



CITY OF MODESTO

**ADMINISTRATIVE
DIRECTIVE**

Original Effective Date: 08/15/2000

Latest Revision Date: 05/14/2008

Policy Number: 1.17

Approved By: 
Interim City Manager

**Subject: COMPUTER USE POLICY INCLUDING INTERNET AND E-MAIL
USAGE (formerly AD 1.17, 1.18, and 1.19)**

Revised: 12/14/05; 2/17/06; 7/20/07; 5/14/08

PURPOSE:

The purpose of this policy is to implement guidelines for the appropriate use of the City's computer system including guidelines for the usage of Internet and electronic mail (e-mail).

BACKGROUND:

The computer system is made available to City staff to improve efficiency and productivity. While the City encourages the use of computer resources to improve employee efficiency and productivity, certain restrictions are necessary to avoid improprieties and ensure that established standards are met. For the purpose of this directive, a computer system is any desktop computer, laptop, palmtop, Personal Digital Assistant (PDA), etc.

To reduce potential liability, the risk of inappropriate use, and possible adverse public perceptions, City provided computer resources are to be used for official City business purposes. This includes the usage of the City's computer resources for Internet and e-mail.

City computer or information network resources shall not be used for illegal, harassing, libelous, obscene, or any other purposes, which may expose the City to liability or cause an adverse public perception. All components of the City of Modesto computer system are the property of the City and remain subject to the City's control.

EXPECTATION OF PRIVACY:

The computer system is provided to conduct City business. As such, City employees shall have no right or expectation of privacy or confidentiality in any activity using City computer systems, equipment, or networks.

The City has the ability to monitor and record all computer usage, including Internet and e-mail. The City reserves the right to filter web and email content for business purposes. Department Directors have the right to authorize the review of an employee's computer usage at any time for any reason. The City reserves the right to inspect any and all files stored in private areas of the City's network to assure compliance with this policy.

Discovery Request Procedures are as follows:

- A discovery request must be in writing to the City's Chief Information Officer.

- Requests must be approved by the Department Director of the employee for whom discovery is requested.
- Unless an alternative point of contact is listed in the memo, any information gathered in discovery will be shared with the Department Director, or designee.

Personal computer systems shall not be brought into the workplace for use in City business. Any exception to this policy must be approved by the Chief Information Officer (CIO).

PASSWORDS:

Since there is no expectation of privacy, no employee shall use a password or other means to prevent the monitoring of their computer. Password control and other means used by an employee to secure a computer or computer data outside of the methods provided by the Information Technology Department are prohibited without written permission from the CIO. Written permission shall contain the password or code necessary to unlock the computer or its data if deemed necessary by the CIO. Additional information and details are contained in the Information Technology Access Control Standards document.

ENCRYPTION INFORMATION:

Employees are prohibited from using encryption software, encrypting computer data or sending/receiving any encrypted computer data outside of the methods provided by the Information Technology Department unless the CIO grants written approval. This written approval may have a time limitation imposed on how long the employee will be allowed to use encryption technology.

DELETIONS AND ERASURES:

The California Public Records Act regulates information that is considered a public record. Employees should be aware of these requirements and the implications of deleting or modifying information stored on the City's information systems.

Under some circumstances, e-mail communications may be subject to public disclosure under the Public Records Act or through litigation. An e-mail need not be retained by the City of Modesto or City employees unless it is either (1) required to be kept by an express provision of law, or (2) necessary or convenient to the discharge of the public officer's duties and was made or retained for the purpose of preserving its informational content for future reference.

Exchange/Outlook e-mail is automatically deleted by the Information Technology Department every 30 days.

If the e-mail is either (1) required to be kept by an express provision of law, or (2) because it is necessary or convenient to the discharge of the public officer's duties and was made or retained for the purpose of preserving its informational content for future reference, then the communication must be retained for the same retention period as other documents in City departments. Disposal of an e-mail retained for the foregoing purpose may only be made after the expiration of this retention period. Since email is primarily a method for transmission of data

and not storage, any email which must be retained should be saved out of the email system and saved as a document to one of the network file systems provided.

No employee shall delete software installed on City computers or computer systems, nor shall an employee delete computer files that the employee did not author or create. Written permission from a Department Director is required to delete any other file(s) and shall be obtained before doing so. No employee shall format or delete computer storage devices without written permission from the Department Director.

