

Computer System Usage Policy

A. Purpose

The City of Yreka, hereafter referred to as “The City”, recognizes that maintaining the integrity of the City’s computer system and the protection of data and confidential information contained on that system are vital for the efficiency, cost-effectiveness, and quality of work generated by City employees. The increasing use of the Internet and the proliferation of technological advances in the field of computers have significantly improved the communications, research, and work productivity of City employees, albeit at the increasing risk of exposing the City’s computer system and data stored on the system to damage caused by external sources, viruses, computer contaminants and unauthorized users. Therefore, the City must impose a strict policy to prohibit the usage of the City’s computer system and network which would undermine the integrity of the system, data and confidentiality of the information contained on the system and tend to impair employee job performance, efficiency or productivity. Given these concerns, any unlawful use of the City’s computer system or network in violation of this policy may result in discipline up to and including termination and may subject and an employee to criminal and civil penalties and/or prosecution.

B. Computer System as City Property

The City’s computer systems (including all hardware and software) are the exclusive property of the City and are provided to employees for creating and transmitting City business-related information. The City treats all computer files, including electronic mail (e-mail) sent and received as City business information. The City retains copies of Internet and certain e-mail passwords, and the existence of such passwords is not an assurance of confidentiality of the communications. The City has the capability and reserves the right, with or without notice, to access, monitor, review, copy, and/or delete any computer files, including e-mails sent and received, and all website communications and/or transactions.

C. Software

The City prohibits the unauthorized use of City owned software including its unauthorized copying, transfer, or reproduction. Employees are also prohibited from loading privately owned software (obtained lawfully or unlawfully) on any portion of the City computer system without the written permission of the City Manager, or his designee. Employees are also advised that the unauthorized copying or reproduction of any software is expressly prohibited under state and federal law. The City reserves the right to refer known unauthorized software copying and reproduction to interested state and federal authorities for criminal prosecution.

D. Unauthorized Access to City Computer System and Files

Employees are prohibited from accessing the City's computer system, network, computer software and related components except as required and authorized as part of performing their employment responsibilities. Employees are prohibited from accessing, taking, copying, or making use of any data or files from the City's computer system and network, or taking copies of any documentation supporting the City's computer system or network, whether existing internal or external to the City computer system or network, except as required and authorized as part of performing their employment responsibilities. Employees are also prohibited (except during authorized, periodic, file purging) from altering, damaging, or deleting any City data, files, computer software, or causing any disruption to the City's computer system or network.

E. Passwords and Access Codes

Employees may not disclose to unauthorized persons or entities assigned passwords or access codes for entry into and use of the City's computer system or network. If possible, employees are encouraged to change their passwords or assigned codes on a regular basis to protect confidentiality. Employees are prohibited from allowing or assisting other unauthorized individuals to gain access to the City's computer system or network. It is strictly prohibited to use another employee's password or code without the permission of the City Manager, or his designee. Further, employees are prohibited from representing oneself as another individual or other employee by some electronic means unless so specifically authorized by that individual and the City Manager or his designee.

F. Privacy

The City's computer system and network are provided to City employees as a tool to assist employees in performing their employment responsibilities. As such, if employees make incidental use of the computer system for personal files or e-mail, employees should not expect the data to be protected from review or deletion by the City Manager, his designee, or other employees. As previously stated, the City expressly reserves the right to access, monitor, review, copy, and delete all computer data. Accordingly, employees should not use the City's computer systems to create or transmit information they wish to keep private.

G. Confidential Information

Employees must exercise caution when creating or transmitting City business information electronically. Business information may not be transmitted to employees or other individuals who are not authorized to receive such information. Electronic mail which contains confidential attorney-client information may not be disclosed to not-City personnel except the City Attorney's office, unless so authorized by the City Manager, or his designee, or required under law. Further, only authorized City representatives are permitted to communicate with non-employees on behalf of the City via the City computer system. If an employee is unsure as to whether a communication is authorized, it is the employee's responsibility to inquire with their supervisor or the City Manager as appropriate.

H. E-Mail Transmissions and Messages in Electronic Format

Employees are required to exercise the highest standards of courtesy and professionalism when communication by messages in electronic format and e-mail and may never transmit defamatory, obscene, discriminatory, offensive or unprofessional messages. Employees should consider that certain e-mails may constitute electronic public records subject to inspection and copying under the Public Records Act or by other means of document production such as subpoena.

All personal e-mail correspondence and other communications such as preliminary drafts, notes, inter-agency and intra-agency memorandum not retained in the ordinary course of City business should be deleted within ten (10) days of receipt or otherwise subject to review and deletion by the City Manager, or his designee. Only those electronic messages, e-mails and attachments containing City business information shall be printed and filed where appropriate and in accordance with the City's applicable record retention schedule and/or departmental administrative procedures.

I. Internet Access and Prohibited Use

The City provides employees with access to the Internet for City business-related purposes. The City has the capacity to filter, monitor, and review website access. Employees should not have any expectation of privacy regarding the websites accessed through the City's computer systems. Computer systems may "leave tracks" at websites visited. Because of the nature of City business, any incidental use of the Internet for personal use must be conducted with the highest level of professionalism.

Employees are prohibited from intentionally accessing any Internet sites that are discriminatory or offensive in nature, or promote or advocate any form or type of discrimination. Employees are prohibited from posting personal opinions on the Internet using the City computer system's access, without the City Manager's, or his designee's, approval.

Any attempt to access a website that has been filtered by the network website filtering software, or any attempt to bypass the City network filtering measures by the use of software or hardware designed for the purpose of bypassing City filtering measures is prohibited. Should the need arise to access a filtered/prohibited website, the employee should contact his or her supervisor and gain official authorization to have the City Manager, or his designee, allow the necessary access for the prescribed period of time.

City computer systems may not be used to solicit or proselytize for commercial ventures, religious or political caused, or outside organizations that are not authorized by the City Manager, or his designee.

J. Procedure for Reporting Harassment/Discrimination or Violations of this Policy

Use of the City's computer systems to engage in any communications or acts that are in violation of this or any other City policy, including but not limited to the acquisition, possession or transmission of defamatory, obscene, offensive, or harassing material, is strictly prohibited. The City does not tolerate

sexual, racial, or other forms of harassment or discrimination. If harassed or discriminated against through the use of the City's computer system, an employee should report the act to his or her immediate supervisor or the City Manager and complete an Employee Harassment/Discrimination Form. If an employee is uncomfortable reporting or discussing the act or harassment or discrimination, or the supervisor is the source of the problem, condones the problem, or ignores the problem, the employee should report the problem to the City Manager. Employees are not required to directly confront the person who is the source of the report, question, or complaint before notifying any of those individuals listed.

If an employee becomes aware of another employee's actual or apparent violation of the City's computer system policy, the employee is encouraged to report the conduct to his or her immediate supervisor for further investigation. If requested, the name of the employee reporting such conduct will be withheld and remain anonymous unless disclosure is required under applicable law.

The City reserves the right to inspect any City computer, computer system, or related equipment for violations of this policy.

Employee Signature

Date