KERN COUNTY SUPERINTENDENT OF SCHOOLS OFFICE

PERSONNEL

EMPLOYEE ACCEPTABLE USE POLICY FOR COMPUTERS, ELECTRONIC DEVICES, NETWORK AND OTHER ELECTRONIC INFORMATION RESOURCES

The Kern County Superintendent of Schools Office recognizes that electronic information resources can enhance productivity, facilitate professional communication, and assist in providing quality educational programs. This policy applies to and describes the responsibilities and obligations of all employees using the office's electronic information resources, including computers, electronic devices, and network.

DESCRIPTION OF ELECTRONIC INFORMATION RESOURCES

Electronic information resources covered by this policy include office computers, electronic devices, and network.

1. Definition of Office Computers

   The term "office computer" means any computer, including a laptop computer that is owned, leased, or rented by the office, purchased with funds from a grant approved by or awarded to this office, or borrowed by this office from another agency, company or entity, whether or not the computer is equipped with a modem or communication peripheral capable of digital connection.

2. Definition of Electronic Devices

   The term "electronic devices" means any device other than a computer that is capable of transmitting, receiving, or storing digital media and is owned, leased, or rented by the office, purchased with funds from a grant approved by or awarded to the office, or borrowed by the office from another agency, company or entity, whether or not the electronic device is portable and whether or not the electronic device is equipped with a modem or other communication peripheral capable of digital connection. Office electronic devices include, but are not limited to the following:

   - telephones
   - cellular telephones
   - radios
   - pagers
   - voice mail
   - e-mail
   - text messages
   - digital cameras

- personal digital assistants such as Blackberries, Palm Pilots and smart phones
- portable storage devices such as thumb drives and zip drives
- portable media devices such as IPODs and MP3 players
- optical storage media such as compact discs (CDs) and digital versatile discs (DVDs)
- printers and copiers
- fax machines
- portable texting devices

3. Definition of Electronic Network

The term "electronic network" means the local area office-wide and Internet systems, including software and e-mail and voice mail systems, remote sites, and VPN connections.

OWNERSHIP

The office electronic information resources, including laptop computers and portable electronic devices are office property provided to meet office needs. They do not belong to employees.

All office computers and electronic devices, including laptop computers and portable electronic devices, are to be registered to the office and not to an employee. All software on office computers and electronic devices, including office laptop computers and portable electronic devices, is to be registered to the office and not to an employee except as provided in Section 6.

No employee shall remove an office computer or electronic device from the Kern County Superintendent of Schools Office's property without the prior, express authorization of the employee's supervisor and the designated technology administrator at the employee's site.

The use of office electronic information resources is a privilege which the office may revoke or restrict at any time without prior notice to the employee.

NO EMPLOYEE PRIVACY

Employees have no privacy whatsoever in their personal or work-related use of the office computers, electronic devices, network and other electronic information resources or to any communications or other information in the office electronic information resources or that may pass through office electronic information resources. The office retains the right, with or without cause, and with or without notice to the employee to remotely monitor, physically inspect or examine the office computers, electronic devices, network or other electronic information resources and any communication or information stored on or passing through the office electronic information resources, including, but not

limited to software, data and image files, internet use, e-mails, text messages, and voice mail.

When an employee leaves the employment of the Kern County Superintendent of Schools Office, management shall be given access to, and the authority to dispose of, any and all of his or her computer files, e-mail, voice mail, text messages, and any other electronically stored information.

PERSONAL USE

Employees shall use the office computers, electronic devices, network and other electronic information resources primarily for purposes related to their employment. Office laptop computers and portable electronic devices shall be used solely by authorized employees and not by family members or other unauthorized persons.

Where approved by the employee's supervisor in advance, an employee may make minimal personal use of office electronic information resources as long as such use does not violate this policy, does not result in any additional fee or charge to the office, and does not interfere with the normal business practices of the office or the performance of an employee's duties. As described in Section 3, employees have no privacy whatsoever in their personal use of the office computers, electronic devices and network, including but not limited to software, data and image files, internet use, text messages, and e-mails.

PASSWORD PROTECTION

To protect against unauthorized use, all office computers and electronic devices, including laptop computers, that are capable of being password protected, shall be password protected, even if a computer or electronic device is assigned to a single employee for his or her sole use. If password protection is not technologically feasible, the employee to whom the computer or electronic device is assigned shall be responsible for physically protecting it against unauthorized use. Any screen saver which is capable of being password protected shall be password protected.

Each employee shall be responsible for registering his or her password(s) with the appropriate administrator, whether the password protection is at the system level or program level. The office needs the ability to access its own equipment.

SOFTWARE AND ELECTRONIC DEVICES

Software, computers, and electronic devices must meet specific standards to protect the office's network and other electronic information resources. In addition, violations of software copyright law have the potential of costing the office millions of dollars.

Only the designated technology chief technology officer/administrator shall be allowed to authorize installation or maintenance of either hardware or software on office computers and electronic devices.