REMOTE CONTROL:

Outside of Information Technology Department employees performing work related duties, no employee shall remotely control another computer, either inside or outside the city network. No employee shall be in control of more than one computer or computer system without written permission from a Department Director.

Inbound Internet connections to City computers are forbidden unless these connections employ an approved virtual private network (VPN) connection. Any inbound remote control session for technical support or any other reason must be approved in advance by Information Technology and the connection monitored by an IT staff member. At the end of the remote control session the connection must be terminated and any non-standard remote control software removed.

AUTOMATIC DEVICE SYNCHRONIZATION:

Systems that automatically exchange data between devices, such as a personal digital assistant (PDA) and a personal computer, may not be enabled unless the systems have been evaluated and approved by the Information Technology Department.

TOOLS TO COMPROMISE SYSTEMS SECURITY

Unless specifically authorized by the Chief Information Officer, City employees may not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise information systems security, passwords, identify security vulnerabilities or decrypt encrypted files.

LOGIN RESTRICTIONS:

No employee shall take control of another computer or login to any computer using another person's identity or a fictitious identity. No employee shall use the login of another employee, nor shall an employee reveal his/her login information or that of another employee. Passwords shared with an Information Technology Department technician for troubleshooting shall be changed after the technician has completed their work. No employee shall allow another person to use his/her login information to gain access to a City of Modesto computer or computer system. Additional information and details are contained in the Information Technology Security Policy document.

COMPUTER USES:

Unless authorized in writing by a Department Director, all computer activities should be directly related to City business. If an employee has a question regarding whether an activity is

permitted, he/she shall get the permission of his/her Department Director before proceeding with the activity.

City employees must conduct themselves honestly, appropriately, and in a professional manner on the computer. All existing City policies apply to an employee's conduct on the computer, including, but not limited to, those that deal with privacy, misuse of City property, harassment, information and data security and confidentiality.

Note: Attachment A provides examples of permitted and prohibited uses of the City computer system. This list is not exhaustive. Common sense and good judgment should be used in determining whether the user is engaging in an activity that violates this policy. If there is concern or doubt, contact the Information Technology Department.

APPROVED NON-BUSINESS USAGE:

During business hours, computer usage is for business-related purposes only. With written approval of a Department Director (Attachment B), employees may use the computer system for non-business purposes during unpaid meal periods or outside their normal business hours. In these instances, the employee uses the system at his/her own risk with no right or expectation of privacy or confidentiality and provided the remaining provisions of this policy are not violated.

CHANGES TO APPLICATION SOFTWARE:

The City has a standard list of permissible software packages that users can run on City computers. Workers must not install other software packages on City computers without obtaining advance permission from the Information Technology department. Workers must not permit automatic software installation routines to be run on City computers unless these routines have been approved by the Information Technology. Unless separate arrangements are made with Information Technology, upgrades to authorized software will be downloaded to City computers by Information Technology technical staff.

Employees may not load, transfer, or store any software, hardware, or other products on the City's network. The Information Technology Department has the responsibility for performing these tasks and should be contacted to address such needs.

Unapproved software may be removed without advance notice to the involved worker.

CHANGES TO OPERATING SYSTEM CONFIGURATIONS:

On City-supplied computer hardware, employees or unauthorized persons shall not change operating system configurations, upgrade existing operating systems, or install new operating systems. If such changes are required, they must be performed by Information Technology Help Desk personnel, in person or with remote system maintenance software.

CHANGES TO HARDWARE:

Computer equipment supplied by the City must not be altered or added to in any way without the prior knowledge of and authorization from the CIO.

ARCHIVAL COPIES:

All personal computer software that is not standard City software must be copied prior to its initial usage, and such copies must be stored in a safe and secure location. These master copies, including the media issued by the vendor, must not be used for ordinary business activities, but must be reserved for recovery from virus infections, hard disk crashes and other computer problems. Documentation about the licenses for such software must be retained to get technical support, qualify for upgrade discounts and verify the legal validity of the licenses.

