Monterey County Office of Education
Employee Computer, Telephone and Network Acceptable Use Policy

TABLE OF CONTENTS

Purpose 2
Employee Acknowledgement 2
Introduction 2
The MCOE Computer and Network Environment 2
Privacy of County Office Records - Student, Staff, and Business Information 3
Ownership 3
Use of Personally Owned Software or Equipment 4
Software Copyright Law 4
Use of the Internet 4
Copyrights and the Internet 5
Use of Computer Resources 6
Your Computer Account 6
Passwords 7
Passwords and Students 7
Computer Viruses 8
Email and Messaging Systems 8
Cautions About Use 8
Monitoring 9
Personal Use 9
State, Federal, and Copyright Laws 9
Restrictions 10
Representation 10
False Identity 11
Security and Confidentiality 11
Use of Telephones, Cell Phones, FAX Numbers, and Voicemail 11
Penalties for Violations 12
Legal References: 12
Employee Acknowledgement and Signature 13

Monterey County Office of Education
Employee Computer, Telephone and Network Acceptable Use Policy

Purpose

Communications and computer technology at the Monterey County Office of Education (MCOE) are provided and maintained for instructional, educational and administrative purposes. The following guidelines implement Board Policy 4040, Employee Use of Technology, and govern the use of these technologies by employees during the performance of their duties.

Employee Acknowledgement

All employees of MCOE who have access to MCOE technology will be required to acknowledge that they have received, and agreed to abide by this Administrative Regulation. (See Employee Acknowledgement and Signature form - Page 14)

Introduction

The Information Age revolution brings with it a host of new laws that reflects the fast paced change of electronic communication. It is important that everyone understand the rules and regulations when using MCOE resources in this new environment. This document describes the computer, telephone, information, and network resources made available by the MCOE and relevant responsibilities and obligations in the use of these resources. All MCOE employees are required to read and sign this document.

The MCOE Computer and Network Environment

MCOE has created extensive networks of information, telephone and computing resources for staff and student use. In addition, the MCOE provides a large and continuously growing number of computer workstations, printers, peripherals, facsimile machines, software, training and supplies to all sites. These items are provided to allow staff and others in the MCOE to perform tasks effectively in meeting the goals and needs for which MCOE was established.

By nature, design, and function, the MCOE computer network and resources must provide a relatively "open" environment. While automatic and procedural security

controls are in place to prevent or reduce unauthorized access to these resources, the primary responsibility for maintaining the security of this information and its resources lies with the employee.

Improper use of any of these resources can cause problems related to the needs of some or all employees and students in the MCOE. Violation of specific local, State, and Federal laws referenced later in this document may call for prosecution under the law including fines and imprisonment. The MCOE may take disciplinary action against employees for misuse of computer, network, and information resources.

Privacy of County Office Records - Student, Staff, and Business Information

It is probable that during their employment with the MCOE, staff members will have access to either student or employee and business information that is confidential. It is the responsibility of individual staff members to safeguard this information from unauthorized persons. Employees shall not seek to use personal or confidential information for their own use or personal gain. All reasonable precautions must be taken to ensure privacy is maintained under the law while handling information in any form; including, but not limited to: voice, electronic (disk file, diskette, CD/DVD ROM, USB portable drives, magnetic tape, email, FAX, etc.), paper, photograph, and microfiche information. Included under this precaution is the proper disposal of any privacy related materials.

Ownership

All staff must recognize and understand that MCOE business information, telephone, network, computer and software resources, peripherals and supplies are MCOE property, provided to meet MCOE needs. They do not belong to individuals, but are only "loaned" to staff members for the purposes required for their position while being employed by the Monterey County Superintendent of Schools.

It is a MCOE policy that online communication is to be used in a responsible, efficient, ethical, and legal manner in support of education, business and/or research and within the educational program and goals of the MCOE. The use of electronic information resources is a privilege, not a right. Each user is personally responsible for this provision at all times when using electronic information services.

All documents, spreadsheets, and other electronic media created by employees while performing their duties for MCOE are the property of MCOE. Upon termination of employment or changing of job responsibilities it is important to retain this work. Intentional deletion of this material is considered a willful act of destruction of MCOE property and may result in prosecution as permitted by local, state, and federal laws.

Use of Personally Owned Software or Equipment

The MCOE attempts to ensure that all hardware and software meet specific standards which will operate without causing disruption of the MCOE's computer and network resources. Therefore, the use of personally owned software or software that can be downloaded from the Internet as well as personally-owned computer hardware is not permitted except where authorized by the Technology and Information Services (TIS) Department.