Unless directed to or authorized by the employee's supervisor and the designated technology administrator at each site, no employee shall install, maintain, or remove software on office computers and electronic devices. Unless directed to or authorized by the employee's supervisor and the designated technology administrator, no employee shall connect an electronic device to office computers, whether hardwired or wireless.

The chief technology office/administrator is authorized to approve employee requests for the installation of non-office software, subject to the following limitations:

1. Software not related to the mission of the office shall not be installed.

2. No software shall be installed without written proof of licensing, which shall be retained by the technology administrator. Multiple installations of the same license number will be assumed to violate copyright unless a multiple license provision can be demonstrated.

3. The employee shall surrender to the office all rights whatsoever he or she may have in the software, including, but not limited to the following:

    - The office has the right to remove the software at any time and for any reason without prior notice to the employee.

    - The office has no obligation to return the software to the employee.

    - If the employee is assigned to a different computer or electronic device, the office has no obligation to install the software on that equipment.

    Employees who have been authorized to download and install software shall run a virus detection program on all files and programs downloaded and shall adhere to copyrights, trademarks, licenses, and contractual agreements applicable to the software, including provisions prohibiting the duplication of material without proper authorization and the inclusion of copyright notices in any use of the material.

FILTERS AND OTHER INTERNET PROTECTION MEASURES

To ensure that the use of the office's network is consistent with the office's mission, the office uses content and/or bandwidth software to prevent access to pornographic and other websites that are inconsistent with the mission and values of the office. No employee shall bypass or evade, or attempt to bypass or evade, the office's filter system.

OTHER UNACCEPTABLE USES

In addition to other provisions of this policy, employees using office computers, electronic devices or network shall be responsible for using them only in compliance with the following requirements, unless the chief technology officer/administrator gives prior express written permission.

1. An employee shall use only his or her assigned account or password to access office computers, electronic devices, and network. No employee shall permit the use of his or her assigned account or password, or use another person's assigned account or password without the prior express written consent of the employee's supervisor and the designated technology administrator at the employee's work site.

2. Employees are prohibited from using office computers, electronic devices, network and other electronic resources for knowingly transmitting, receiving, or storing any oral or written communication that is obscene, threatening or disruptive, or that reasonably could be construed as harassment or disparagement of others based on their race, religious creed, color, national origin, ancestry, physical disability, mental disability, medical condition, marital status, sex, age, or sexual orientation. This prohibition applies to written and oral communication of any kind, including music.

3. Employees are prohibited from using office computers, electronic devices and network for knowingly transmitting, receiving, or storing any image file that depicts actual or simulated torture, bondage, or physical abuse of any human being or other creature, or that is sexually explicit.

    a. "Sexually explicit" means a visual depiction of actual or simulated human sex acts, or the unclothed human genitalia, pubic area, anus, buttocks, or female breast that lacks serious artistic, literary, scientific, or political value.

    b. This prohibition applies to visual depictions of any kind, including screensavers, drawings, cartoons and animations.

4. Employees shall not knowingly store or transmit copyrighted material on office computers, electronic devices, or network without the permission of the holder of the copyright. Employees shall download copyrighted material only in accordance with applicable copyright laws.

5. Employees are prohibited from knowingly using the office's computers, electronic devices, and network to intentionally access information intended to be private or restricted; change data created or owned by another user or any other agency, company or network; make any unauthorized changes to the appearance or operational characteristics of the office's system; load, upload, download or

create a computer virus; alter the file of any other user or entity; or remove, change or add a password, alter system settings, preloaded software settings, firmware and hardware without the approval of the designated technology administrator at the employee's site.

6. Employees are prohibited from remotely accessing any office computer or server without prior express written approval of the chief technology officer/administrator.

7. Employees are prohibited from uploading to a non-office server any file contained on an office computer or server, whether the file is work related or personal, unless the employee has been granted the prior express written approval of the chief technology officer/administrator.

8. Any text transmission can only be used by authorized office blog messaging system and or device.

9. Employees also are prohibited from using office computers, electronic devices, and network for the following:

    - personal financial gain
    - commercial advertising
    - political activity as defined in Education Code Sections 7050-7058
    - religious advocacy
    - promoting charitable organizations
    - communicating in someone else's name
    - attempting to breach network security
    - creating, sending or receiving materials that are inconsistent with the mission and values of the office
    - mass distribution of e-mail to a school site without the prior approval of the site administrator
    - mass distribution of e-mail to the office without the approval of the chief technology officer, superintendent, or designee
    - accessing pornographic or other websites that are inconsistent with the mission and values of the office

- any activity prohibited by law, board policy, or administrative regulations, or the rules of conduct described in the Education Code

VIOLATION OF THIS POLICY

Management personnel shall promptly report violations of this policy to the chief technology officer and the appropriate associate/assistant superintendent.

Employees who violate this policy are subject to discipline, up to and including termination, pursuant to the provisions of applicable laws governing employee discipline, and applicable office policies, procedures, and collective bargaining agreements. The employee's use of office electronic information resources also may be restricted, suspended, or revoked.

Legal Reference:
EDUCATION CODE
7050-7058 Political Activities of School Officers and Employees