CITY OF CLOVIS

# MEMORANDUM

DATE: December 13, 2010

TO: All Users of City Technology Resources

FROM: Rob Woolley, Interim City Manager

SUBJECT: Updated Technology Users Policy and Agreement

As technology advances it has become necessary for the City to update its Technology Users Policy and Agreement. The attached replaces Administrative Memorandum 00-01 to include text messaging systems and cellular phones as Technology Resources. The section addressing Electronic Mail (email) has been expanded to provide clear guidelines regarding email record retention and classification of public records. The policy has been updated to address social networking technologies such as Facebook. Finally, the policy has been reformatted to make the policy easier to read.

This updated policy is being provided to you as a user of City technology resources. As a user of these resources you will need to read and retain the attached policy. You also need to read, sign and return the Technology Users Agreement to Personnel/Risk Management.

If you have any questions concerning the attached policy contact Jesse Velez, Information Technology Manager at ext. 2188.

# CITY OF CLOVIS
# TECHNOLOGY USERS POLICY AND AGREEMENT

## A. INTRODUCTION, PURPOSE, AND DEFINITION OF TECHNOLOGY RESOURCES.

1. Purpose. This Policy and Agreement ("Policy") is designed to provide employees with definitive guidelines of acceptable and unacceptable use of Technology Resources for the protection of both employees and the City.

2. Technology Resources Defined. For purposes of this Policy "Technology Resources" includes, but is not limited to, City provided hardware and software, including computers, Voice over Internet Protocol (VoIP) Phones, e-mail, text messaging systems, cellular phones and Internet connection tools.

NOTE: There may be restrictions on using personally provided technology equipment for City business, whether at the work site or from home. Employees must check with their supervisor and the Information Technology ("IT") Manager regarding the use of personal technology equipment to conduct City business.

3. Violation of Policy. The right to use Technology Resources is a revocable privilege and a failure to comply with this Policy may result in loss of access to some or all Technology Resources. In addition, the individual may be subject to disciplinary action, up to and including termination for misuse of Technology Resources. .

4. Questions. If employees have any questions or need clarification regarding any provision of this Policy and Agreement, they shall contact the City Clerk at Ext. 2070 or the IT Manager at Ext. 2188.

## B. TECHNOLOGY USERS AGREEMENT.

For the purposes of this Policy, employees who use Technology Resources shall be defined as Technology Users ("Users"). The Technology Users Agreement ("Agreement") attached to this Policy shall be signed prior to all new employees, volunteers, contractors, or vendors utilizing Technology Resources. Employees currently using Technology Resources (Users who currently have a login and password) will be required to sign the Agreement within fifteen (15) days of receipt of this Policy or risk the loss of access privileges.

## C. CONFIDENTIALITY AND PRIVACY.

1. Privacy. There is no expectation of personal privacy in any use of Technology Resources, including personal e-mail, text messages, and voice messages. The City regularly monitors technology use and reserves the right to monitor all e-mail, computer transmissions, IP Phone recordings, messages (voice and data), information stored on

City-owned equipment including text messages, or created or received by City employees with the City's Technology Resources. Technology Resources are monitored to protect the public interest by ensuring that they are operating efficiently and are not misused or mismanaged.

2. City Records. All computer applications, programs, and work-related information, created or stored by employees on Technology Resources, are City property and may be public record.

3. Permissions and Accessibility Rights. The City reserves the right to set permissions and accessibility rights to all City technology resources as necessary. Rules prohibiting theft or vandalism apply to software and data as well as to physical equipment. All software, data, reports, messages (voice and data) and information stored on local and network hard drives, as well as other products created using the Technology Resources, are the property of the City of Clovis and access to them may not be obtained without prior authorization by the user/creator or the City Manager or designee.

4. Confidentiality. Most communication among City employees is not considered confidential. However, certain communications, such as police investigations, employees records, and communications with the City Attorney's office or other attorneys representing the City, may be confidential or contain confidential information. Questions about whether communications are confidential should be raised with the employee's supervisor.

a. Confidential information must be stored and transmitted in the confines of a secured network drive or folder.

b. Employees shall exercise caution in sending confidential information on the e-mail system given the ease with which such information may be retransmitted.

c. Confidential information may not be transmitted to individuals or entities not authorized to receive that information nor to other City employees not directly involved with the specific matter.

d. Employees shall exercise caution to ensure information is not inadvertently sent to unintended recipients. In particular, exercise care when using distribution lists to make sure all addressees are appropriate recipients of the information.