In order to ensure proper configuration and to safeguard network security and performance, users should not attach computers, printers, network equipment (including wireless access points), or other types of hardware to MCOE's network without prior approval and support of the TIS Department. With the exception of the "Guest" wireless network, connecting personally owned technology equipment to MCOE hardware or to the MCOE network is not allowed. Any equipment found to be in violation of this policy will be immediately disconnected.

Software Copyright Law

Staff is prohibited from installing any software without having proof of licensing. Violations of copyright law have the potential of costing the MCOE millions of dollars. Software licensed for one workstation may not be installed on multiple machines. Employees should be aware that if, for example, a department purchases a new workstation, the department must also purchase new software licenses for the software that will be installed on it. If the computer being replaced will be retired from use, the software may be removed from it and transferred to a new workstation.

Use of the Internet

The Internet provides an extremely valuable resource for learning and communicating with people throughout the world. It can be a marvelous tool to enhance student and staff education and productivity. Unfortunately, the Internet also contains a large amount of information that is inappropriate for use in an educational Institution.

Supervisors have the right to monitor Internet usage of employees.

While electronic information resources offer tremendous opportunities of educational value, they also offer persons with illegal or unethical purposes avenues for reaching students, teachers, and others, including parents. MCOE does not have control of the information on commercial electronic information services or the information on the Internet, although it attempts to provide prudent and available barriers. Sites

accessible via the Internet may contain material that is illegal, defamatory, inaccurate or potentially offensive to some people.

Should an employee see any unacceptable materials or inappropriate use, he/she shall notify the site administrator or supervisor immediately. Employees shall report any instances where the Acceptable Use Policy or security may be violated. Employees shall also report inappropriate Internet web sites to TIS so that access to the sites can be blocked in the future.

If there is any doubt as to the appropriate use of an MCOE-provided electronic system, employees must review the use in advance with their supervisor and/or the Chief Technology and Operations Officer or his/her designee.

Internet resources are provided at County Office expense to enhance job functions and maximize job effectiveness. Employees are not to let personal use of the Internet encroach on or displace time spent performing their work duties. Incidental personal use of the Internet is allowed, provided that it is kept to a minimum. Such use should be restricted to breaks or lunch periods, or before or after work hours. Inasmuch as every transaction completed on the Internet publicly represents the County Office of Education and everything it stands for, it is imperative that employees not use the Internet in such a way as to bring civil or criminal liability or public reproach upon the County Office of Education.

No person shall use County network resources for personal gain or profit, or for personal reasons that would result in depleting County resources, impeding the organization's ability to conduct business, or cause any interruption or delay in service to the public.

Copyrights and the Internet

Materials obtained from the Internet are copyrighted and, with proper citation, limited educational use is permitted under the principle of Fair Use under U.S. copyright law. These materials may not be redistributed on the Internet or in any other manner without written consent of the copyright owner or as permitted by law. Materials are protected by copyright whether they bear copyright information or not.

Copyrighted material shall be posted online only in accordance with applicable copyright laws.

File-sharing software cannot be installed or used on MCOE computers for the purpose of illegally sharing copyrighted materials such as music, images and software. This type of software is often used to "pirate", or illegally copy, music across the Internet. These software packages are distributed under many different names but all use some form of peer-to-peer sharing protocol for which the use is illegal when used to share

copyrighted material. The most common use is the illegal "swapping" of music encoded in the MP3 format and is a violation of U.S. copyright laws.

Use of Computer Resources

The computing and network resources of the MCOE are used by thousands of employees and students across the County. In order to ensure that these resources are available and working properly, personal use of these resources must not negatively impact others. For example, employees may not attempt to break into computer systems or other resources to which they have not been granted authorization. Users may not attempt to maliciously alter, erase, damage, destroy or make otherwise unusable or inaccessible any data, software, computer, or network system. Attempts or actions of this nature are illegal and may result in any combination of disciplinary action and/or prosecution and fines including litigation costs and payment of damages under applicable local, State, and Federal statutes.

Equipment abuses are unacceptable whether out of frustration, misuse, negligence or carelessness. Users are responsible for damage to, or loss of, MCOE equipment. MCOE vandalism policies apply, making users liable for intentionally inflicted damage.

Users should not attempt repairs without authorization or support from designated personnel. Volunteers – parents, family members, or friends – are not authorized to attempt repairs on MCOE equipment.

Guidelines for the care and use of computer software are similar to hardware policies. Users are responsible for damage to or loss of MCOE software systems. MCOE vandalism policies apply to software as well, making users liable for intentionally inflicted damage.

Users should not store personal files or applications on MCOE electronic media systems including computers, file storage, etc.