USB Devices

USB memory devices provide easily accessible storage of data including files, pictures, reports etc. Because of its convenient small physical size and large logical size, large amounts of data can be stored to a USB. While the most common examples include USB memory sticks or “jump drives”, many other devices are capable of storing data files such as IPODs, Digital Cameras, MP3 players, mobile phones, etc. and are subject to this directive.

If any USB stored data is confidential, it becomes a risk and legal liability in the event the media is lost. Confidential data is not authorized to be copied to a USB Device. This includes data that could be used to personally identify city staff, other agency employees or citizens. Any loss of a USB memory device with suspected confidential data must immediately be reported directly to the CIO.

COPYRIGHT PROTECTION:

Making unauthorized copies of licensed and copyrighted software, even for “evaluation” purposes, is forbidden. City of Modesto permits reproduction of copyrighted materials only to the extent legally considered fair use or with the permission of the author or owner. If employees have any questions about the relevance of copyright laws, they should contact City legal counsel. Unless they receive information to the contrary, employees should assume that software and other materials are copyrighted.

E-MAIL AND INSTANT MESSAGING:

The purpose of e-mail is to communicate between individuals and groups and to promote the effective and efficient use of time and resources in order to carry out the business of the City.

The City e-mail system is to be used for official City purposes. However, limited personal use is permitted that is reasonable and does not interfere with the employee’s performance of duties and responsibilities. During business hours, computer usage is for business-related purposes only. With approval of the Department Director, employees may use the computer system for non-business purposes during unpaid meal periods or outside their normal business hours. For example, the incidental use of e-mail to communicate with employees in another department that may contain non-City related matters (such as asking what that employee is doing for lunch) is permitted. In all cases, however, the employee uses the system at his/her own risk, with no right or expectation of privacy or confidentiality and provided that the remaining provisions of this policy are not violated.

1. In drafting any e-mail the employee should exercise care and diligence as the e-mail reflects on the City and the employee's department. An employee should always conduct himself/herself in a professional manner and should never send anything by way of e-mail, which could not appear in a memo or letter.
2. City email accounts and addresses are for official city use only. These accounts and addresses shall not be used for personal transactions. (i.e.: personal email, list serves, on-line chat rooms, etc).
3. An employee shall use no more than one e-mail system, e-mail software, or e-mail provider when using a City of Modesto computer or computer system. The City has the ability to restrict access to outside messaging systems at its discretion. The one e-mail system is controlled and operated by the City of Modesto, and shall be from no other source. Any variance from this requires written permission from the employee's Department Director in consultation with the Information Technology Department.
4. E-mail may be used only for incidental employee association communication or for communicating with City management regarding association-City business. Bargaining unit-wide communications; distribution of association newsletters or other documents; or association debates, discussions, or endorsements are prohibited on City e-mail.

The City of Modesto has chosen not to adopt Instant Messaging as an approved communication method due to the relatively high security risks inherent in current Instant Messaging applications. Any use of Instant Messaging from City systems or within the City network is subject to written approval by the Chief Information Officer

Data & File Storage

Employees must not download, access, save or store files on city computer systems that are not work related. Examples include, but are not limited to, the storage of personal and/or copyrighted material such as is frequently contained in picture, video and audio files. Intermittent searches for audio (MP3, WMA, M4P, etc) files and audio (MOV, MPEG, MPG, etc) files will be conducted by the Information Technology Department. Users having directories found to contain possible copyrighted or personal multimedia files will be contacted via their supervisors, prior to deletion. The use of the Internet for recreational streaming (internet radio stations, YouTube, XM Radio, etc) is prohibited without Department Head approval.

REPORTING PROBLEMS:

Users must promptly report all information security alerts, warnings and suspected vulnerabilities to the Information Technology Help Desk. Users should not use City systems to forward such information to other users, whether the users are internal or external to the City.

VIOLATIONS:

Any employee violating this policy may have his/her computer access restricted or revoked. Further, an employee violating this policy may be subject to formal disciplinary action up to and including termination from City employment.

ACKNOWLEDGMENT:

Each employee is required to sign an acknowledgement form for this Administrative Directive. This acknowledgement is filed in the employee's personnel file.

ACKNOWLEDGMENT

This is to acknowledge that I have received and read the Administrative Directive 1.17 entitled “Computer Use Policy Including Internet and E-Mail Usage.”

I understand that failure to follow the provisions of this Directive may lead to disciplinary action up to and including termination. I further acknowledge that this document will be placed in my Personnel file.

