Personnel – All Personnel

STAFF ACCEPTABLE USE OF TECHNOLOGY

The Contra Costa County Office of Education's (the "CCCOE") technology resources — including desktop and laptop computers, personal digital assistants, Internet access, electronic mail, intranet, telephones, voice mail, scanners, and fax machines — enable employees to quickly and efficiently access and exchange information. When used properly, the County Superintendent of Schools recognizes that technological resources can enhance employee performance by improving access to and exchange of information, offering effective tools to assist in providing a quality instructional program, increasing educational opportunities, and facilitating CCCOE operations. This regulation explains how the CCCOE expects you to use these technology resources.

All employees are expected to learn and use the available technological resources that will assist them in the performance of their job responsibilities. These resources are provided at the public's expense and maintained by CCCOE and therefore, are to be used by members of the school community with respect for the public trust through which they have been provided.

CCCOE periodically updates technology standards as directed by the County Superintendent of Schools. Staff members who agree to abide by these defined standards will have access to appropriate, available resources, with guidance and support provided by the Technology Systems Department.

Board Policy 4177 has established ethical standards for the use of technology and technological resources in our schools. All CCCOE policies, including this Acceptable Use Policy, apply to all CCCOE staff, whether or not they come into direct contact with students. This Acceptable Use Policy applies to all technology resources owned or leased by CCCOE; used on, or accessed from CCCOE premises; or used in CCCOE business. This policy also applies to all activities using any CCCOE-paid accounts, subscriptions, or other technical services, such as Internet access, cell phones, voicemail, and e-mail. This policy applies whether or not the activities are conducted from CCCOE premises. Use of CCCOE technology resources is a privilege, which may be revoked at any time.

This Acceptable Use Policy does not attempt to articulate all required or prohibited behavior by users. Additional guidance and support is provided by the Technology Systems Department. Successful operation of such resources requires that all users conduct themselves in a responsible, confidential, ethical, decent, and polite manner, consistent with CCCOE Mission and Goals.

A. Acceptable Business Uses of Technology Resources

1. General Policy: CCCOE's technology resources are provided to conduct CCCOE business for CCCOE's benefit. Use of CCCOE's technology resources must not interfere with work productivity or the operation of CCCOE's technology resources. Each employee is responsible for the content of all text, audio and images that he or she creates, retrieves or sends using CCCOE's technology resources. All of CCCOE's policies and procedures regarding employee conduct apply to employees' use of CCCOE's technology resources.

Personnel – All Personnel

STAFF ACCEPTABLE USE OF TECHNOLOGY

2. Electronic Mail: Because e-mail seems informal, they are sometimes offhand, like a conversation, and not as carefully thought out as a letter or memorandum. Like any other document, e-mail and instant messages can later be used to indicate what an employee knew or how an employee acted. You should keep this in mind when creating e-mail and other documents. You also should keep in mind that even after you delete an e-mail or close a computer session, the message may still be recoverable and may even remain on the system.

3. Use of Wireless Devices: You should not use any wireless device to connect to the CCCOE's intranet unless the connection is secured or encrypted. If you are not sure whether a wireless device provides a secure connection, please contact your Technology Systems representative.

4. Use of E-Mail Distribution Lists: Because some information is intended for specific individuals and may not be appropriate for general distribution, users should exercise caution when forwarding messages or using distribution lists.

5. Use of CCCOE E-Mail Accounts: Employees should not use personal e-mail accounts to conduct any CCCOE related business.

6. Commitment to Applicable Laws: The CCCOE is committed to meeting the provisions established in the Family Educational Rights and Privacy Act (FERPA) and California Education Code, which protect the rights of students regarding education records. CCCOE is committed to meeting the provisions established in the Health Insurance Portability and Accountability Act (HIPAA), which protects the rights of students and employees regarding Protected Health Information. When technology resources are used to transmit confidential information about students, employees, and/or CCCOE business, all appropriate safeguards must be used.

   In addition, the CCCOE is committed to meeting the provisions established in the Children's Internet Protection Act (CIPA), which protects the safety and privacy of minors. Consequently, CCCOE uses appropriate filtering technology to limit access to the Internet, in an attempt to prevent online access to materials that are obscene, contain child pornography, or are harmful to minors. All use of the CCCOE's technology resources must comply with the applicable federal and state laws and the CCCOE's commitment to comply with and uphold such laws.

Personnel – All Personnel

STAFF ACCEPTABLE USE OF TECHNOLOGY

B. Acceptable Non-Business Use of Technology Resources

1. General Policy: Employees are permitted to use the CCCOE's electronic resources for occasional and important non-business purposes such as coordinating child care with a family member, communicating a change in work schedule, or scheduling an appointment with a health care provider. Non-business uses should not involve significant use of the CCCOE's electronic resources, such as your or others' work time, computer time, or bandwidth.