Employee Computer Accounts

In order for employees to utilize the MCOE computer and network resources, they will be assigned user accounts with login IDs and passwords. Based on individual assignment and with proper position authorization, employees may be provided with access levels which allow them to view, create, alter, delete, print, and electronically transmit information.

Individual staff members are responsible for maintaining the security of their individual accounts and may not release them for use by any other individual. Employees must accord user accounts the same significance as their hand-written signature. Failure to

do so by releasing this information to another individual may be considered false representation and result in disciplinary action.

Employees should never leave their workstation unattended while signed on to any account; doing so allows anyone to sit at the employee's workstation and "hijack" their account, users rights and privileges, to potentially perform destructive acts.

Passwords

It is extremely important that employees use passwords that cannot be guessed by others through knowledge about the individual. For example, users should never use personal names such as children or pets or names that begin or end with numbers. Never use your Social Security Number, bank PIN or words which can be found in any dictionary, names spelled backwards, or adjacent keys on a computer keyboard (i.e., QWERTY). All of the above provide an easy way for a hacker to break into a computer system and, cause damage and destruction. Staff members are advised to never write down user IDs or passwords unless they store them with their personal possessions or other location away from their place of work. Employees are directed to contact the TIS Department if they suspect someone else may have accessed their account. It is a simple matter to change a password but could take days to reconstruct damaged records or computer systems if someone breaks in using an authorized employee's account rights. Where employees have the ability to change their own password, they are to make a habit of periodically changing passwords for these accounts.

When passwords are used, the employee's supervisor may request that they have a record of the password and be notified of any changes. Passwords may be changed upon a supervisor's request.

Under certain circumstances, user IDs and passwords may be shared by a group of employees where doing so makes information access convenient with a minimum of administrative overhead. Group IDs and passwords should be held in confidence and never shared with students. If you suspect that the security of such information has been compromised, notify the TIS Department at once.

Additional information regarding MCOE's recommended password protocols can be found on the TIS website at http://www.montereycoe.org/TIS/passwordprotocols.pdf.

Passwords and Students

Only employees may have direct publishing (write privilege) access to MCOE web, mail, and listservs. Those who assume responsibility for posting student work must never delegate this responsibility to students.

Computer Viruses

The computer industry faces a continuing onslaught of malicious viruses, worms, and other damaging programs that attack computer and network resources. The MCOE attempts to maintain anti-virus software in order to minimize the impact of these viruses, but it is the employee's responsibility to take precautions to protect their computer and all others throughout the MCOE. Be very aware of opening email attachments. When in doubt, do NOT open.

Likewise, do not download any software from the Internet unless directed to do so and authorized by the TIS Department. It is not uncommon for even a very respectable company to unknowingly release products that include hidden or unknown viruses. Do not share any downloaded software with others until you have verified that it does not harbor viruses.

Email and Messaging Systems

MCOE encourages the use of electronic mail (email) to enhance communication and business activities. Users of this service need to be aware, however, that this technology is still developing, and acceptable use policies are necessary to ensure appropriate use and to prevent or limit disruptions to work activity and computer services. Emails stored on MCOE systems are legally discoverable documents reflective of the activities of the organization. All use of MCOE email systems is to be conducted in a professional manner in accordance with the provisions that follow.

Cautions About Use

The nature of electronic mail makes it susceptible to misuse. Users need to be aware that sensitive or private information can be easily forwarded to other individuals the originator never intended, both within MCOE as well as externally throughout the world.

Because of backup procedures in place with the MCOE computer services, the fact that an email message has been "deleted" does not necessarily mean that it cannot be retrieved.

Users of the MCOE email services need to be aware that use of these services is a privilege granted with the expectation that it will be used for business purposes and in a professional and courteous manner similar to other forms of communication. All email sent or received by individuals through MCOE employee accounts is the property of MCOE and may be requested by your supervisor and examined with just cause.

There is no guarantee that email received was in fact sent by the purported sender, since it is a simple matter, although a violation of this policy, to disguise the sender's

identity. Furthermore, email that is forwarded may be modified by the forwarder. As with any document, if a message is received which appears unusual or which may be questionable, check with the purported sender to verify authorship and authenticity. While encryption of email is a potential solution to ensure authenticity, it is an emerging technology that is not in widespread use and rather difficult to use consistently.

Monitoring

While MCOE does not have the time nor inclination to monitor or read individual email messages, in the event that questionable or inappropriate use is suspected or known, such email may be examined and may be cause for disciplinary action ranging from revoking your email account up to termination. Users should also be aware that in the general course of business, System Administrators and email operators may require observation of messages in order to verify proper system operation.

MCOE reserves the right to monitor and log all email, telephone, pager, text, and instant messaging activity of a user using county owned property with or without notice. Users should have no expectation of privacy or confidentiality when using these resources.

