5.16 Computer and E-mail Usage

Effective Date: 4/1/99

Computers, computer files, the e-mail system, and software furnished to employees are the City property intended for business use. Employees should not use a password, access a file, or retrieve any stored communication without authorization. To ensure compliance with this policy, computer and e-mail usage may be monitored.

To ensure the efficient exchange of information, employees must check for e-mail messages at least twice per day.

The City strives to maintain a workplace free of harassment and sensitive to the diversity of its employees. Therefore, the City prohibits the use of computers and the e-mail system in ways that are disruptive, offensive to others, or harmful to morale.

For example, the display or transmission of sexually explicit images, messages, and cartoons is not allowed. Other such misuse includes, but is not limited to, ethnic slurs, racial comments, off-color jokes, or anything that may be construed as harassment or showing disrespect for others.

E-mail may not be used to solicit others for commercial ventures, religious or political causes, outside organizations, or other non-business matters.

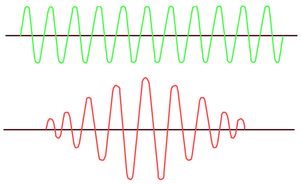
The City purchases and licenses the use of various computer software for business purposes and does not own the copyright to this software or its related documentation. Unless authorized by the software developer, the City does not have the right to reproduce such software for use on more than one computer.

Employees may only use software on local area networks or on multiple machines according to the software license agreement. The City prohibits the illegal duplication of software and its related documentation.

Employees should notify their immediate supervisor, the Personnel Department or any member of management upon learning of violations of this policy. Employees who violate this policy will be subject to disciplinary action, up to and including termination of employment.

5.17 Internet Usage

Effective Date: 4/1/99



Internet access to global electronic information resources on the World Wide Web is provided by the City to assist employees in obtaining work-related data and technology. The following guidelines have been established to help ensure responsible and productive Internet usage. While Internet usage is intended for job-related activities, incidental and occasional brief personal use is permitted within reasonable limits.

All Internet data that is composed, transmitted, or received via our computer communications systems is considered to be part of the official records of the City and, as such, is subject to disclosure to law enforcement or other third parties. Consequently, employees should always ensure that the business information contained in Internet e-mail messages and other transmissions is accurate, appropriate, ethical, and lawful.

The equipment, services, and technology provided to access the Internet remain at all times the property of the City. As such, the City reserves the right to monitor Internet traffic, and retrieve and read any data composed, sent, or received through our online connections and stored in our computer systems.

Data that is composed, transmitted, accessed, or received via the Internet must not contain content that could be considered discriminatory, offensive, obscene, threatening, harassing, intimidating, or disruptive to any employee or other person. Examples of unacceptable content may include, but are not limited to, sexual comments or images, racial slurs, gender-specific comments, or any other comments or images that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.

The unauthorized use, installation, copying, or distribution of copyrighted, trademarked, or patented material on the Internet is expressly prohibited. As a general rule, if an employee did not create material, does not own the rights to it, or has not gotten authorization for its use, it should not be put on the Internet. Employees are also responsible for ensuring that the person sending any material over the Internet has the appropriate distribution rights.

Internet users should take the necessary anti-virus precautions before downloading or copying any file from the Internet. All downloaded files are to be checked for viruses; all compressed files are to be checked before and after decompression.

Abuse of the Internet access provided by the City in violation of law or the City policies will result in disciplinary action, up to and including termination of employment. Employees may also be held personally liable for any violations of this policy. The following behaviors are examples of previously stated or additional actions and activities that are prohibited and can result in disciplinary action:

- Sending or posting discriminatory, harassing, or threatening messages or images
- Using the organization's time and resources for personal gain
- Stealing, using, or disclosing someone else's code or password without authorization
- Copying, pirating, or downloading software and electronic files without permission
- Sending or posting confidential material, trade secrets, or proprietary information outside of the organization
- Violating copyright law
- Failing to observe licensing agreements
- Engaging in unauthorized transactions that may incur a cost to the organization or initiate unwanted Internet services and transmissions
- Sending or posting messages or material that could damage the organization's image or reputation
- Participating in the viewing or exchange of pornography or obscene materials
- Sending or posting messages that defame or slander other individuals
- Attempting to break into the computer system of another organization or person
- Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities
- Using the Internet for political causes or activities, religious activities, or any sort of gambling
- Jeopardizing the security of the organization's electronic communications systems
- Passing off personal views as representing those of the organization
- Sending anonymous e-mail messages
- Engaging in any other illegal activities