KERN COUNTY SUPERINTENDENT OF SCHOOLS

PERSONNEL

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

The office recognizes that electronic information resources can enhance productivity, facilitate professional communication, and assist in providing quality educational programs. This policyapplies to and describes the responsibilities and obligations of all employees using the office'selectronic information resources, including computers, electronic devices, and network, and portions of this policy also apply to an employee's personal computer and electronic devices under certain circumstances.

DEFINITIONS

1. The term "electronic information resources" ("EIR") includes office computers,electronic devices, and the office's electronic network and software.

2. The term "office electronic record" means any writing containing information relating to conduct of the office's business where the writing was prepared, owned, used, or retainedin electronic/digital format by the office, regardless of where or how the record may havebeen prepared or where the record is retained. Records containing no more than incidental references to the office are not considered office electronic records. For this purpose, "writing" means anything in an electronic/digital format including sounds, images, symbols, words, or any combination thereof, specifically including electronic mail (email) and all other forms of electronic files.

3. The term "computer" means any computer, including a laptop or notebook, whether or not the computer is equipped with a modem or communication peripheral capable of digital connection.

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

5. The term "electronic device" means any device, other than a computer, capable of transmitting, receiving, or storing digital media, whether or not the electronic device isportable and whether or not it is equipped with a modem or other communication peripheral capable of digital connection. Electronic devices include but are not limited to the following:

    - Telephones
    - Cellphones, including "smartphones"
    - Radios
    - Pagers
    - Digital cameras

- Personal digital assistants, including but not limited to Blackberries, Palm Pilots,and "smartphones"
- Portable storage devices, including but not limited to thumb drives and zip drives
- Portable media devices, including but not limited to iPods, iPads, other tablets(e.g., Nook, Kindle, etc.), and MP3 players
- Optical storage media such as compact discs (CDs) and digital versatile discs (DVDs)
- Printers and copiers
- Fax machines
- Portable texting devices

6. The term "office electronic device" means any electronic device owned, leased, or rentedby the office, purchased with funds from a grant approved by or awarded to the office, or borrowed by or loaned to the office from another agency.

7. The term "office electronic network" means the office's local area office-wide networkand internet systems, whether hardwired or wireless, including software, email and voicemail systems, remote sites, and/or VPN connections.

8. The terms "personal computer" and "personal electronic device" mean computers and/ordevices as defined in this policy that are not office computers or electronic devices, typically computers and/or devices owned by individuals including employees and visitors. Personal cell or smartphones, iPads, and similar devices are personal electronicdevices, whether or not supported by an office stipend paid to the employee.

OWNERSHIP

Office EIR is office property provided to meet office needs and does not belong to employees. Use of office EIR is a privilege which the office may revoke or restrict at any time without priornotice to the employee.

All office computers and office electronic devices are to be registered to the office and not to an employee. All software on office computers and office electronic devices is to be registered to the office and not to an employee, except as otherwise provided in this policy.

No employee shall remove an office computer or office electronic device from officeproperty without the prior, express authorization of the employee's supervisor.

NO EMPLOYEE PRIVACY

Employees have no privacy whatsoever in their personal or work-related use of office EIR, or to any communications or other information contained in office EIR or that may pass through office EIR. With or without cause and with or without notice to the employee, the office retainsthe right to remotely monitor, physically inspect, or examine office computers, electronic devices, network, or other EIR, and any communication or information stored on or passingthrough office EIR, including but not limited to software, data and image files, internet use, emails, text messages, and voicemail.

All email sent and received via the office email system, including email of a personal nature, will be captured and retained in a central location for a period of time determined by the officeto be appropriate. Deletion of email from computers and electronic devices will not deletecaptured and retained email. The email that is captured and retained in a central location is the office's official record of the email, no matter where other copies of that email may be found.

Office EIR will be inspected for software and/or virus-like programming, including commercialsoftware applications ("Apps") that harvest, collect, or compromise data or information resources. Any computer or electronic device containing those elements may be disconnected, blocked, or otherwise isolated at any time and without notice in order to protect office EIR. This includes personal computers and/or electronic devices that an employee may connect, with or without proper authorization, to office EIR. Due to the commonplace presenceof such software and Apps on personal computers and/or devices, their connection to office EIRwithout prior authorization is discouraged.

When an employee leaves employment with the office, management shall be given access to andthe authority to dispose of any and all office electronic records, including the employee's computer files, email, voicemail, text messages, and any other electronic information stored onoffice EIR. Employees leaving their employment shall provide the office with all files and other electronic records from personal computers and devices, and employees shall not delete those items from office EIR.