**D. SECURITY - USER ID.**

1. User ID. Each User shall have a unique identity, referred to as a "User-ID", protected by a "password" in order to gain access to the system. The User ID identifies a User in various system activities, provides access to certain software and data that is based on his/her department-established authorization, and associates his/her own software and data with his/her identity.

2. Passwords. Users shall use passwords associated with a particular City information system only on that system.
When setting up an account on a different information system that will be accessed using the Internet or other on-line service, choose a password that is different from the ones used on City information systems. Do not use the same password for both local and remote systems accessed via the Internet or another on-line service. Passwords should not be so obvious so that others could easily guess them. Passwords must be changed every sixty (60) days.

3. Employee Responsibility. An employee's password and User-ID are unique, identifying him/her as the user accessing a particular workstation or PC. The employee is responsible for any modifications or access to system information made using his/her User-ID. Every change to technology information is logged with the identification of the person who signed on. Users shall not share passwords and no PC, terminal, or workstation shall be left unattended while logged on (i.e. Users should either logoff or lock their workstations). Users should be aware that merely turning a PC off does not always log the user off the system. Users needing assistance with logging off procedures or locking their workstation should contact the I.T. Division at Ext. 2150.

4. Terminating Sessions. Users shall log off or execute an alternate termination procedure when finished using any technology system or program, especially the Internet and other external technology systems. This will help prevent a potential breach of security.

5. Unencrypted E-Mail. Unencrypted e- mail sent or received on Technology Resources cannot be expected to be secure. Users should always be aware that the sender has no control over what the recipient does with the message and that the message may be sent to the wrong address or intercepted by hackers.

**E. INTERNET.**

1. Use. The use of the Internet is provided to City employees as a tool to assist employees in performing official duties. Use of the Internet shall follow generally accepted business practices and current laws.

2. Content and Monitoring. The City has no control over the content of messages or information postings on external Internet sites. The City reserves the right to monitor Internet sites visited by employees. The City also reserves the right to use available technology to screen out inappropriate and offensive information. This technology cannot block all sites that may contain inappropriate/offensive material.

**F. E-MAIL.**

1. Use. The City's e-mail system is provided to City employees as a tool to assist employees in performing official duties. Incidental and occasional personal use is

permitted within the City, but such messages will be treated the same as other messages.

2. Privacy. Users should not expect or assume any personal privacy regarding the content of electronic mail communications, including personal e-mails. Employees who make incidental use of the e-mail system for personal e-mails should not expect the content to be protected from review or deletion by the City.

3. Monitoring. The City reserves the right to access and use the contents of all messages sent over e-mail systems, including e-mail sent using the City's Technology Resources and messages sent over the Internet.

4. Work Related Announcements. General interest work-related announcements should be posted to the "City Information Bulletin Board" known as the Clovis Chalkboard, not sent to individual addresses or mailing lists.

5. Medium of Communication. It is the City's policy that City e-mails and e-mail systems are intended to be a medium of communication. Routine e-mail messages are comparable to telephonic communications and are not intended to be retained in the ordinary course of City business. The informational content of such communications is neither necessary nor intended to be preserved for future City use or reference. Each user shall delete messages from folders within the e-mail system on a rolling sixty (60) day schedule. This includes items in "received" and "sent" folders as well as any folders set up by individual users. Messages the user wishes to retain shall be filed elsewhere. Messages older than 90 calendar days will also be purged regularly by the City's IT Division. An e-mail is considered destroyed as soon as it has been deleted from a user's mailbox, even though it is temporarily stored in the trash folder before being purged from the e-mail system.

6. Records. City e-mail systems are not intended to be, and shall not be used for, the electronic storage or maintenance of City records. Upon removal from the e-mail system, the messages will be disposed of in the City's ordinary course of business. However, until removed, e-mails will constitute public records and may be discloseable under specified circumstances. In addition, certain e-mails will have to be retained as set forth in the City's Records Retention Policy.

