

COMPUTER USE POLICY

PURPOSE

The _____ (the “**City or County**”) relies on its **Computer Resources** to conduct its business, which includes the facilitation and delivery of public safety services, financial records and other administrative information. To ensure its Computer Resources remain in optimal working condition and are used properly by its employees, elected officials, independent contractors, agents, and other computer users, the City/County has created this **Computer Use Policy** (the “**Policy**”).

The rules and obligations described in this **Policy** apply to all users (the “**Users**”) of the City’s/County’s computer resources wherever they may be located. Violations will be taken very seriously and may result in disciplinary action, including possible termination, civil and/or criminal liability.

It is every user’s duty to use the City’s/County’s computer resources responsibly, professionally, ethically, and lawfully.

DEFINITIONS

Computer Resources, refers to the City’s/County’s entire computer network. Specifically, **Computer Resources** includes, but is not limited to: host computers, file servers, fax servers, web servers, workstations, stand-alone computers, laptops, software, data files, and all internal and external computer and communications networks (e.g., Internet, computer online services, value-added networks and e-mail systems) that may be accessed directly or indirectly from or through the City’s/County’s computer network.

Users, refers to all elected officials, appointees, employees, independent contractors, consultants, temporary workers, and other persons or entities who use the City’s/County’s computer resources.

POLICY

The City’s/County’s computer resources are the property of the City and may be used only for legitimate business purposes. Users are permitted access to the computer resources to assist them in the performance of their jobs. Use of the computer system is a privilege that may be revoked at any time.

In using or accessing the City’s/County’s computer resources, Users must comply with the following provisions:

A. NO EXPECTATION OF PRIVACY

No expectation of privacy. The computer resources and computer accounts given to Users are to assist them in the performance of their jobs. Users do not have privacy, nor should they have an expectation of privacy, in anything they create, store, send, or receive on the computer system.

Monitoring of computer usage. The City has the right, but not the duty, to monitor any and all aspects of its computer system, including, but not limited to; monitoring sites visited by Users on the Internet, monitoring chat-groups and news-groups, reviewing material downloaded or uploaded by Users to the Internet, and reviewing e-mail sent and received by Users. Users are hereby notified that the City may use human or automated means to monitor use of its Computer Resources.

B. PROHIBITED ACTIVITIES

Inappropriate or unlawful material. Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate may not be sent by e-mail or any other form of electronic communication (such as; bulletin-board systems, news-groups, chat-groups), downloaded from the Internet, displayed, and/or stored in the City's/County's computers. Users encountering or receiving this kind of material should immediately report the incident to their supervisor(s).

Note: This prohibition does not extend to the legitimate need to report, record and relay certain information directly related to the City's/County's administrative and law enforcement duties.

Prohibited Uses. The City's/County's computer resources may not be used for dissemination or storage of commercial or personal advertisements, solicitations, promotions, destructive programs (such as, viruses or self-replicating code), political material, or any other unauthorized use.

Games and entertainment software. Users may not use the City's/County's computer resources and/or Internet connection to play or download games and other entertainment software, including screen savers.

Waste of computer resources. Users may not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive amounts of time on the Internet, playing games, engaging in online chat groups, printing unnecessary multiple copies of documents, or otherwise creating unnecessary network traffic.

Copying of software. Users may not illegally copy material protected under copyright law or make that material available to others for copying. Users are responsible for complying with copyright law and applicable licenses that apply to software, files, documents, messages, and other material they wish to download or copy. Users may not agree to a license or download any material for which a registration fee is charged without first obtaining the express written permission of either the Mayor, City Administrator, or the Chief of Police or their respective designate(s).

Communication of confidential information. Unless expressly authorized by the Mayor, City Administrator or the Chief of Police or their respective designate(s), the sending, transmitting, or otherwise disseminating confidential or legally protected information or data pertaining to or maintained by the City, or any department thereof is strictly prohibited. Unauthorized dissemination of this information may result in substantial civil liability as well as severe criminal penalties.

C. USE OF E-MAIL

Forwarding e-mail. Users may not initiate or forward chain e-mail. Chain e-mail is a message sent to a number of people asking each recipient to send copies with the same request to a specified, or in some cases unspecified, number of others.

Altering attribution information. Users must not alter the "From:" line or any other attribution-of-origin information in e-mail, messages, or postings. Anonymous or pseudonymous electronic communications are forbidden.

Communicating information. Content of all communications should be accurate. Users should use the same care in drafting e-mail and other electronic documents as they would for any other written communication. Anything created on the computer may, and likely will, be reviewed by others.

E-mail retention. Users should discard inactive e-mail after sixty (60) days unless directed to the contrary by a supervisor. Inactive e-mail is that e-mail for which there is no further known need or reason to forward, reply, or otherwise use for legitimate business purposes.

D. USE OF THE INTERNET

Certain Users may be provided with access to the Internet to assist them in the performance of their jobs. The Internet can be a valuable source of information and research. However, its use must be tempered with common sense and good judgement. Users abusing their privilege to use the Internet will have their access restricted or eliminated. In addition, abuse may subject the abusing party to disciplinary action, including possible termination, civil and/or criminal liability.

Accessing the Internet. To ensure security and avoid the spread of viruses, accessing the Internet directly by modem is strictly prohibited unless the computer in use is not connected to the City's/County's network.

