

CITY OF EUREKA

Category: ADMINISTRATION

POLICIES & PROCEDURES

Subject: Use of Office
Communication Equipment

Date Adopted: February
24, 2004

File
Number 1.75

PURPOSE

To establish guidelines for the proper use of electronic equipment, systems and/or tools provided by the City of Eureka to its employees, elected officials and volunteers for the purpose of performing job functions including communication, information exchange and research.

DEFINITIONS

Office communication equipment is office equipment used as a basis for communication or data processing, conveyance or storage, including but not limited to, telephone, cellular phone, pager, voice mail, fax machine, copy machine, office automation equipment (computer terminals, personal computers or laptops, including electronic mail and calendar, internet access, network equipment), etc. As used herein, office communication equipment includes any other equipment or devices the City may choose to utilize in the future for the purposes stated above.

Employee is described as any employee, elected official, volunteer or other agent (including authorized consultant and contractor) of the City of Eureka.

POLICY

This policy will be provided to all office communication equipment users.

All office communication equipment provided by the City of Eureka is the property of the City and is provided for official business use only. Personal use of telephone equipment should be kept to a minimum and the City must be reimbursed for any additional charges incurred for personal phone calls (i.e. long distance charges or local cell phone calls).

Employees who use office communication equipment provided by the City of Eureka have no expectation of privacy in any uses of such equipment, except as specifically provided by law. Under the Public Records Act, internet and e-mail records may be subject to public disclosure. In addition, supervisors have the authority to inspect the contents of any office communication equipment, file(s), calendars or electronic mail of their subordinates in the normal course of their supervisory responsibilities. Information Services staff shall extract information, files, documents, voice mail, electronic mail, etc when requested by authorized supervisory personnel. Additionally, Information Services staff will have access to all such information while troubleshooting and/or upgrading hardware and/or software. Reasons for review include: system, hardware or software problems, general system failure, a lawsuit against the City, suspicion of a crime or violation of policy, or a need to perform work or provide a service when the employee is unavailable.

Uses of Office Communication Equipment

Office communication equipment is provided for the purpose of conducting business for the City of Eureka.

- A. Allowable uses of office communication equipment include the following, to the extent these uses are for the purpose of conducting City business:
 1. To facilitate performance of job functions
 2. To facilitate the communication of information in a timely manner
 3. To coordinate meetings of individuals, locations and City resources

CITY OF EUREKA

Category: ADMINISTRATION

POLICIES & PROCEDURES

Subject: Use of Office
Communication Equipment

Date Adopted: February
24, 2004

File
Number 1.75

4. To communicate with departments throughout the City
 5. To communicate with outside organizations, agencies and individuals as required in order to perform an employee's job functions
- B. Prohibited uses of office communication equipment include, but are not limited to, the following:
1. Illegal activities
 2. City policy violation, including but not limited to violations of the City's Zero Tolerance Against Harassment Policy and/or the Policy for Prevention of Violence in the Workplace.
 3. Slander
 4. Defamation
 5. Political endorsements
 6. Commercial activities
 7. Using non-business software including games or entertainment software during business hours
 8. Use of hardware or software not authorized by Information Services staff

Internet Access

Use of the internet is becoming increasingly necessary for City employees to provide superior customer service. The efficient utilization of the internet for communications and research can improve the quality, productivity, and general cost effectiveness of the City's work force.

Internet access is provided to City employees to encourage and facilitate research and information exchange in the performance of City business. Employees are encouraged to use the internet as much as necessary to perform their job and/or promote effectiveness. However, employees may not 'surf the net' on City time. Employees may use City equipment to conduct personal research on the internet during non-work hours only, and only after receiving approval from their supervisor.

Users are encouraged to develop uses which meet the individual needs of their job and which take advantage of the internet's functions.

- A. Acceptable uses of the internet include the following, to the extent these uses support reference, research and communication within and outside the City and are for the purpose of conducting City business:
1. To facilitate performance of job functions
 2. To facilitate the communication of information in a timely manner
 3. To communicate with departments throughout the City
 4. To communicate with outside organizations, agencies and individuals as required in order to perform an employee's job functions
- B. Unacceptable uses of the City's internet access during working and non-working hours include, but are not limited to, the following:
1. Violation of laws or City policy, including but not limited to privacy issues.
 2. Using profanity, obscenity, or any other language which may be offensive to

CITY OF EUREKA

Category: ADMINISTRATION

POLICIES & PROCEDURES

Subject: Use of Office
Communication Equipment

Date Adopted: February
24, 2004

File
Number 1.75

another user.

3. Re-posting personal communications without the author's prior consent.
4. Copying commercial software in violation of copyright law.
5. Using the network for financial gain or for any commercial or illegal activity.
6. Using the internet in such a manner as to create a security breach through the introduction of computer viruses or through the provision of information which might permit unauthorized access to the system. Deliberate attempts to degrade or disrupt system performance will be viewed as criminal activity under applicable state and federal law.

Internet users are responsible for learning proper techniques and standards for participation and for understanding that if they misuse the internet, they will lose their privilege to use the City's account(s) and may incur administrative or legal penalties.

Privacy

Email communication, information access on the internet and data on computers/networks utilized by the City is not considered personal or private material, but is considered the business property of the City. **Users are given no expectation of privacy as discussed on Page 1 of this policy.**

The City retains the right to examine, without notice, all electronic communications systems, electronic storage media, data files, logs, and programs used in conjunction with the City's computer equipment.