2. Non-business use is subject to the following:

   a. All non-business communications are subject to this policy in its entirety and to all other CCCOE policies. All non-business communications may be monitored at any time in accordance with this policy.

   b. You should not use the CCCOE's electronic resources for communications that you wish to keep private, such as communications with a physician or your personal attorney.

   c. When feasible, non-business uses should be made during breaks or lunch periods.

   d. Non-business uses do not preempt any business activity and must not interfere with the user's or others' productivity and the use cannot be otherwise prohibited by CCCOE policies.

   e. Employees' access to personal e-mail accounts during working hours is subject to all of the requirements contained in this policy.

   f. A CCCOE employee, acting in an individual capacity and outside the scope of employment, may, during non-working time, express views and opinions that do not necessarily state or reflect those of CCCOE. Any such expression shall neither state nor imply that it is made on behalf of CCCOE. A CCCOE employee shall not communicate information otherwise prohibited by CCCOE policy or procedures using technological resources.

Personnel – All Personnel

STAFF ACCEPTABLE USE OF TECHNOLOGY

C. Unacceptable Uses of Technology Resources

Misuse or abuse of the CCCOE's technology resources and, in particular, the CCCOE's e-mail system, could expose the CCCOE and any individual who engages in the improper conduct to civil and even criminal liability. For this reason, all of the CCCOE's employees should carefully review the following list of prohibited conduct and comply with it. This list is not necessarily all inclusive. Any conduct listed below as well as any other conduct constituting misuse or abuse of the CCCOE's technology resources is grounds for discipline, up to and including termination, in accordance with applicable collective bargaining agreement, Board Policy, Administrative Regulation, and applicable law as well as revocation of the privilege of using the technology resources:

1. Non-Disclosure of Confidential Information: The CCCOE's technology resources may not be used to disclose Confidential Information, without proper authorization, regarding students, employees, or the CCCOE's operations. For additional information concerning the protection of the CCCOE's Confidential Information for students, please see Administrative Regulation 5125.1, "Student Records: Confidentiality." The CCCOE's Confidential information regarding students, employees or CCCOE's operations should not be stored on the local or "C" drive of any computer or on any portable storage medium without the prior authorization of the Technology Systems Department. Any such storage should be for short-term purposes only, such as accessibility of information during business travel, and the stored information should be deleted promptly after the short-term purpose has been accomplished.

2. No Offensive or Harassing Messages: Using CCCOE resources to send, save, post, publish or view offensive or threatening material is prohibited. Messages stored and/or transmitted by computer, voice mail, e-mail, or telephone systems must not contain content that may reasonably be considered offensive to any employee. Offensive material includes, but is not limited to, sexual comments, jokes or images; racial slurs; gender-specific comments; or any comments, jokes or images that would offend someone on the basis of his or her race, color, creed, sex, sexual orientation, age, national origin or ancestry, physical or mental disability, veteran status, as well as any other category protected by federal, state, or local laws. Any use of the Internet/World Wide Web or intranet to harass or discriminate is unlawful and strictly prohibited by the CCCOE.

3. No Illegal or Unethical Conduct: Employees shall not use the CCCOE's technology resources to engage in unethical practices or any activity prohibited by law, Board Policy or Administrative Regulation.

Personnel – All Personnel

STAFF ACCEPTABLE USE OF TECHNOLOGY

4. No Duplication or Alteration of Data: Data, files, passwords, computer systems and programs, or other property of the CCCOE, may not be downloaded, duplicated, altered, removed or installed for purposes unrelated to the CCCOE's business without the prior, written authorization of the Chief Technology Officer.

5. No Downloading of Software or Copyrighted Material: Employees may not download any copyrighted material, or install any software, to the CCCOE's technology resources without the prior, written authorization of the Chief Technology Officer. For instance, a CCCOE employee may not download any software or electronic files without implementing virus protection measures that have been approved by CCCOE. This prohibition applies to the use of iPods (or similar equipment) and to the downloading of unauthorized instant messaging software. The Chief Technology Officer will not approve the downloading or installation of any copyrighted materials unless the CCCOE has first obtained a license or permission to do so. Failure to observe a copyright may result in legal action by the copyright owner. Any questions concerning these rights should be directed to the Chief Technology Officer.