Personal Use

Incidental private or personal non-commercial use of the County Office of Education email is permitted as long as it is kept to a minimum and does not interfere with the County Office of Education normal business practices and/or the performance of the individual's tasks. Such use should be restricted to breaks or lunch periods, or before or after work hours. Individuals should exercise sound judgment and sensitivity to others when exchanging personal messages in the workplace.

No person shall use County network resources for personal gain or profit, or for personal reasons that would result in depleting County resources, impeding the organization’s ability to conduct business, or cause any interruption or delay in service to the public.

State, Federal, and Copyright Laws

In addition to this policy, use of the MCOE email services is subject to all applicable Federal and State communications and privacy laws. In particular, users need to be aware that attaching programs, sound, video, and images to email messages may violate copyright laws, and data files containing employee and/or student information are subject to all privacy laws.

Restrictions

Electronic mail may not be used for:

- Unlawful activities
- Spam mail or Mail "bombs"
- Use that violates County Office, State or Federal polices
- Any other use which interferes with computing facilities and services of the MCOE

In addition, email services shall not be used for purposes that could reasonably be expected to cause, either directly or indirectly, excessive strain on MCOE computing facilities or cause interference with others' use of email, email systems, or any computing facilities or services.

For example, attaching excessively large files and sending these to multiple users or repeatedly to the same user is a violation of this policy.

Representation

Users shall not give the impression that they are representing, giving opinions or otherwise making statements on behalf of the MCOE unless they are appropriately authorized, explicitly or implicitly, to do so. Where appropriate and based on context, an appropriate disclaimer would be, "These are my own statements and views and do not represent those of the Monterey County Office of Education."

An employee's signature line shall appear on all email messages. The signature must include:

- Name
- Title
- Department
- MCOE
- Telephone number

Example:

John Doe
Secretary
Alternative Education
Monterey County Office of Education
(831) 555-1212

For questions about constructing an automatic signature line to be inserted in email messages, please contact the TIS Help Desk at (831) 755-0322.

False Identity

Employees shall not employ a false identity in sending email or alter forwarded mail out of the context of its original meaning.

Security and Confidentiality

The confidentiality of electronic mail cannot be assured. Users should exercise extreme caution in using email to communicate confidential or sensitive material.

MCOE maintains an ongoing backup schedule of computer data in order to ensure that email services may be restored in the event of damage and/or destruction.

Users' email accounts have a size limitation. When the size limitation is nearly reached, an automatic notification will be sent to the user's account. If the overall size of the account is not reduced, users will continue to receive a warning that their mailbox is almost full. If no action is taken and the account size continues to grow and reaches the maximum size allowed, users will no longer be able to send messages and the receiving of new messages may be impacted. Users must delete and/or archive old email and remember to keep their Deleted Items folder emptied to allow for adequate space for new messages.

Use of Telephones, Cell Phones, FAX Numbers, and Voicemail

Telephones and cell phones are provided to conduct the business of the MCOE. In many cases, voice mail is also provided. These services are intended to provide a means of communication for employees to contact parents and students, agencies, vendors, other institutions and government officials. When using these services, staff should always reflect a businesslike and professional demeanor. If a phone or FAX is used for personal business, the MCOE must be reimbursed for any charges incurred. Private use of the phones should be kept to a minimum.

MCOE reserves the right to monitor and log all email, telephone, pager, text, and instant messaging activity of a user using county owned property with or without notice. Users should have no expectation of privacy or confidentiality when using these resources.

Penalties for Violations

Violation of the Acceptable Use Policy may result in a reduction or loss of access privileges. In many cases, access privileges may be essential to job functions. Additionally, those failing to follow the guidelines contained in this Administrative Regulation may face disciplinary action in accordance with collective bargaining agreements, state law, and Board policy.

Legal References:

Information Practices Act of 1977 (Civil Code section 1798-1798.1)
Public Records Act (Gov. Code section 6250-6270)
Penal Codes, Section 502
Federal Statutes:
Federal Family Educational Rights and Privacy Act of 1974
Federal Privacy Act of 1974
Electronic Communications Privacy Act of 1986

Adopted: 8/02/2010

Revised: 05/12/14

MONTEREY COUNTY OFFICE OF EDUCATION
EMPLOYEE USE OF TECHNOLOGY
Acceptable Use Agreement

Employee Acknowledgement and Signature

My signature below indicates that I understand and agree to abide by the guidelines according to Administrative Regulation 4040 "Employee Computer, Telephone and Network Acceptable Use."

My signature below further indicates that all of my questions and concerns regarding AR 4040 have been addressed.

_____ _____
Print Name Dept/Site

_____
Position

_____ _____
Signature Date