PERSONAL USE

Employees shall use office EIR primarily for purposes related to their employment. Office laptop computers and portable electronic devices shall be used solely by authorized employeesand not by family members or other unauthorized persons.

When approved by the employee's supervisor in advance, an employee may make minimal personal use of office EIR as long as that 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 ofthe office or the performance of the employee's duties. Should an employee use office EIR to access personal software, websites, Apps, social media, or other personal accounts, the employeeshall be responsible for any disclosure of office electronic records, including student records, resulting from that use. As described in this policy, employees have no privacy whatsoever in their personal use of office EIR, including but not limited to software, data and image files, internet use, text messages, and emails. As noted in this policy, all emails sent and received viathe office email system are captured and retained by the office.

PASSWORD AND DEVICE PROTECTIONS

To protect against unauthorized use of and/or access to office EIR and electronic records, all office computers and electronic devices that can be password protected must be password protected, even if a computer or electronic device is assigned to a single employee for his or hersole use.

All personal computers and electronic devices connected to the office EIR, including the email system, or which otherwise contain office electronic records or access to those records, shall have user passwords installed and utilized to preclude unauthorized access to and/or use of the personal computer or device and/or its connection to office EIR. Whenever possible, individualprograms, Apps, and/or

connections on personal computers and electronic devices shall each be password protected, requiring manual entry of a password before the computer or devicecan connect to any office EIR, including email, or to any office electronic records. Office passwords should be different from personal passwords.

Any screensaver that can be password protected must be password protected in addition to any network login requirement. Whether or not password protection is technologically feasible, theemployee who owns a computer or electronic device that can be connected to office EIR, or that contains office electronic records, shall be responsible for physically protecting it against unauthorized use.

The Superintendent/designee may authorize and require installation of special software on officedevices to enable remote shutdown to prevent unauthorized disclosures of office records should the device be lost or stolen. The Superintendent/designee may authorize installation of special software on personal devices that may contain office records, or have access to office records, toenable remote shutdown should the device be lost or stolen.

SOFTWARE AND ELECTRONIC DEVICES

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

Computers, cellphones, tablets, and similar devices, are capable of downloading, storing, andusing various software, including Apps from both office-approved and non-approved providers.Some Apps are known to collect data from devices onto which they are loaded and from otherdevices to which the device is connected. That collection, and any dissemination of collected data, is a threat to the confidentiality of electronic records stored on office EIR and a breach of information security. For this reason, employees shall not download non-approved Apps ontooffice computers or devices. If an employee downloads a non-approved App onto an office computer or device, the employee may be held personally liable for any resulting unauthorized disclosure of office electronic records, including student records, in addition to any disciplinaryactions taken for the unauthorized download.

Employees are discouraged from downloading non-approved Apps onto personal computersand devices that may contain office electronic records or be connected to or used with office EIR. Employees are responsible to ensure that no office electronic records are compromised and no confidential information is inappropriately disclosed or breached because of the employee's use of personal computers or devices or any software downloaded onto them.

The Superintendent/designee is authorized to approve employee requests for installation of non-office software onto office computers and devices, 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. Approval shall be limited, as follows:

   - 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 officehas no obligation to install the software on that equipment.

Employees who have been authorized to download and install software shall adhere to copyrights, trademarks, licenses, and any contractual agreements applicable to the software,including provisions prohibiting the duplication of material without proper authorization and/or inclusion of copyright notices in any use of the material.

FILTERS AND OTHER INTERNET PROTECTION MEASURES

To ensure that 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 areinconsistent with the mission and values of the office. No employee shall bypass or evade, orattempt to bypass or evade, the office's filter system. This prohibition includes the use of personal computers, devices, or internet connections to access inappropriate content while in an office facility.

OTHER UNACCEPTABLE USES

In addition to other provisions of this policy, employees using office EIR shall be responsible for using them only in compliance with the following requirements unless theSuperintendent/designee gives prior express 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 thedesignated technology administrator at the employee's worksite.

2. Employees are prohibited from using office EIR for knowingly transmitting, receiving,or storing any oral or written communication that is obscene, threatening, or disruptive,or that reasonably could be construed as discrimination, harassment, bullying, or disparagement of others based on actual or perceived characteristics of race, ethnicity,religion, color, national origin, nationality, ancestry, ethnic group identification, physicaldisability, mental disability, medical condition, marital status, sex, age, sexual orientation, gender, gender identity, gender expression, genetic information (or association with a person or group with one or more of these actual or perceived characteristics). This prohibition applies to written and oral communication of any kind,including music and images.

