
Information Technology Use

320.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the proper use of Department information technology resources, including computers, electronic devices, hardware, software and systems.

320.1.1 DEFINITIONS

Definitions related to this policy include:

Computer system - All computers (on-site and portable), electronic devices, hardware, software, and resources owned, leased, rented or licensed by the Redding Police Department that are provided for official use by its members. This includes all access to, and use of, Internet Service Providers (ISP) or other service providers provided by or through the Department or Department funding.

Hardware - Includes, but is not limited to, computers, computer terminals, network equipment, electronic devices, telephones, including cellular and satellite, pagers, modems or any other tangible computer device generally understood to comprise hardware.

Software - Includes, but is not limited to, all computer programs, systems and applications, including shareware. This does not include files created by the individual user.

Temporary file, permanent file or file - Any electronic document, information or data residing or located, in whole or in part, on the system including, but not limited to, spreadsheets, calendar entries, appointments, tasks, notes, letters, reports, messages, photographs or videos.

320.2 POLICY

It is the policy of the Redding Police Department that members shall use information technology resources, including computers, software and systems, that are issued or maintained by the Department in a professional manner and in accordance with this policy. This policy is to be in addition to the City Policy in regard to Information Technology Use. Refer to the City Policy for further.

[See attachment: COR IT Policy.pdf](#)

320.3 PRIVACY EXPECTATION

Members forfeit any expectation of privacy with regard to emails, texts, or anything published, shared, transmitted, or maintained through file-sharing software or any internet site that is accessed, transmitted, received, or reviewed on any department computer system.

The Department reserves the right to access, audit, and disclose, for whatever reason, any message, including attachments, and any information accessed, transmitted, received, or reviewed over any technology that is issued or maintained by the Department, including the department email system, computer network, and/or any information placed into storage on any department system or device. This includes records of all keystrokes or Web-browsing history

Redding Police Department

RPD Policy Manual

Information Technology Use

made at any department computer or over any department network. The fact that access to a database, service, or website requires a username or password will not create an expectation of privacy if it is accessed through department computers, electronic devices, or networks.

The Department shall not require a member to disclose a personal username or password for accessing personal social media or to open a personal social website; however, the Department may request access when it is reasonably believed to be relevant to the investigation of allegations of work-related misconduct (Labor Code § 980).

320.4 RESTRICTED USE

Members shall not access computers, devices, software or systems for which they have not received prior authorization or the required training. Members shall immediately report unauthorized access or use of computers, devices, software or systems by another member to their supervisors or Watch Commanders.

Members shall not use another person's access passwords, logon information and other individual security data, protocols and procedures unless directed to do so by a supervisor.

320.4.1 SOFTWARE

Members shall not copy or duplicate any copyrighted or licensed software except for a single copy for backup purposes in accordance with the software company's copyright and license agreement.

To reduce the risk of a computer virus or malicious software, members shall not install any unlicensed or unauthorized software on any Department computer. Members shall not install personal copies of any software onto any Department computer.

When related to criminal investigations, software program files may be downloaded only with the approval of the information systems technology (IT) staff and with the authorization of the Chief of Police or the authorized designee.

No member shall knowingly make, acquire or use unauthorized copies of computer software that is not licensed to the Department while on Department premises, computer systems or electronic devices. Such unauthorized use of software exposes the Department and involved members to severe civil and criminal penalties.

Introduction of software by members should only occur as part of the automated maintenance or update process of Department- or City-approved or installed programs by the original manufacturer, producer or developer of the software.

Any other introduction of software requires prior authorization from IT staff and a full scan for malicious attachments.

320.4.2 HARDWARE

Access to technology resources provided by or through the Department shall be strictly limited to Department-related activities. Data stored on or available through Department computer systems shall only be accessed by authorized members who are engaged in an active investigation

Redding Police Department

RPD Policy Manual

Information Technology Use

or assisting in an active investigation, or who otherwise have a legitimate law enforcement or Department-related purpose to access such data. Any exceptions to this policy must be approved by a supervisor.

