.

B. Computer Location/Extension Cable Policy.

When used at locations with an existing local area network (LAN) connection, no computer will be located more than 10 feet from the existing network outlet. Except for temporary circumstances (i.e., in a conference room), no county-owned computer will be connected to a LAN using a network cable that is more than 10 feet long. Network cables longer than 10 feet can cause network reliability problems and are a safety/tripping hazard. In the event a computer must be permanently located more than 10 feet from an existing network outlet, the program responsible will, through the Technology Department, hire a contractor to move the existing outlet or install a new outlet.

C. Wireless LAN/WAN Configuration.

We will only use wireless hardware and software that fully complies with the applicable IEEE specifications. County offices will not run open

wireless systems. Systems used will allow the generation of encryption keys using pass phrases. Pass phrases will be no longer than 16 characters, will not be easily guessed words, and will include a mix of upper and lower case letters, numbers, and special characters/punctuation.

The SCSOS may configure wireless access in conference rooms that allow guest access to outside services such as SMTP, Web, FTP, etc. These services will only be available during normal business hours.

D. General User Responsibilities:

Each user is responsible for the care and maintenance of any computer systems in their care. Users are responsible for:

1. Maintaining any software issued with the computer.
2. Ensuring the virus protection software is functioning.
3. Ensuring that the virus software definitions are current.
4. Ensuring that user data on the computer is backed up.
5. Ensuring that the operating system is kept updated.

E. Support for non-required applications.

Using county computers for personal reasons is not prohibited. However, personal use of a county computer shall not interfere in county business, will be kept to a minimum, and will not be supported at county expense. Example: Asking the Technology Department to trouble shoot non-functioning CD-ROMs when the only use of the CD-ROM is to play personal music CDs.

F. Software Piracy.

Software piracy is not permitted under the law. Employees must ensure that any software they install is legally obtained. Employees will not install software obtained from other users or sources, other than the Technology Department, unless they can document that the software was obtained legally, and has not already been installed on another employee's computer.

NOTE: Each software vendor's licensing policy is different. Some vendors allow you to install their software on multiple computers. An example: Some Microsoft product licenses allow you to install their software on both your office and home computers. The critical point in many of these

licenses is that the software may only be used by the individual employee and can never be in use on two computers at the same time.

In other words, the employee may use the software on their county-owned computer while they are at work and may use the same software on a personally owned computer while at home. The employee would violate the terms of the software license if the employee installed the software on a home computer, and then allowed a family member or friend to use that software. The employee would also be violating the license if he/she used the software at home while another employee used the software on his/her computer in the office at the same time.

The Technology Department will, in certain circumstances, install county-owned software on home computers if the employee understands the limits of the software license and will comply with them. The key to such a situation is that the employee is required by their supervisor to perform county work on a home computer. Under no circumstances will the Technology Department install software on an employee's home computer when that employee has been issued a county-owned laptop, since by definition, the laptop can be taken home and used instead of the employee's personal computer.

Each employee is ultimately responsible for ensuring appropriate licenses exist for all installed software on their computer systems.

G. Using personal software.

Using personal software on county computers is not prohibited. However, if the software is loaded, the employee accepts full responsibility for installing and using that software and any damage that use causes. Should problems occur the employee can be held liable for the costs of correcting those problems. The Technology Department will not, as a rule, install or troubleshoot personal software, and can direct that personal software be removed if that software is, or could be, conflicting with required software or peripherals.

H. Student Accessible Computers.

Programs purchasing computers for student use must ensure the Technology Department is aware that the computer will be used by students. During the configuration of the computer, the Technology Department will create a login for the teacher and a separate login for the students. The teacher's login will have administrative privileges; the student login will have restricted privileges. This will allow the teacher to

keep his/her E-Mail private from the students and will allow the teacher to install software, printers, etc.

Under no circumstances will a student be allowed to access a teacher or other staff member's computer. Under no circumstances will a student access a student computer on a teacher's or other staff member's login.

I. E-Mail:

1. E-Mail communications are subject to the same county policies that apply to written communications.

2. SCSOS provides the E-Mail system for county business. Personal use is permitted so long as that use is appropriate, does not violate any other county policies, and is acceptable to the individual employee's supervisor. The following practices are specifically prohibited:

   (a) Sending or relaying chain letters.