3. Employees are prohibited from using office EIR for knowingly accessing, transmitting, receiving, or storing any image file that depicts actual or simulated torture, bondage, orphysical abuse of any human being or other creature, or that is sexually explicit orpornographic. This

prohibition does not apply to technology department employees engaged in authorized tracking/ investigative activities regarding technology usage history of another employee.

A. "Sexually explicit" means a visual depiction of actual or simulated human sexacts, 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, transmit, or download copyrighted material on EIRwithout permission of the copyright holder. Employees shall only download copyrighted material in accordance with applicable copyright laws.

5. Employees are prohibited from knowingly using EIR to intentionally access information intended to be private or restricted; change data created or owned by another user or anyother agency, company, or network; make unauthorized changes to the appearance oroperational characteristics of the office's system; load, upload, download, or create acomputer virus; alter the file of any other user or entity; remove a password; or alter system settings, preloaded software settings, firmware, and hardware without prior approval of the designated technology administrator at the employee's worksite.

6. Employees are prohibited from remotely accessing the office electronic network withoutprior express approval of the Superintendent/designee.

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, without prior approval of the designated technology administrator at the employee's worksite.This prohibition is not intended to prevent uploads or file copying for appropriate work-related purposes.

8. Any text transmission concerning an office matter should be done using an authorizedoffice messaging system and/or device, or in a manner that protects the confidentialityand/or future recoverability of the message.

9. Employees also are prohibited from using EIR for the following:

- Personal financial gain
- Commercial advertising
- Political activity as defined in California Education Code Sections 7050-7058
- Religious advocacy
- Promoting charitable organizations without prior authorization
- Communicating in someone else's name
- Attempting to breach network security
- Creating, sending, or receiving materials that are inconsistent with the missionand values of the office

- Mass distribution of email to a school site without prior approval of the site administrator
- Mass distribution of email to the office without approval of the Superintendent/designee
- Any activity prohibited by law, board policy, administrative regulation, or therules of conduct described in the Education Code

10. Employees are prohibited from using personal computers, devices, or internet connections for any unacceptable use identified in this policy while physically located onor in an office facility.

APPROPRIATE USE OF PERSONAL COMPUTERS AND DEVICES, PUBLICRECORDS, AND COLLECTION OF OFFICE ELECTRONIC RECORDS

To the extent described, this policy also applies to an employee's personal computer or electronic device that either contains office electronic records or is being used with or connected to the office's EIR, and also applies to the use of personal computers and deviceswhile they are physically located on office property. Without limitation, this includes personal cellphones or other devices, the use of which is supported by an office stipend.

While use of personal computers and other personal devices for office business is permitted, it isalso discouraged. Employees are advised that any and all office electronic records contained on any personal device are the property of the office and their disclosure may be required.
Employees have no expectation of privacy in such records. Office business communications andrecords may constitute "public records" under the California Public Records Act, and may be records which the office is required to maintain under applicable law, including Title 5 of the California Code of Regulations. The office may be required to collect, disclose, produce and/or store such records, regardless of the ownership of the computer or device on which the records are located. There is no expectation of privacy in any public record located on a personal computer or device. Upon request, employees will search personal computers, personal devices,and personal email and messaging systems for the presence of office electronic records and deliver them to the office.

For example, use of an employee's personal email account to send or receive email related to office business could result in the personal email account containing records potentially deemedto be public records subject to collection and disclosure or office retention and such email shall be forwarded to the office email system, unless the email already reflects it is sent from or is copied to the office email system. The forwarded or copied email becomes the official office record of the email, will be retained by the office email system, and such email on the
employee's personal email system, and/or reflected in the personal computer or device, wouldonly be only a duplicate copy, not subject to required collection in response to a public recordsrequest, and should thereafter be deleted from the employee's personal email account. In suchinstances, there should be no expectation of privacy in the email.

If the employee works on, prepares, creates, or possesses an electronic record pertaining to office business, in any form, on a personal computer or device, that record would potentially be deemed a public record or record subject to collection, disclosure, or office retention. In those instances, there should be no expectation of privacy in the office electronic record locatedon an employee's personal computer or device in any form or format. Upon request, the employee shall transmit the record in electronic format to the office, either through use of theoffice email system or other means, and then

delete the record from the employee's personalcomputer or device.

When an employee is requested to search for public records on a personal computer or device, apersonal server, or in personal email or other accounts, the employee shall conduct a search for the records in a timely manner and may report on the search results in one or more of the following ways: 1) delivering the located public records to the office, or 2) providing an affidavitstating that no public records were found, or 3) providing an affidavit with sufficient informationabout a record to show it should not be deemed a public record.