The following guidelines apply:

a. E-mail messages and attachments comparable to hard copy documents that would be retained under the Records Retention Policy must be printed in hardcopy or converted to the appropriate electronic format and retained for the required time period as outlined in the Records Retention Policy.

b. It is the responsibility of individual employees and their department heads to determine if an e-mail is an official City record that must be retained in accordance with the City's Record Retention Policy. The City Clerk will assist you in making such a

determination. You should keep in mind, however, that preliminary drafts, notes or interagency or intra-agency memoranda, which are not retained by the City in the ordinary course of business are generally not considered to be official City records subject to retention or disclosure. Generally, the City employee who sends the e-mail should be the person responsible for printing and filing it accordingly, but persons responsible for a particular program or project file shall be responsible for retaining all e-mail they send or receive related to that program or project.

c. Any e-mail messages that relate to a claim or a potential claim against the City must be preserved. Likewise, any e-mail messages that may relate to a lawsuit filed against the City, even if a subpoena or court order for such e-mail messages has not yet been issue, must be preserved. The City has a duty to preserve any relevant data when there is even a hint of possible litigation. Therefore, when City employees become aware of a potential claim, an actual claim, or a lawsuit against the City, they must preserve any e-mail messages and attachments that have any information relevant to that matter. Your department head can provide you with guidance on these issues.

d. The City receives requests for inspection or production of documents pursuant to the Public Records Act, as well as demands by subpoena or court order for documents. In the event a records request or court-issued demand is made for e-mail, the employees having control over such e-mail, once they become aware of the request or demand, shall use their best efforts, by any responsible means available to temporarily preserve any e-mail which is in existence until it is determined whether such e-mail is subject to preservation, public inspection, or disclosure

## G. COMPUTER SOFTWARE.

1. Registration. Each piece of proprietary software operating on a City computer must have valid registration or be covered by a user's license. Proprietary software and associated documentation are subject to copyright laws and licensing agreements, and are not to be reproduced unless authorized under a licensing agreement. Appropriate documentation to substantiate the legitimacy of the software is necessary. Employees shall not use unauthorized software on City Technology Resources.

2. Personal Software. Personally owned software, including games, screen savers and shareware, shall not be installed or copied to City-owned hardware.

3. Inspection. Any software obtained from a source other than the City IS Division must be checked for viruses prior to use.

4. Modification. Users shall not attempt to modify City-owned or licensed software or data files without prior written approval by the City Manager or designee.

## H. RULES GOVERNING USE OF TECHNOLOGY RESOURCES.

1. Use of Hardware, Software, Subscription Services, Chat Services, Social Networking, and Similar.

a. Users shall not copy any City-owned or licensed software or data to another technology system for personal or external use.

b. Users shall not install or use non City-owned hardware with Technology Resources without prior authorization from the IT Manager or designee.

c. Users shall not take or use City-owned hardware for use at home without prior authorization from the City Manager or designee.

d. Users shall not install free, purchased, fee-based or subscription on-line services, e-mail software, Internet services, etc. without prior approval by the City Manager or designee.

e. Users shall not use "chat services" such as ICQ, AOL-Instant Messenger, Yahoo-Pager, etc., and these are not to be installed or used on Technology Resources.

f. Users shall not use "social networking" services such as MySpace, Twitter, Facebook etc., unless the use of such services is to support the mission of the Department and/or City.

g. Users shall not download music, whether free or for purchase, with or on Technology Resources. Users shall not use streaming music players on Technology Resources.

2. Confidential Reports. User shall not intentionally seek out information on, obtain copies of, modify, or divulge files, reports, and other data, which is private, confidential or not open to public inspection, or release such information unless specifically authorized to do so when the legal conditions for release are satisfied.

3. Copying and Printing. Users shall not intentionally copy or print any software, electronic file, program or data without a prior, good faith determination that such copying or printing is, in fact, permissible. Any efforts to obtain permission shall be documented.

4. Authority, Passwords and Identity. Users shall not:

a. Intentionally seek information on, obtain copies of, or modify files or data without proper authorization. Seeking passwords of others, or the exchange of passwords, is prohibited.

b. Intentionally represent themselves electronically as another user, either on the City network or on the Internet or other on-line services, unless explicitly authorized to do so by the City Manager or designee. Users shall not circumvent established policies defining eligibility for access to information or systems.

c. Allow an unauthorized individual to use the User's identity or use another person's User ID, even if they are City employees, volunteers, or contractors.

5. Disruption of Operations. Users shall not:

a. Intentionally develop programs designed to infiltrate a technology or computing system, and/or damage or alter software components or hardware.

b. Attempt to damage or disrupt the operation of Technology Resources or telecommunication equipment lines.