Note: Users may assume that Internet access through a computer attached to the City's/County's network is through an approved Internet firewall and thereby authorized.

History Files. Internet History files, Temporary Internet Files, and Internet Cookie Files shall not be cleared, deleted or changed by any user. Internet browser settings shall be set to clear history files automatically by the system administrator. The City Administrator and the Chief of Police shall determine the standard setting for their respective departments. Internet History files, Temporary Internet Files, and Internet Cookie Files are subject to review without prior notice.

Disclaimer of liability for use of the Internet. The City is not responsible for material viewed or downloaded by users from the Internet. The Internet is a worldwide network of computers that contains millions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material.

In general, it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. In addition, having an e-mail address on the Internet may lead to receipt of unsolicited e-mail containing offensive content. Users accessing the Internet do so at their own risk and should log and report such incidents as they occur.

E. PASSWORDS

Responsibility for passwords. Users are responsible for safeguarding their passwords for access to the computer resources. Individual passwords should not be printed, stored online, or given to anyone other than a supervisor. Users are responsible for all transactions made using their passwords. Users must access the computer system using a password and no User may access the computer system with another User's password or account. Users may not use passwords or encryption keys that are unknown to their immediate as well as command level supervisors or department head.

Passwords do not imply privacy. Use of passwords to gain access to the computer system or to encode particular files or messages does not imply that Users have an expectation of privacy in the material they create or receive on the computer system. The City has global passwords that permit it access to all material stored on its computer system-regardless of whether that material has been encoded with a particular User's password.

F. SECURITY

Accessing other user's files. Users may not alter or copy a file belonging to another User without first obtaining permission from the owner of the file. The ability to read, alter, or copy a file belonging to another User does not imply permission to read, alter, or copy that file. Users may not use the computer system to "snoop" or pry into the affairs of others by unnecessarily reviewing their files and e-mail.

Accessing other computers and networks. A User's ability to connect to other computer systems through the network or by a modem does not imply a right to connect to those systems or to make use of those systems unless specifically authorized by the operators of those systems.

Computer Security. Each User is responsible for ensuring that the use of outside computers and networks such as the Internet does not compromise the security of the City's/County's computer resources. This duty includes taking reasonable precautions to prevent intruders from accessing the City's/County's network without authorization and to prevent the introduction and spread of viruses.

Users have the responsibility to "sign off" after each use of any computer resource to prevent others from accessing theirs or others files, computer(s), and/or other Computer Resources or use of access privileges.

G. VIRUSES

Virus detection. Viruses can cause substantial damage to computer systems. Each User is responsible for taking reasonable precautions to ensure he or she does not introduce viruses into the City's/County's Computer Resources. To that end, all material received on floppy disk or other magnetic or optical medium and all material downloaded from the Internet or from other computers or networks that do not belong to the City, MUST be scanned for viruses and other destructive programs before being placed onto the computer system.

Users should understand that their home computers and laptops might contain viruses. All disks transferred from these computers to the City's/County's network MUST be scanned for viruses.

It is the responsibility of each User to provide all other material received on floppy disk or other magnetic or optical medium to the network administrator or other designated person or party, for scanning prior to installation.

Note: Users may assume that materials downloaded from the Internet through the City's/County's computer network will automatically be scanned for viruses.

Virus Alerts. Users with knowledge of or suspecting the introduction of a virus into the City's/County's Computer Resources shall notify his or her supervisor immediately.

H. ENCRYPTION SOFTWARE

Use of encryption software. Users may not install or use encryption software on any of the City's/County's computers without first obtaining written permission from the City Administrator, Chief of Police or their respective designate(s). Users may not use passwords or encryption keys that are unknown to their immediate as well as Command Level Supervisor(s) or Department Head.

I. MISCELLANEOUS

Attorney-Client Communications

E-mail sent to or from in-house counsel or any attorney representing the City and/or employees and elected officials should include the following “**Warning header**” and “**Footer**” on each page:

Warning-header

“ATTORNEY-CLIENT PRIVILEGED; DO NOT FORWARD WITHOUT PERMISSION.”

Standard Footer

“This e-mail and any files transmitted with it are confidential and are intended solely for the use of the individual or entity to whom they are addressed. This communication may contain material protected by the attorney-client privilege. If you are not the intended recipient or the person responsible for delivering the e-mail to the intended recipient, be advised that you may have received this e-mail in error and that any use, dissemination, forwarding, printing, or copying of this e-mail is strictly prohibited. If you have received this e-mail in error, please immediately notify the City Administrator at _____ or the Chief of Police at _____. You will be reimbursed for reasonable notification costs.

Compliance with applicable laws and licenses. In their use of computer resources, Users must comply with all software licenses; copyrights; and all other state, federal and international laws governing intellectual property and online activities.

Other policies applicable. In their use of Computer Resources, Users must observe and comply with all other policies and guidelines of the City.

Amendments and revisions. This Policy may be amended or revised from time to time as the need arises. Users will be provided with copies of all amendments and revisions.

Management rights. Management reserves the right to grant certain privileges to individual Users that may be or seem contrary and/or beyond the scope of this policy. All such privileges shall only be granted with the express permission of the Mayor, City Administrator or Chief of Police or their respective designate(s).

No additional rights. This policy is not intended to, and does not grant, Users any contractual rights.