Only the office's designated chief technology administrator is allowed to authorize installationor maintenance of either hardware or software on office or personal computers and electronic devices, with the following exceptions:

Employees required by the office to have personal electronic devices may install such connection software as required to permit uploading, downloading, and syncing their required devices with an office computer;

Employees required by the office to have personal electronic devices will be provided authorized software, including authorized Apps for the devices; downloading non-authorizedApps onto such devices is discouraged;

Employees authorized to connect personal electronic devices to office EIR may be required toinstall appropriate security protection software on the device and the chief technology administrator may, in his/her discretion, elect to provide the required security protection software.

Certain activities on personal computers or devices while those devices are physically located onoffice property or sites may be permissible as long as those activities do not violate this policy, do not result in any additional fee or charge to the office, and do not interfere with the normal business practices of the office or performance of the employee's duties. For example only, while physically located on or in an office facility, employees may use a personal device to check personal email or take a call.

USE OF WEB-BASED PRODUCTS AND SERVICES

1. The office has elected to use various web-based products for both instructional use with students and other internal purposes. Examples of those products include but are not limited to Microsoft Offcie 365, Microsoft OneDrive, Google Applications, Canvas, Etc. For purposes of this policy, student information includes both personally identifiable information and covered information, as follows:

   "Personally identifiable information" includes but is not limited to a student's name, the name of the student's parents or other family members, the student's address, a personal identifier(such as the student's social security number), student number or biometric record, indirect identifiers(such as the student's date of birth, place of birth, and mother'smaiden name), other information that alone or in combination is linked or linkable to a specific student that would allow a reasonable person in the school community, who doesnot have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or information requested by a person who the agency reasonably believes knows the identity of the student to whom the education record relates.

"Covered information" includes personally identifiable information or materials in any media or format that is created or provided by a student, or the student's parent or legal guardian, or is created or provided by an employee or agent of the office, or which is descriptive of a student or otherwise identifies a student, including educational records oremail, first and last name, home address, telephone number, email address, or other information that allows physical or online contact, discipline records, test results, specialeducation data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security number, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voicerecordings, or geolocation information.

2. Employees should make themselves aware of the presence or absence of student information in their use of web-based products and services. Any communication containingstudent information made with persons inside or outside the office, including via email orany web-based application for sharing information, should be made only with persons legally entitled to receive the student information without violating rules against unauthorized disclosure. Student information shared by an employee with anyone outside the office without express permission from the designated technology administrator at the employee's worksite is shared at the employee's own risk.

3. Employees will only log in to office web-based products and services using their assigned office web-based log-in information, which may be different from their regular office log-in information; employees will not log in to office web-based products and/or services using any personal or non-assigned web-based log-in information.

4. Employees will not log in to office web-based products and services using any personal computer or personal device that contains non-office web-based products or services withoutexpress permission from the designated technology administrator at the employee's worksite.

5. When using office web-based products and services, employees may be exposed to links to other web-based applications that are not part of the office-approved core applications or sites. Those linked applications and sites are not required to be secure or confidential and may collect and share sensitive information, including student educational records, student covered information, or employee sensitive information. Employees will not use links or access non-office-approved web-based applications or sites and will immediately exit any linked applicationsor sites if accessed.

6. Employees understand that their use of office EIR is subject to this policy and that itsterms take precedence over anything to the contrary contained or represented in any web-based documents or policies.

7. Employees understand that email and documents created within office web-based productsand services may not be maintained in or on office EIR, that they are stored within the architecture of the web-based products and services, and that the office has no control overthe safety, security, or maintenance of the email and documents. Email and documentspertaining to the business of the office, including student instructional material, may bepublic records and may be records that are required to be retained and employees shall not delete or discard public or other records that require retention by the office.

8. Employees who are designated as or otherwise become administrators of a web-based network within the office shall make all privacy and other settings the most restrictiveand protective of student information unless expressly authorized not to do so by an administrator at the office cabinet level.

9. Employees working with an office web-based application shall not attempt to bypass or avoid the privacy settings of the application.

DISCLAIMER

The office makes no guarantees about the quality of the EIR provided and is not responsible forany claims, losses, damages, costs, or other obligations arising from employee use of office EIR.Any charges an employee accrues due to personal use of office EIR are to be borne by the employee. The office also denies any responsibility for the accuracy or quality of the information obtained through employee access.

VIOLATION OF THIS POLICY

Violation of this policy shall be promptly reported to management personnel. Management personnel shall then promptly report any violation of this policy to the Superintendent/designee.

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. An employee's use of office EIR may also be restricted, suspended, or revoked.

Policy History: Approved 9/19/07, Revised: 9/19/07, 10/2/13, 5/19/16, 7/12/17, 6/21/23