

08/20/2007

Part I – Acceptable Use Policy

- I. Responsibilities: It is the responsibility of all Pleasant Grove School employees and students who use county provided internet access and email accounts to understand and follow these policies. Superintendent of Schools Office (SCOE) to substitute for or replace district acceptable use policies. However, in matters pertaining to the use of SutterNet, SCOE must meet the requirements set by our Internet provider, the Digital California Project (DCP). In matters pertaining to use of the DCP, DCP AUP supersedes local AUPs. This AUP meets or exceeds the DCP AUP.
- II. Core concepts:
 - A. Rights and Responsibilities: Computers and networks 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 SCOE regulations and policies apply, including not only those laws and regulations that are specific to computers and networks, but also those that may apply generally to personal conduct.
 - C. Users do not own accounts on SCOE computers, but are granted the privilege of exclusive use. Under the Electronic Communications Privacy Act of 1986 (Title 18 U.S.C. section 2510 et. seq.), users are entitled to privacy regarding information contained on these accounts. This act, however, allows system administrators or other SCOE employees to access user files in the normal course of their employment when necessary to protect the integrity of computer systems or the rights or property of the SCOE. For example, system administrators may examine or make copies of files that are suspected of misuse or that have been corrupted or damaged. User files may be subject to search by law enforcement agencies under court order if such files contain information which may be used as evidence in a court of law. In addition, student files on SCOE computer facilities are considered "educational records" under the Family Educational Rights and Privacy Act of 1974 (Title 20 U.S.C. section 1232[g]).
 - D. Misuse of computing, networking or information resources may result in the loss of computing and/or network access. Additionally, misuse can be prosecuted under applicable statutes. Users may be held accountable for their conduct under any applicable SCOE procedure, or collective bargaining agreement. Illegal production of software and other intellectual property protected by U.S. copyright law is subject to civil damages and criminal punishment including fines and imprisonment.
 - E. Other organizations operating computing and network facilities that are reachable via the SCOE network may have their own policies governing the use of those resources. When accessing remote resources from SCOE, users are responsible for obeying both the policies set forth in this document and the policies of the other organizations.

F. Users of county owned and operated information systems must respect the privacy of other users and the integrity of those systems; for example, users shall not seek information on, obtain copies of, or modify files, other data or passwords belonging to other users unless explicitly authorized to do so by those users. Nor shall they intentionally develop programs that harass other users. Nor shall they infiltrate a computer or information system and/or damage or maliciously alter the software components of a computer or information system

G. School users must comply with copyright laws and license agreements.

H. Pleasant Grove School is maintained under the Sutter County Schools internet access system. Sutter County Schools obtains its Internet connection from the Digital California Project, which is administered by the Corporation for Education Network Initiatives in California (CENIC), and is subject to CENIC's Acceptable Use Policies. The DCP and Sutter County Network are for authorized users only. As a rule, CENIC and Sutter County Schools do not routinely inspect, monitor or disclose content. However, anyone using the network consents to monitoring and is advised that, if the monitoring process reveals evidence of criminal activity, CENIC and Sutter County Schools might provide the content and transmission details to law enforcement and national defense agencies as appropriate. In the course of network maintenance or performance monitoring, the activities of individuals using the network may be monitored. Individuals found to be using the network in excess of their authority or contrary to this AUP are subject to having all of their activities on the network monitored and recorded to ensure subsequent compliance with policies and procedures.

I. Employees and other users have no expectation of privacy while using county computer systems or accounts. All information on county owned computer systems is subject to examination without notice.

J. Unacceptable Uses:

- Any illegal use in support of illegal activities is prohibited. Illegal use shall be defined as use that violates local, state and/or federal law. This includes, but is not limited to, the following: Stalking others, transmitting or originating any unlawful, fraudulent or defamatory communications, transmitting copyrighted material beyond the scope of fair use without permission of the copyright owner, or any communications where the message or its transmission or distribution, would constitute or would encourage conduct that is a criminal offense.
- Activities that interfere with or disrupt network users, services, or equipment. 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 county systems or the DCP to make or attempt to make unauthorized entry to other computational, informational or communications devices or resources. For the purpose of this AUP, "unsolicited advertising" includes any transmission that describes goods, products, or services that is initiated by a vendor, provider, retailer, or manufacturer of the described

goods, products, or services, or by a third party retained by, affiliated with, or related to the vendor, providers, retailers, or manufacturer.

- Use in furtherance of profit-making activities (consulting for pay, sales or distribution of commercial products or services for profit, etc.) or use by for-profit companies, unless specifically authorized by the Sutter County Schools and DCP Program Steering Committee and CENIC Board of Directors.
- Use in support of partisan political activities
- Use for private or personal activities that exceed Sutter County Schools or DCP related research, instruction, or administrative applications, or when there is personal monetary gain.
- Visiting pornographic, racist or otherwise objectionable Web sites.
- Any other use that is unacceptable or not in keeping with role, mission or goals of this organization as determined by the leadership of the Pleasant Grove School District.

Part II – Specific Policies and Examples for 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 Coordinator, 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 Coordinator's prior approval.

III. General Computer Configuration/Policies

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. Only wireless hardware and software that fully complies with the applicable IEEE specifications. The wireless standard currently used by this organization is 802.11b. 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.

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

- a. Maintaining any software issued with the computer.
- b. Ensuring the virus protection software is functioning.
- c. Ensuring that the virus software definitions are current.
- d. Ensuring that user data on the computer is backed up.
- e. Ensuring that the operating system is kept updated.

- F. Software Piracy.** Software piracy is not permitted under the law. Users must ensure that any software they install is legally obtained. Users 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 user's computer. **NOTE:** Each software vendor's licensing policy is different. Some vendors allow you to install their software on multiple machines. An Example: Some Microsoft product licenses allow you to install their software on both your office and home machine. The critical point in these types of licenses is that the software may only be used by the individual employee, and the software can never be in use on two machines 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 she installed the software on her home machine, and then allowed her husband or kids to use that software. She would also be violating the license if she used the software at home, while another employee used the software on her machine in the office at the same time. The Technology Department will, in certain circumstances, install some county owned software on home machines, if the user understands the limits of the software license, and will comply with them. The key to such a situation is that the user is **required** by their supervisor to perform county work on a home machine. Under no circumstances will the Technology Department install software on a user's home computer when that user 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 user is ultimate 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 user accepts full responsibility for installing and using that software and any damage that use causes. Should problems occur the user can be held liable for the costs of correcting those problems. The Technology Coordinator 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 computer 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 their 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 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. The Sutter County Schools Office 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 receive 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. School 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.

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. Software shall not be downloaded from the Internet unless all copyright provisions are adhered to.
3. Software downloaded from the Internet shall not be installed on school computers without the Technology Coordinator's approval. This includes media players, screen savers, and wall paper.
4. All downloaded software shall be scanned with a current virus-scanner software package.
5. Pornographic material shall not be viewed, downloaded or E-Mailed.

K. Passwords:

1. Users are responsible for securing their passwords. Users 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. All users, especially those working in areas accessible by students, will take extreme care to prevent students from learning usernames and passwords.

VI. Computer Equipment/Software Disposal:

- A. Old or excess equipment will be disposed of per established board policies.
- B. The hard drives of computers being disposed of will be wiped 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 can not be wiped per the above standard, the hard drive will be removed from the computer and physically destroyed.
- 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. Pleasant Grove School will not support or maintain any donated or transferred equipment or software.

I have read and will comply with this acceptable use policy.

Print Employee Name: _____

Signature: _____

Date: _____