(supervisor signature)

(employee signature)

(print name)

(print name)

(date)

(date)

ATTACHMENT A
(this is not intended as an complete listing)

EXAMPLES OF APPROPRIATE/PERMITTED COMPUTER, E-MAIL, INTERNET USAGE:

- Preparing or distributing documents for City business (e.g. memos, letters, etc)
- Storing City business documents or files
- Preparing or storing general announcements within the scope of the employee's job responsibilities (e.g. city sponsored events, etc)
- Use of City e-mail address for business related subscriptions
- Obtaining information regarding City business (e.g. policy, legislation, public meetings, technical research, etc.)
- Transmitting a document or file (in conjunction with an e-mail) provided the document or e-mail does not contain confidential information (e.g. attorney/client privilege; personnel information)
- Preparing or providing information regarding City business to the public (e.g. City Council meeting agendas or minutes, key points of contact, etc.)

EXAMPLES OF INAPPROPRIATE/PROHIBITED COMPUTER, E-MAIL, INTERNET USAGE:

- Generating, sending, requesting, displaying, playing, archiving, or storing any material in any form (e.g. text or graphics) containing comments or images that are discriminatory, offensive, defamatory or harassing in nature
- Displaying, playing, transmitting, archiving, or storing sensitive or offensive material on individual workstations which may result in a perceived "hostile environment" to coworkers
- Violating software licensing laws
- Conducting personal business from the City's computer systems such as creating documents or transmitting/receiving communications related to an employee's commercial business or outside employment. Examples of prohibited use include, but are not limited to: E-Bay postings or transactions; Avon, Tupperware, Amway, real estate, insurance, consulting, academic instruction, building contracting, or any other commercial business communications/transactions, related to an employee's commercial business, their self-employment, or their outside employment.
- Illegal activities (e.g. gambling, placing wagers or bets, bidding, etc.)
- Copyright infringement (3rd Party Liability) involving copyright or intellectual property violations for unauthorized display or use of protected information
- Committing acts of fraud, waste or abuse through computer related activities
- Visiting inappropriate sites.

- Transmitting any City sensitive or confidential information over the Internet (e.g. unauthorized dissemination of city credit card or other financial information)
- Logging on to the Internet and leaving it running all day, unless necessary for a business-related purpose (e.g. logging on to NASDAQ and checking stocks throughout the day; using a certain website as wallpaper, etc.)
- E-mails or messages advertising or notifying of personal sale items.
- E-mails or messages of a political nature or having to do with political activities or endorsements.
- E-mails or messages of a fundraising nature or having to do with non-city sponsored charity efforts.
- E-mailing or downloading large file items, such as but not limited to E-Books, Music files, video files, and streaming files. Exceptions to this rule must be approved by an employee's Department Director or designee.
- E-mailing formal or informal corrective, disciplinary, or other personnel actions sent to the subject of the action
- Creating e-mail messages purporting to be from another person without their permission
- Obtaining e-mail subscriptions for non-business activities (e.g. Joke of the Day Club, etc)
- Sending mass e-mail messages without approval of supervisor or Department Director (e.g. "Staff" messages)

ATTACHMENT B

City of Modesto
Interoffice Memorandum

To: Appropriate Department Director

Through:

From:

Date:

Subject: Non-Business Use Request

As required by City policy, I request permission to use the City-owned computer system for non-business use. I have read and agree to abide by the City's Administrative Directive No. 1.17, "Computer Use Policy including Internet and E-Mail Usage."

I understand that with my Department Director's approval, I may use the computer for non-business purposes during unpaid meal periods or outside normal business hours.

I understand the e-mail system is for City use only. However, limited personal use is permitted that is reasonable and does not interfere with the performance of my duties and responsibilities.

I understand that the incidental use of e-mail to communicate with employees in another department that may contain non-City related matters (such as asking about lunch plans) is permitted.

I understand that I shall have no right or expectation of privacy or confidentiality in any activity while using City computing systems, equipment, or networks.

I understand that failure to follow the provisions of said policies could lead to disciplinary action up to and including termination. I further acknowledge that this document will be placed in my personnel file.

Department Head signature

Employee signature

print name

print name

date approved

date signed

cc: Personnel