6. No Unauthorized Monitoring or Interception: Only authorized employees may monitor, intercept or review the electronic communications or files of another employee. Employees shall not attempt to interfere or interfere with other users' ability to send or receive electronic communications, nor shall they attempt to read, delete, copy, modify or forge other users' electronic communications.

7. No Falsification of Identity: Users must never send e-mail from the account of another employee or use another employee's user ID and password to gain access to any system, thus misrepresenting himself or herself as that person. Users may not examine, change, or use another person's files, output, records, or user name for which they do not have explicit authorization.

8. No Sending or Receiving or Malicious Software: Employees should not knowingly upload, send or receive malicious software, *i.e.,* worms, viruses, or Trojan horses, using the CCCOE's technology resources. Employees should take care to avoid inadvertently sending, receiving, or opening malicious software. Employees, for example, should not open any e-mail attachments received from an unknown source. Additionally, employees shall not maliciously attempt to harm or destroy CCCOE equipment or materials or the data of any other user, including "hacking."

9. No Solicitation: Solicitation, including advertisement, for outside business ventures, political purposes, charitable contributions, religious purposes, or non CCCOE activities or events using CCCOE resources, is prohibited. Employee postings are not permitted on the CCCOE's intranet.

Personnel – All Personnel

STAFF ACCEPTABLE USE OF TECHNOLOGY

10. No Game Playing: Employees may not use the CCCOE's technology resources to play games, such as fantasy football, or to gamble.

11. Use of Cellular Phones/Mobile Communication Devices: Employees shall not use a cellular phone or other mobile communication device for personal business while on duty, except in emergency situations and/or during scheduled work breaks.

12. No Mass Distribution of Electronic Mail: Senders may not engage in blanket forwarding of messages to parties outside of the CCCOE's system or in sending e-mail to more than employees within the CCCOE unless the sender has obtained prior permission of the department manager.

13. CCCOE discourages staff from engaging in social networking with students. Staff cannot have associations with students through virtual technology and/or posts on social networking Internet web sites if they are irregular, unprofessional, improper or imprudent in ways that negatively affect the goals of CCCOE, or are otherwise prohibited by CCCOE policy or procedures using technological resources. Any conduct, which reflects poorly upon personnel or CCCOE, may be grounds for disciplinary action. The County Superintendent of Schools has discretion in determining if conduct reflects poorly on our students, staff and CCCOE.

14. An employee may not interfere with the normal operation of the CCCOE's network, including creating unsanctioned high-volume network traffic that substantially hinders others in their use of the network. This includes causing congestion or disruption of the CCCOE network through inappropriate downloads of large files, streaming audio/video, or other such activities.

D. No Expectation of Privacy

1. Use of Electronic Resources Is Not Private or Confidential: Communications and files transmitted over, or stored on, the CCCOE's computer, e-mail, voice mail, systems, including back-up copies, whether for business or non-business reason, are not private or confidential. All Communications Are the CCCOE's Property: The CCCOE's computer, voice mail, e-mail systems, and the data stored on them, are and remain at all times the property of the CCCOE. As a result, computer data, voice mail messages, e-mail messages, instant messages and other stored data are readily available to numerous persons.

Personnel – All Personnel

STAFF ACCEPTABLE USE OF TECHNOLOGY

2. The CCCOE's Right to Monitor and Review Stored Communications and Files: The CCCOE may monitor, audit, delete and read any information stored on its information systems, including e-mail, voice mail systems, Internet usage, word processing documents, spreadsheets, *etc*., at any time without advance notice or consent, and may copy, store, or delete any electronic communication or files and disclose them to others as it deems necessary. While it is not the CCCOE's policy to regularly monitor or review the contents of these communications or files, the CCCOE may do so at any time to support business, maintenance, auditing, security and investigative activities. Any electronically stored information that you create, send to, or receive from others may be retrieved and reviewed when doing so serves the legitimate business interests of the CCCOE. You should also be aware that, even when a file or message is erased, or a visit to a Web site is closed, the CCCOE still may be able to recreate the message or locate the Web site. The CCCOE's not exercising its rights with respect to certain communications or files in no way modifies or waives the CCCOE's right to monitor other electronic communications or files. The CCCOE's right to monitor may be altered or modified only in a writing signed by the County Superintendent of Schools.

3. The CCCOE May Override Any Password or Encryption: Although you may have passwords to access computer, voice mail, and e-mail systems, these technical resources still belong to the CCCOE, are to be accessible at all times by the CCCOE, and are subject to inspections by the CCCOE, with or without notice. The CCCOE may override any applicable passwords or codes to inspect, investigate, or search an employee's files and messages. All passwords must be made available to the Chief Technology Officer.

