H. COMPUTER AND ELECTRONIC COMMUNICATIONS POLICY IMPLEMENTATION

PURPOSE

The Computer and Electronic Communications Policy ("policy") outlines the policies and guidelines that must be followed at all times to minimize business risks and maximize the benefits of the use of computing and electronic communications resources owned, leased or controlled by the City of Redlands. This policy establishes standards for the acceptable use of the electronic communications systems of the City.

POLICY

1. Scope

The City owns, has a property interest in, and has a right to specify the use of:

- All information processing and communications resources used to conduct its business, including hardware: computers, laptops, fax machines, telephones, cellular phones, smart phones, tablets, printers, copiers, storage media and all other hardware; and non-physical resources, such as: software, applications, online accounts, email, texts, pings, Internet/Intranet/Extranet access, network accounts, voice mail and instant messaging files, other messages and all other non-physical assets used or stored in its offices and facilities; and,
  All such information processing and communications resources employed in its business that are connected to or able to be connected to its facilities from locations outside of the City's premises, including personal information processing, hosted services, and communications equipment and/or software owned or leased by the City or supplied to City personnel for their use.

All such resources are collectively referred to in this policy as "computing and electronic communications resources" or "resources." All other data processing hardware, software, licenses and any other physical equipment, electronic accounts, applications and / or appurtenances required to transact City business electronically not expressly mentioned above also constitute the computing and electronic communications resources at City facilities.

The Complete Policy can be found in the Personnel Roles and Regulations

PROCEDURE

Usage Rules

NO USER SHOULD HAVE AN EXPECTATION OF PRIVACY IN THE USE OF ANY CITY COMPUTING AND ELECTRONIC COMMUNICATIONS RESOURCES.

a. Ownership
The City of Redlands owns leases and has the right to specify the use of all computers and electronic communications resources. No employee has any property interest in the City's electronic communications resources.

b. Authorized Users
Full and part-time employees, elected officials, interns, volunteers, contractors and all other affiliated individuals (collectively referred to as "User" or "Users") conducting business on behalf of the City of Redlands are eligible to use computing and electronic communications resources but may do so only in accordance with this policy.

c. Acceptable Use
During an employee's designated working hours or working schedule, Users may only use City-owned computers and/or electronic communications resources to conduct City business. Examples of legitimate City business use are:

- Performing essential job functions;
- Participating in job-related conferences and discussions or collaborating via resources such as web sites, newsgroups, chats, and bulletin boards;
- Performing research, obtaining information or support, or pursuing approved job-related education
- Promoting and communicating City business or related information.

Usage must also comply with any and all other terms established by the Personnel Rules and Regulations.

Employees requiring remote access to City systems and data will be given access using a virtual private network (VPN) established by the City's Division of Innovation and Technology. VPN connections will only be installed after written authorization from the employee's department head and only on City-owned computing equipment. No requests to use personal devices will be granted.

d. Personal Use
The City understands that personal use of certain resources (i.e., cell phones, smart phones) is anticipated to varying extents, however such personal use must adhere to the terms contained in this policy.

The City's computing and electronic communications resources are an asset that must be used primarily for legitimate City business purposes. Significant investments have been committed and are expended to provide these resources to Users for conducting City business. Personal use is not forbidden, but such use:

- Must be limited to non-working hours.
  - The exception to this rule is if a mobile device is assigned to an employee and that employee engages in a payroll deduction for their personal use of the device. The extent of use depends on the features selected by the employee (minutes, text, data) for deduction and is clarified by the City Cell Phone Program / Device Acknowledgment Receipt required for all mobile phones assigned to users.
- Must not affect work performance and normal business activities.
- Must not directly or indirectly interfere with the City's operation of computer systems and electronic communications resources or the securing thereof.
- Must not compromise the physical security or reputation of the City.
- Must not burden the City with noticeable costs, or excessively drain network resources (i.e., bandwidth).

Personal use is not permissible if the use requires substantial expenditures of time, uses for profit or uses that would otherwise violate City policy with regard to employee time commitments or use of City equipment.

NO USER SHOULD HAVE AN EXPECTATION OF PRIVACY IN THE USE OF ANY CITY COMPUTING AND ELECTRONIC COMMUNICATIONS RESOURCES.

e. Account Ownership

The safety and security of the City's computer system must be considered at all times when using computers or electronic communications resources. Users are responsible for their own computer network and software accounts. Users are prohibited from providing their account and password information to any unauthorized person, and from obtaining another user's password by any unauthorized means. Management shall not require or keep lists of user names or passwords. Please reference the City of Redlands Password Policy for further clarification.

f. Proprietary or Confidential Information

If a user employs City of Redlands computer or electronic communications resources to subscribe or make postings to any Internet newsgroup, social networking site, public forum, blog or mailing list he or she shall not discuss or disclose proprietary or confidential information in any of those places, nor shall he or she disseminate such information through any other means.

g. Disclaimers
If a user employs City of Redlands computers or electronic communications resources to subscribe or make postings to any Internet newsgroup, social networking site, public forum, blog or mailing list he or she must include a disclaimer stating that views expressed are strictly their own and not necessarily those of the City, unless otherwise authorized.