It is **not** the policy of the City of Eureka to regularly monitor the content of email and internet access, but the content can be monitored and the usage of electronic communications systems **will** be monitored to support operational, maintenance, auditing, security and investigative activities.

Users are not to violate the privacy of others. Users are not to attempt to gain access to the computer systems, data files or directories of another user or department without specific authorization to do so. Users are not to attempt to intercept or otherwise monitor any network communications not explicitly directed to them.

Security

With the increasing reliance upon the City's computer network to maintain the City's critical and sensitive data, communicate with outside sources and to do research on the internet, and with the continuing evolution of security threats such as viruses and worms which may damage the network or destroy data, or worse, penetrate the network and steal sensitive data, it has become more important than ever to provide a secure and reliable environment for the local users to accomplish their assigned tasks. This does require the user be diligent about keeping their desktop computers, laptops and data secure from all possible sources of harm, destruction or loss of sensitive data.

Users must

- Maintain username/password security by
 - ◇ Creating a unique password every 60 days.
 - ◇ Creating a password which is a minimum of 6 characters
 - ◇ Creating a password which is a combination of alpha and numeric characters and

CITY OF EUREKA

Category: ADMINISTRATION

POLICIES & PROCEDURES

Subject: Use of Office
Communication Equipment

Date Adopted: February
24, 2004

File
Number 1.75

which is not a word found in the dictionary.

- ◇ Never disclosing username and password to another person
- Password protect their screensaver so their data will be secure if they have to walk away from their workstation for a period of time.
- Shut off their computers when they leave for the night

Users are not to interfere with the integrity of any network or computer system, by:

- Use of another's username and password
- Disclosing username and password to another person
- Impersonation of other individuals in email
- Attempts to capture others' passwords or data
- Loading any software on their computer without the knowledge of the Information Services Division of the Finance Department
- Intentional introduction of contaminants of any kind, such as a computer virus or worm
- Destruction or alteration of data or programs

Users should report to their Department Head or Information Services whenever they suspect a virus has infected a system.

Users should report suspected security violations to their Department Head.

Violations

If users violate the City's "Use of Office Communications Equipment" policy, they may be subject to disciplinary sanctions up to and including dismissal from City of Eureka employment or termination of City contracts, as appropriate.

If users commit a computer crime by illegally using the City of Eureka computer systems or data network, they may be charged with a felony which is punishable by a fine not exceeding ten thousand dollars (\$10,000) or by imprisonment in the state prison for 16, 24, or 36 months, or by both such fine and imprisonment; or charged with a misdemeanor which is punishable by a fine not exceeding five thousand dollars (\$5,000), or by imprisonment in the county jail not exceeding one year, or by both such fine and imprisonment. (See Appendix for excerpts from California Penal Code Section 502.)

CITY OF EUREKA

Category: ADMINISTRATION

POLICIES & PROCEDURES

Subject: Use of Office
Communication Equipment

Date Adopted: February
24, 2004

File
Number 1.75

The following is included for informational purposes only.

INTERNET ETIQUETTE

1. Compose longer email and bulletins off line (as word processing documents) in order to reduce editing frustrations and unnecessary network traffic.
2. Make your "subject line" as descriptive as possible.
3. A salutation after your "subject line" and before your message can be used to convey a sense of personal acknowledgment.
4. Appending your name at the end of the message is also considered good etiquette.
5. Always restate or describe the question that you are answering or the issue on which you are commenting.
6. Always acknowledge that you have received a document or file someone has sent you.
7. Check your email once or twice a day if you are expecting replies.
8. Delete email once you have read it or save it to a local file.
9. Don't send personal messages on conferences, bulletin boards or digests. Send such messages directly to the party with whom you wish to communicate.
10. Don't expect an answer in less than 2-3 days.
11. When sending a file, give as much information as possible: length, type, contents and be considerate of other party's storage capacity which may be limited.
12. Conference and bulletin board messages are "showcases". Proofread and edit all messages, particularly when your communication can be considered an official response from the City.
13. Don't be vulgar or offensive. Electronic text allows no context clues to convey shades of irony, sarcasm, or harmless humor.
14. Don't publicly (on bulletin boards or conferences) criticize (or "flame") other users. Contact someone privately by personal email for private discussion of differences.
15. Protect the privacy of others.
16. Observe standard copyright restrictions; they are the same as for printed materials.
17. Don't upload or download software illegally. It is a serious federal crime.
18. Don't access services illegally.
19. Be careful not to spread computer viruses. Always check downloaded files.
20. Don't use capital letters as the standard form of the message. Using "all caps" is the internet

CITY OF EUREKA

Category: ADMINISTRATION

POLICIES & PROCEDURES

Subject: Use of Office
Communication Equipment

Date Adopted: February
24, 2004

File
Number 1.75

equivalent of SHOUTING!

CITY OF EUREKA

Category: ADMINISTRATION

POLICIES & PROCEDURES

Subject: Use of Office
Communication Equipment

Date Adopted: February
24, 2004

File
Number 1.75

Appendix

Computer Crime Laws

California Penal Code Section 502 states, in part, that any person is guilty of a public offense who:

1. Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either A) devise or execute any scheme or artifice to defraud, deceive, or extort, or B) wrongfully control or obtain money, property, or data.
2. Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.
3. Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.
4. Knowingly introduces any computer contaminant into any computer, computer system, or computer network.