



Computers, Network Systems and Internet Usage Policy

General Provisions:

This Policy is intended to supplement Section 16.4 of the City's Personnel Policies and Procedures Manual adopted July 22, 2009, and will govern the use of the City's computer information systems and related equipment ("System") by City employees. This policy refers to all system resources including personal computers, portable (laptop) computers, network servers, printers and associated peripherals and includes all software. Access to these systems, which are owned or operated by the City of Willits imposes certain responsibilities and obligations on City employees (hereinafter termed "users") and is subject to the City of Willits' policies and local, state and federal laws.

The e-mail, voice mail and computer systems are the property of the City of Willits and are provided solely as business tools to be used exclusively by its employees to facilitate the management of and the transmittal of business-related information. The City is providing employees with access to the City's computer system and electronic communication system, which may include internet access. The purpose of the System is to assist employees in communicating with others, enhance productivity, and assist employees in upgrading their skills through an exchange of information with their peers. The City's System will also assist in sharing information with the public. To be deemed acceptable under this policy, use must be ethical, reflect honesty and show restraint in the consumption of shared resources. The use must demonstrate respect for intellectual property, ownership of information, system security mechanisms, and the individual's right to privacy and freedom from intimidation, harassment, and unwarranted annoyance.

Policy:

1. Users of the City's System have a responsibility not to abuse network or computer resources and to respect the rights of others. Computer System administrators may and are entitled to routinely monitor and log usage data and review this data for evidence of a violation of these policies. The City Manager, in consultation with the Department Head, may limit or suspend computer and network privileges of an individual user for violation of these policies. Continued violation of these policies may result in disciplinary action, up to and including termination, and/or legal action. Employees who violate this policy may also be required to reimburse the City for any costs incurred as a result of unauthorized use of City property. Users will be personally responsible and liable for any copyright infringing activities.

2. Users will respect the copyrights and licenses of software and other on-line information. All software and other information protected by copyright will not be copied except as stipulated by the copyright requirements. Users who violate any copyright declarations are acting outside the course and scope of their employment, or other authority, and City of Willits shall be relieved of any legal responsibility. In such a situation, City of Willits shall be entitled to hold the user personally liable for all damages or other liabilities assessed against City of Willits. Any and all software installations will be processed under the direction of the Department Head and original disks will be maintained in a secure place.

3. Users will not attempt to modify, move or remove computer equipment, software or peripherals without the permission of the City Manager. Use of any computer equipment assigned to a user which may be supplied for home use, or is portable, will be approved by the City Manager.

4. Users will respect the privacy and personal rights of others. Users will not access the personal files and directories of other users without permission. Private messages will be marked by the sender as "Private" or "Confidential," or have a clear indication that the message is for the intended receiver only. However, employees should not expect any protection of privacy with regard to the City's information systems. Employees should expect that any e-mail or voice mail message that is created, sent or received and that any file in the computer network, in local PC's or on disks located on City property may be read or listened to at any time. The City expressly reserves the right to intercept, read, review, access and disclose all e-mail messages, voice-mail messages, and computer files. Every time a user logs onto these devices he or she is consenting to these terms and conditions. The reasons include, without limitation, the right to investigate wrongdoing, to determine whether security breaches have occurred, to monitor compliance with policies and to obtain work products needed by other employees. The use of a password does not mean information on the system shall be considered private or confidential.

5. Users will not intentionally develop or use programs which disrupt or inhibit other computer users, provide unauthorized access to restricted portions of the System, or will damage the hardware or software components of the computer system. Users will not make deliberate attempts to disrupt the computer system performance or destroy data by spreading computer viruses or by any other means.

6. Users will not use the City's System to engage in any illegal acts or acts that affect the reputation of the City, the City Council, or City personnel.