6. Acceptable Uses. The following is a non-exclusive representative list of acceptable uses for Technology Resources:

a. Communication and information exchange directly related to the City or Department mission and objectives and/or to the User's work tasks.

b. Communication and exchange of information for professional development, to obtain training or education, or to discuss issues related to the User's official job duties.

c. Use in applying for, or administering, grants or contracts for City programs.

d. Use to obtain advisory information, standards, research data, analysis, and professional society activities related to official job duties.

e. Obtaining announcements and/or tracking of new laws, procedures, policies, rules, services, programs, information, or activities.

f. Use of governmental administrative communications not requiring a high level of security.

g. For City-related business, communication with professional associations, public agencies, universities, research, and/or continuing education.

7. Unacceptable Uses. The following is a non-exclusive representative list of unacceptable uses for Technology Resources:

a. Use for any purpose that violates local, State or Federal laws or regulations, including, for example, downloading or distributing pirated software or data.

b. Deliberately generating and/or disseminating any virus or any other destructive programming, or experimenting with malicious computer code, such as worms and viruses.

c. Use for purposes not directly related to the mission or work tasks of the User's department during normal business hours.

d. Use for private business, including commercial advertising, and sending or replying to "chain letters." Use of City computing resources for external consulting is prohibited.

e. Use for any for-profit activities.

f. Accessing, sending, or soliciting sexually oriented messages or images.

g. Libelous, offensive, or harassing statements, including disparagement of others based on their race, national origin, sex, sexual orientation, age, disability, religious, political beliefs, veteran's status, family status or union affiliation.

h. Use for access to, and distribution of, games. Use of Internet based games is also prohibited.

i. Use that interferes with, or disrupts, network users, services, or equipment.

j. Use for fund raising, partisan politics, or public relations activities outside of the User's official duties.

## I. USE BY CONTRACTORS, VOLUNTEERS, AND OTHER NON-EMPLOYEES.

Contractors, volunteers, and other non- employees may be granted access to the Technology Resources at the discretion of the City Manager or designee. Employees shall ask the department head to contact the City Manager or designee when this type of access is required. Contractors, volunteers, and other non-City employees use is subject to the same policies and guidelines as any User and these individuals shall review and sign the Technology Users Agreement.

## J. ETIQUETTE.

1. Generally Accepted Standards. Users must follow generally accepted etiquette of e-mail, the Internet, and other on-line services. Users must avoid uses that reflect poorly on their Department, the City, or government in general.

2. City Representation. The public may perceive a User's postings and e-mail as official City policy. When using e-mail, the Internet, and other on-line services provided by the City, Users should remember that they represent the City. Users shall avoid making statements of personal opinion that may be misinterpreted as official City policy.

Users must recognize that anything they put in writing may become a public record, regardless of the original intent of the message.

3. Relationship With Others. Users must respect the rights of other Users and the Public. Users shall not use Technology Resources to invade the privacy of another person, ascertain confidential information, or abuse or harass another person.

4. Ethical Rules and Regulations. Existing and evolving rules, regulations, and guidelines on ethical behavior of government employees and the appropriate use of government resources apply to the use of Technology Resources.

**CITY OF CLOVIS**
**TECHNOLOGY USERS POLICY**

## Technology Users Agreement

I, the undersigned, have received and read a copy of Administrative Memorandum #00-01 (as revised October 2010), Technology Users Policy and Agreement.

I understand I have no expectation of privacy regarding my use of Technology Resources, including Internet access, e-mail, text message, IP Phones, or cellular phone records on City issued equipment. I understand that messages transmitted over the City's computer network on the Internet and e-mail, as well as my use of all computer files, should be City business-related and that the City's security software may record for management use the Internet address of any site that I visit and keep a record of any network activity in which I transmit or receive any kind of file or message.

I further acknowledge that all e-mail messages, cellular phone records on City issued equipment and files are the property of the City of Clovis and may be subject to record retention laws and the California Public Records Act. The City reserves the right to access, audit, and disclose, for whatever reason or purpose, all computer files or messages sent through or in storage on the City's computer system or maintained by third-party carriers as applied to City issued cellular phones.

I recognize that the law and associated policy regarding the use of Technology Resources are continually evolving. Therefore, I understand that my regular review of the City policies is required. I agree to abide by and adhere to this Technology Users Policy and understand that failure to comply with this Policy may result in disciplinary actions, up to and including termination.

| | |
|---|---|
| _____ | _____ |
| Employee Signature | Date |
| _____ | _____ |
| Print Employee Name | Print Employee ID Number |
| _____ | _____ |
| Print Department and Division | Print Name of Supervisor |
| _____ | _____ |
| Witness Signature | Date |
| _____ | _____ |
| Print Witness Name | Title |