Prohibited Activities

The following uses of the City of Redlands' computing and electronic communication resources are strictly prohibited:

a. Sending, receiving, downloading, displaying, printing, or otherwise disseminating material that is sexually explicit, profane, obscene, harassing, discriminatory, fraudulent, racially offensive, defamatory or otherwise unlawful or contrary to City policy.

b. Sending, receiving, downloading, displaying, printing or otherwise disseminating confidential information, documents or materials that are not authorized for dissemination.

c. Misrepresenting an individual's opinion as City policy or the City's position.

d. Disseminating or storing commercial or personal advertisements, solicitations, promotions, political information or any other unauthorized material.

e. Promoting private enterprise of any kind or for solicitations unrelated to City business.

f. Wasting computing and electronic communication resources by, among other things, sending mass mailings or chain letters, forwarding unauthorized attachments, unnecessary printing of email messages, excessive personal use or otherwise creating unnecessary network traffic.

g. Sending or forwarding email with attachments known or suspected to contain malicious software code, e.g., viruses and worms.

h. Sending unsolicited email messages, e.g., spam.

i. Employing a false identity (the name or electronic identification of another) or forging, or attempting to forge any portion of email or instant messages. Authorized users may not send email anonymously, e.g., when the sender's name or electronic identification is hidden.

j. Sending email messages using another person's email account.

k. Downloading files and/or software that contain malicious software code, and may contaminate City information systems and databases.

l. Using work time to access non-work related information or to "surf" the Internet.

m. Accessing the Internet through an anonymous proxy server or engaging in any activity that attempts to conceal web surfing or otherwise conceals actions that are prohibited by this policy.

n. Copying, installing, or using any software or data files that are in violation of applicable copyrights or license agreements.

o. Copying, installing, or using any software or data files that are not authorized for use by the City.

p. Use of electronic communications resources by any person who is not a "user" as defined by Section VII, 2 (b).

q. Excessive use of bandwidth or other network resources for non-work use (i.e., streaming video, audio, content-rich applications).

Monitoring, Auditing and Access

The City retains the right to monitor and audit all use of its computing and electronic communications resources, regardless of where such use is initiated. Additionally, the City retains the right to access all data, files and messages stored on, or processed through, its systems. Although the use of passwords and other forms of security are provided for confidentiality, no employee should expect, nor do they have any personal right of privacy with respect to any file or message contained within or processed through the City's computing and electronic communications resources.

The City reserves the right to monitor City-provided Internet access and usage.

This policy distinguishes between access and monitoring. Access involves opening and reviewing the content of files. Monitoring focuses on traffic patterns, general and individual levels of usage, file subjects and types, file origins and destinations, and network efficiency and security. Without providing prior notice, the City reserves the right to review any material created, stored, sent, or received in its computer systems.

a. Purposes

- Computing and electronic communications resources may be monitored and audited, and computer files may be accessed, by authorized personnel for a number of purposes including:
- Maintaining and protecting the resources for the benefit of City compliance with law.
- Undertaking the professional and statutory obligations of the City,
- Ascertaining and helping to ensure compliance with City policies,
- Ensuring the proper operation of the resources, and
- Investigating suspicious circumstances.

Monitoring is used only to obtain information that is relevant to the workplace, and is not used to obtain confidential personal information about employees. The City may engage in monitoring of electronic communications resources or other electronic files created by employees only in specific instances in which it has a legitimate business interest for such monitoring or some legal obligation to do so. In such cases, the City shall limit monitoring to actions reasonably required under the circumstances.

b. Surveillance Software

The City may use system software and software utilities, collectively, "surveillance software," to log, analyze and document use of the resources. Supervisors may receive reports generated by such software. The surveillance software may also be applied to transmissions from the City network between remote locations and portable devices.

c. Telephone Conversations

In compliance with federal law, audio or video telephone conversations shall not be recorded or monitored without advising the participants unless a court has explicitly approved such monitoring or recording.

d. Monitoring of the Workplace

In order to promote the safety of employees, visitors, and the public in and around City facilities, as well as the security of such facilities, the City reserves the right to monitor any portion of these premises at any time. Monitoring devices may be positioned in appropriate places within and around City buildings and public areas.

Exceptions to this policy include private areas of restrooms, showers and dressing rooms.

e. Litigation Hold Notice

The City has established a procedure for the Notice of Mandatory Preservation of all Documents, Records, Email, and Electronic Data. As a part of this process, users are to preserve and safeguard, and must not alter, delete, destroy or discard, any electronic documents or data in his or her possession related to such a Notice. Certain instances of such a Notice may require access to user files relating to the Notice for the relevant time period.

f. Employee Location Monitoring

The City reserves the right to monitor the location of City equipment. Locations may be determined within City buildings and along City streets. City-owned vehicles and equipment may be equipped with GPS or similar technology at any time.

Such monitoring technologies assist in maintaining productivity and providing an additionally secure and safe workplace. The City will ensure all location monitoring is for business-related purposes only.

The Complete Policy can be found in the Personnel Roles and Regulations