7. Users of electronic communication will not send fraudulent, harassing, obscene or threatening messages, or use mail or messaging services to harass, threaten, intimidate or otherwise annoy another person. Users will not use the City System to access material that is profane or obscene (pornography), that advocates illegal acts, or that advocates violence or unlawful discrimination toward other people. If a user unintentionally accesses such information, they will immediately disclose the access to their Supervisor. This will protect the user against an allegation that they have intentionally violated this policy. Users will not engage in using abusive or obscene language in either public or private messages. Users will exercise care not to display on computers any images, sounds or messages which would create an atmosphere of discomfort or harassment to others.

8. Passwords will be used by individuals for access to the network and other computer systems. Passwords should be known only by the individual user and System Manager and should be nontrivial. Passwords should be changed at least semi-annually. Users should avoid using passwords such as names, initials, birth dates, social security numbers or other common items. Avoid posting passwords on workstations, under the keyboard or in other easily discovered areas.

9. At the discretion of the employee's Supervisor, City employees may access the System for personal use, provided the access and use:

- (1) is not excessive;
- (2) does not interfere with the employees' work performance;
- (3) is done on the employee's break, lunch or while "off the clock";
- (4) does not interfere with others' access to the System;
- (5) is in compliance with City policies;
- (6) does not involve gambling, pornography or any illegal activity; and
- (7) does not expose the City to unauthorized expense.

10. When System changes in hardware, software or procedures are planned, when possible, users will be notified of the change to ensure that they will have enough time to prepare for the changes.

11. The City's accounting data is backed up on a daily basis. One backup tape will be stored off site, in the City's safe deposit box at Savings Bank of Mendocino County, and will be rotated weekly.

12. Users are responsible for learning proper techniques and standards for participation and for understanding that misuse of the network may lead to disciplinary actions. Particular concerns include issues of public records retention and access, copyright infringement, e-mail etiquette, offensive content, computer viruses, and appropriate use of access and file transfer services. Appropriate training will be provided, when needed.

13. The City may establish a web site and will develop web pages that will present information about the City to the public. The City Clerk, or designee, will be designated the Webmaster who will be responsible for maintaining the City web site. No information will be posted to this site without the permission of the Webmaster. All employees will be required to use our official domain name when using the internet.

14. The internet should be treated as a formal communication tool, just as the telephone, radio and written communications are. Users will be responsible and accountable for their actions and communication. E-mail messages and other transfer of information must adhere to the Government Records Access Management Act (GRAMA) and State laws relating to disclosure and retention of information.

15. Employees will be required to use proper online etiquette when responding to questions directed to them via email and the City's web site. Proper on-line etiquette includes, but is not limited to:

(1) Subject lines should be as descriptive as possible. A salutation after the subject line and before the message can be used to convey a sense of personal acknowledgment.

(2) Appending your name at the end of the message is also considered good etiquette. If communicating with someone outside the system, it is appropriate to type your name and include your e-mail address.

(3) Always copy the message that is being answered in the body of a response.

(4) Always acknowledge receipt of a document or a file someone has sent you.

(5) E-mail should be checked at least once or twice a day when expecting a reply. Emails should be deleted or saved to a local file once they have been read. Hard copies should be made for the file when appropriate.

(6) Unnecessary “surfing” on City time or while using City equipment and software is not permitted.

(7) Conference and bulletin board messages are “showcases.” All messages should be proofread and edited since communications are considered an official response from the City.

(8) Be respectful and responsive when communicating. When answering the public, always ensure that a proper and timely response is provided even if given by other individuals within the City.

(9) Do not publicly (on bulletin boards or conferences) criticize other network users or City employees.

(10) Protect others’ privacy. Internet communications are **not secure** and confidential information should not be used, sent, or attached as files for distribution purposes.

(11) Do not use capital letters as the standard form of the message. Using “all caps” is the network equivalent of SHOUTING!

(12) The City will offer periodic internet training. It is the employee’s responsibility to acquire proper training and to stay current with new tools. If special assistance is needed, the employee’s supervisor should be contacted.

(13) Each user will sign a form which indicates their understanding of the policies contained herein.

(14) This document may be updated on an as-needed basis and is subject to change.