   To facilitate the CCCOE's access to information on its computer and voice mail networks, you may not encrypt or encode any voice mail or e-mail communication or any other files or data stored or exchanged on the CCCOE's systems without the prior, written authorization of Chief Technology Officer. The Chief Technology Officer will not approve any such request unless you provide the Technology Systems Department with any password, encryption key or code, or software needed to access the encrypted information in your absence.

4. Disclosures to Third Parties: All data transmitted over, or stored on, the CCCOE's electronic resources potentially is subject to disclosure, at the CCCOE's discretion, to law enforcement or to other third parties without prior consent of the sender or the recipient.

E. Electronic Communications Through Third-Party Service Providers

1. Employees are prohibited from using any third-party electronic communications service, such as, Yahoo!, America Online, or a cell phone carrier's text messaging capability, to conduct CCCOE business unless the CCCOE is the subscriber to the service.

Personnel – All Personnel

STAFF ACCEPTABLE USE OF TECHNOLOGY

2. Communications by employees through any third-party electronic communications service for which the CCCOE is the subscriber are subject to all CCCOE policies, including this policy.

3. The CCCOE may request, at any time, that an employee execute a consent agreement to permit access by the CCCOE to electronic communications stored by a third-party electronic communications service for which the CCCOE is the subscriber. Employees are required to cooperate with the CCCOE in obtaining such consents as well as in the CCCOE's obtaining access to the stored communications.

4. Upon the CCCOE's request, employees using a communications device, such as a Blackberry or a cell phone, issued, or paid for, by the CCCOE must provide the device to the CCCOE for inspection.

F. Other

1. Users must immediately report violations of this policy or security issues to the County Superintendent of Schools or designee.

2. Users may keep e-mails related to their job in their personal folders accessible through GroupWise. Users should purge messages monthly from their personal e-mail storage areas which the CCCOE no longer needs for business purposes. After a specified period, the Technology Systems staff will delete e-mail messages backed up to a separate data storage media to free scarce storage space. [See CCCOE Email Retention Policy AR4178.] This policy should be suspended by any user of the CCCOE's technology resources who receives notice that a "litigation hold" has been implemented.

3. Employees are given access and the ability to use technology resources that students may not receive. Employees agree to monitor student's use of technology resources while under the employee's supervision. Employees shall not allow students access to the CCCOE's technology resources through the employee's own login and password and agree to maintain security on their computers, accounts, and the CCCOE's network.

4. Violations of this Policy may result in revocation of the privilege to use the CCCOE's technology resources as well as disciplinary action up to and including, dismissal and/or legal action in accordance with applicable law, collective bargaining agreements, Board Policy, and Administrative Regulations.

Personnel – All Personnel

STAFF ACCEPTABLE USE OF TECHNOLOGY

5. The CCCOE does not consider conduct in violation of this policy to be within the course and scope of employment or the direct consequence of the discharge of one's duties. Accordingly, to the extent permitted by law, the CCCOE reserves the right not to provide a defense or pay damages assessed against an employee for conduct in violation of this policy.

6. Although CCCOE will make a concerted effort to protect staff from adverse consequences resulting from use of CCCOE technology resources, all users must exercise individual vigilance and responsibility to avoid inappropriate and/or illegal activities. Users are ultimately responsible for their actions in accessing and using CCCOE computers and/or mobile devices and the CCCOE computer network. CCCOE accepts no liability relative to information stored and/or retrieved on CCCOE-owned technology resources. CCCOE accepts no liability for employee-owned technology resources used on CCCOE property.

CCCOE employees are expected to review, understand, and abide by the requirements described in this regulation, Board Policy 4177, and the procedures provided by the Technology Systems Department. The signature, at the end of this document, is legally binding and indicates that the party who signed has read the terms and conditions carefully and understands their significance. All employees must review and sign this document annually. CCCOE supervisors are required to enforce these policies and regulations consistently and uniformly. No supervisor has the authority to override the policies and regulations. Only the County Superintendent of Schools may override these policies and regulations and must do so in writing.

ACKNOWLEDGMENT

I hereby acknowledge that I have reviewed the CCCOE's Employee Acceptable Use Policy, BP 4177 and AR 4177. I understand that my use, or continued use, of the CCCOE's technology resources is conditioned upon my agreement to this Policy and Regulation and reflects my consent to this Policy. I hereby agree to abide by the Policy and Regulation. I also consent to the CCCOE's monitoring of my communications over the CCCOE's technology resources as described in the Policy and Regulation.

Signature:_____ Date: _____

Printed Name:_____

Regulation approved: May 28, 1997

Regulation amended: June 20, 2012
September 19, 2012