320.4.3 INTERNET USE

Internet access provided by or through the Department shall be strictly limited to department-related activities. Internet sites containing information that is not appropriate or applicable to department use and which shall not be intentionally accessed include, but are not limited to, adult forums, pornography, gambling, chat rooms and similar or related Internet sites. Certain exceptions may be permitted with the express approval of a supervisor as a function of a member's assignment.

Downloaded information shall be limited to messages, mail and data files.

320.4.4 OFF-DUTY USE

Members shall only use technology resources provided by the Department while on-duty or in conjunction with specific on-call assignments unless specifically authorized by a supervisor. This includes the use of telephones, cell phones, texting, email or any other "off the clock" work-related activities. This also applies to personally owned devices that are used to access department resources. This does not apply to exempt members at the Department.

Refer to the Personal Communication Devices Policy for guidelines regarding off-duty use of personally owned technology.

320.5 PROTECTION OF AGENCY SYSTEMS AND FILES

All members have a duty to protect the computer system and related systems and devices from physical and environmental damage and are responsible for the correct use, operation, care and maintenance of the computer system.

Members shall ensure department computers and access terminals are not viewable by persons who are not authorized users. Computers and terminals should be secured, users logged off and password protections enabled whenever the user is not present. Access passwords, logon information and other individual security data, protocols and procedures are confidential information and are not to be shared. Password length, format, structure and content shall meet the prescribed standards required by the computer system or as directed by a supervisor and shall be changed at intervals as directed by IT staff or a supervisor.

It is prohibited for a member to allow an unauthorized user to access the computer system at any time or for any reason. Members shall promptly report any unauthorized access to the computer system or suspected intrusion from outside sources (including the Internet) to a supervisor.

320.6 INSPECTION OR REVIEW

A supervisor or the authorized designee has the express authority to inspect or review the computer system, all temporary or permanent files, related electronic systems or devices, and any

Redding Police Department

RPD Policy Manual

Information Technology Use

contents thereof, whether such inspection or review is in the ordinary course of his/her supervisory duties or based on cause.

Reasons for inspection or review may include, but are not limited to, computer system malfunctions, problems or general computer system failure, a lawsuit against the Department involving one of its members or a member's duties, an alleged or suspected violation of any department policy, a request for disclosure of data, or a need to perform or provide a service.

The IT staff may extract, download or otherwise obtain any and all temporary or permanent files residing or located in or on the department computer system when requested by a supervisor or during the course of regular duties that require such information.

Attachments

COR IT Policy.pdf

CITY OF REDDING
Personnel Policies and Procedures Manual

Section: Miscellaneous Policies

Subject: Policy Regarding Use of Computers and Management of Electronic Records

Personnel Director: Rinda Johnson **Date:** 10-24-08

City Manager: [Signature] **Date:** 10/27/08

City Council Resolution No. (if applicable) N/A **Effective Date:** 9/1/98

Purpose

The routine use of electronic equipment by City employees raises a number of issues, including appropriate use of equipment and software, confidentiality of City data; retention or deletion of electronic information; ownership and access to equipment; and prohibited uses. The purpose of this item is to establish a City of Redding policy regarding the appropriate and professional use of computers and related technology.

Policy

It is the policy of the City of Redding to abide by the United States Copyright Laws. Any employee that has access to copyrighted or licensed software and makes unauthorized copies of copyrighted or licensed programs is in violation of these copyright laws. Therefore, no City personnel shall duplicate a licensed program without written authorization from the vendor or unless the software license agreement authorizes it.

The use of employee-owned personal computer hardware or software at the workplace is prohibited without permission of the Department Director. The City will not be held liable for any damage or loss to, nor will the City be responsible for the maintenance of, employee-owned hardware, software, or data even if such materials or equipment are used in the course of conducting authorized City business.

Only Information Technology personnel or other personnel authorized by Information Technology will load software and/or hardware onto City computers. Software will be loaded only if: (1) it is licensed by the City, or (2) it is licensed to an employee of the City and its use has been approved by the Department Director.

Configuration of each workstation shall be determined first by City-wide policy and then by department policy. Only Information Technology or department personnel authorized by Information Technology may change the configuration of computer systems.