   (b) Using the system to advertise for a private business or non-profit group. Employees will not use private E-Mail addresses to send advertisements or unsolicited material to other county employees at the receiving employee's county E-Mail address.

   (c) Sending unsolicited jokes or similar material.

3. Employees must understand that there is no expectation of privacy when using the county E-Mail system.

4. County employees shall not transmit confidential financial or personal information, data, or documents via E-Mail.

5. Use of the E-Mail system to transmit harassing, threatening, or obscene correspondence is prohibited.

6. Employees may not use other employee's E-Mail name or address.

7. E-Mail communications are subject to monitoring and review.

8. E-Mail accounts that show no activity after 90 days will be closed.

9. E-Mail Archiving: The county will create and follow an E-Mail Archiving Policy. The Technology Department will maintain an

E-Mail archiving system to store all E-Mail transiting the county system. Employees will not retain E- Mail on the MS Exchange system for longer than 6 months. Employees may create archives on their assigned computers to retain E-Mail older than six months.

J. Internet Use:

1. Private use of the Internet or "surfing" shall be kept to a minimum, shall not interfere with assigned duties, and can be prohibited by an individual's supervisor if the situation warrants.

2. All downloaded software shall be scanned with a current virus-scanner software package.

3. All information posted on the SCSOS Website or posted to other Websites as official SCSOS information or policy, must have prior approval of a supervisor or the Technology Department.

K. Passwords:

1. All employees, especially those working in areas accessible by students, will take extreme care to prevent students from learning or otherwise securing usernames and passwords. Employees will not post or hide password reminders on or near their desks or computers. Password/username issue letters will be kept in secure locations not accessible to unauthorized users.

IV. Requesting Technical Support: (Locations other than Klamath Lane)

A. All requests for technical support require a work order. This is an automated system and can be accessed from any Internet connected computer at: https://www.sutter.k12.ca.us/Content/Tech/WorkOrder/WorkStart.aspx

B. As a rule, computers requiring service must be dropped off at the Technology Department with a printed copy of the work order attached. Employees must follow all the instructions on the Work Order entry form.

V. Dropping off Computers at the Technology Department for Service

A. Work Orders are required.

B. Employees will be told when to bring computers to the Technology Department. Do not bring your computer to the Technology Department

until asked to do so as a result of a Work Order submitted at: https://www.sutter.k12.ca.us/Content/Tech/WorkOrder/WorkStart.aspx

C. When dropping off desktop computers, unless instructed otherwise, bring in only the CPU and the software originally issued with the computer. Do not bring in any cables, keyboards, mice, monitors, or other peripherals.

D. When dropping off laptops, bring all the issued software and parts, such as power supplies, floppy drives and CD-ROM drives.

E. Attach a copy of the Work Order to the computer.

F. Many times the only way to resolve software issues is to initialize the hard drive and do a complete "new" installation of the hard drive. The Technology Department does not have the resources to backup and restore employee data. It is the employee's responsibility to ensure their important files, including E-Mail addresses and messages, are backed up prior to dropping the computer off for service.

VI. Computer Equipment/Software Disposal

A. Old or excess equipment will be disposed of per established board policies.

B. Employees disposing of computers will remove the hard drive from the computer and send the drive to the Technology Department. The Technology Department will wipe the drive with a hard drive wiping utility that wipes the drive in accordance with US Department of Defense 5220.22-M Clearing and Sanitization Matrix.

C. In the event the hard drive cannot be wiped per the above standard, the Technology Department will physically destroy the hard drive.

D. Any software donated or transferred to other agencies or persons must be accompanied with all original software disks and license documents. Software purchased under educational software purchasing agreements may only be transferred to other educational entities eligible to purchase the software under that same purchase agreement. All software transfers must comply with all applicable license agreements.

E. Excess software not eligible for transfer per the above requirements will be destroyed.

F. Agencies accepting donated or transferred equipment or software must agree to accept all transfers or donations as is. The SCSOS Office will not support or maintain any donated or transferred equipment or software.

I acknowledge that I have read, understand, and agree to the AUP and may be subject to disciplinary action or limitations in using technology should I violate this AUP. This AUP applies to all SCSOS employees, whether the employee has signed the AUP or not.

Signature: _____

Print Employee Name: _____

Date: _____