The City seeks to protect its proprietary interest in City records stored on its computer systems. Rules prohibiting theft or vandalism apply to software and data as well as to physical equipment. All software, data, reports, messages and information stored on local and network resources are the property of the City.

Therefore, no data relating to the conduct of City business shall be removed or transmitted via e-mail or any method of electronic file transfer to any other agency or person unless it is for the sole purpose of completing City business. Messages/e-mail, both internal and via Internet, created, received, or sent over any City-owned computer system may be subject to public disclosure in accordance with applicable law.

Employees are not guaranteed enjoyment of privacy rights for any mail, messages, or files created, stored, received, or transmitted on City computer systems and networks containing personal information unrelated to City business. Furthermore, City management reserves the right to review any and all such mail, messages, files, etc., to ensure compliance with this Policy and any other applicable City policies, laws, rules, and regulations.

Employees are expected to exercise good judgment while using the City's hardware, software, and networks. These tools should be used in a responsible, efficient, ethical, and legal manner in accordance with this and other administrative policies, regulations, and work standards. An employee's User-ID and Password are unique, identifying his/her as the user accessing a workstation or PC. The employee is responsible for any modifications or access to system information made using their User-ID. Therefore, employees shall at all times use extreme care to avoid exposing the City's automated systems and networks to security violations.

Individual departments may adopt more restrictive or additional policies or regulations applicable to the use of these technologies. Said information will be disseminated to the affected employees. If a conflict exists, the more restrictive policies will apply.

The City has no control over the content of messages or information postings on the Internet or on-line services. Employees using these services must understand that they may receive unsolicited e-mail/information which may be considered offensive. Due to the nature of the Internet, at this time there is not a way to safeguard this activity. The City will take all reasonable measures to protect City users from this type of intrusion. The use and distribution of electronic messages and/or images are subject to the City's policies regarding harassment, discrimination, workplace violence, employee conduct and honesty, and any other City policies.

Prohibited Uses Include But Are Not Limited to:

- a. Illegal activities
- b. Threats
- c. Harassment
- d. Slander
- e. Gambling
- f. Defamation
- g. Obscene language or images
- h. Political endorsements
- i. Excessive use for personal matters unrelated to City business

- j. Personal (non-City) for profit activities
- k. Copying commercial software in violation of copyright law
- l. Sharing passwords or disseminating information which may be used to gain unauthorized access to City's systems, networks, or data
- m. Accessing the Internet or other electronic bulletin boards for inappropriate activities (e.g. pornography, profane/hate materials, etc.)

Retention and Deletion of Electronic Communications

Electronic communications, by their nature, are not customarily preserved and retained by the City or its officers or employees, but are transitory in nature similar to, and often used as a substitute for, telephonic or person-to-person communications. The City recognizes its legal obligations relating to the preservation and/or public disclosure of public records pursuant to the requirements of destruction of records laws and/or the PRA. However, the City's electronic communication systems has a limited capacity and therefore the City routinely purges, (deletes) e-mail and voice-mail communications from the system. Each system, to function as intended, anticipates or requires that employees regularly delete the communications from the system. Accordingly, an electronic communication should not to be used by any City official or employee as the exclusive means to memorialize important information when it is necessary or intended that the informational content of the communication be preserved for future City use or reference.

All electronic communications to, from, between or among any City officials or employees by use of an electronic communication system to facilitate any business of the City, where it is neither necessary nor intended that the informational content of the communication be preserved for future City use or reference, may be deleted from the City's computer system without preserving the informational content of the communication or any portion thereof, unless (1) a law expressly requires such communication to be kept; or (2) preservation of the communication is necessary or convenient to the discharge of the public officer's or employee's duties and the communication was made or retained for the purpose of preserving this informational content for future City use or reference.

If the City is required to maintain any electronic communication as a permanent record, it must be printed out in hard copy form for permanent filing or copied and stored to an electronic file for archiving separate from ordinary entries or message logs, and capable of being retrieved in readable or audible and comprehensible form.

Violation

Anyone found in violation of this policy will be subject to disciplinary action up to and including termination of employment and/or criminal prosecution, if appropriate.