COMPUTER AND INTERNET USE POLICY 408

I. PURPOSE

The City of Visalia (City) recognizes the importance of personal computers and network-client computing in providing responsible local government activities. It shall be the policy of the City to provide computer resources, up to and including Internet and e-mail (electronic mail) access where determined to be of benefit to the City. Unauthorized use of the City's computer resources is prohibited. Violation of this policy can result in revocation of a user's access to the City's computer resources, employee disciplinary action as established within the City of Visalia's disciplinary policy, and a referral for prosecution to other entities for violation of federal, state and/or local laws and regulations.

The purpose of this policy and procedure shall be to define appropriate uses for City owned, operated and maintained computer resources (including, but not limited to, hardware, software and Internet/on-line access).

II. POLICY/PROCEDURE

City computing resources are made available to employees to assist in the pursuit of departmental and organizational goals. Computer resources shall be defined as any hardware (personal computers, personal digital assistants (PDAs), mobile digital terminals (MDTs), host systems, printers, scanners, network, etc.), software, remote access, electronic mail (e-mail) and Internet connection tools deemed necessary to fulfill the duties required to provide responsible service to Visalia residents. Users are expected to cooperate with each other to promote the most effective use of computing resources, and to respect each other's work even though it is in electronic rather than printed form. Individuals and departments will be held no less accountable for their actions involving computers than they would be in other situations.

A. Confidentiality & Privacy

1. The City seeks to protect the confidentiality of 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 received and stored on local and network hard drives or other storage medium, as well as other products created using the City's computer resources, are the property of the City. Therefore, access to these products may be obtained by authorized City staff without prior

authorization by the user/creator.

2. The City reserves the right to set permissions and accessibility rights as it deems necessary to all city computer resources.

3. **There is no expectation of personal privacy in the use of City computing resources, the Internet, or e-mail**. Computer files, no matter on what medium they are stored or transmitted, may be subject to the California Public Records Act (CPRA) if stored on the City's computers, and therefore subject to disclosure to anyone requesting a copy of the message. That fact notwithstanding, no one should look at, copy, alter, or destroy anyone else's personal files, or portions thereof, without explicit permission (unless authorized or required to do so by law or regulation). Simply being able to access a file or other information does not imply permission to do so.

B. Personal Use

City computer resources exist for conducting City business. Mindful of this goal, employees may use City computer resources for personal business if:

- All other requirements of this policy are adhered to;
- Use time is personal time before or after normal work hours and not City time;
- Personal use does not interfere with normal City business or City computer operations;
- Personal files are saved on a removable media and not stored on City devices;
- Printed output is minimal and paper is provided by the employee;
- Written approval has been granted from the immediate supervisor (see Personal Computer Use Authorization attachment).

C. Property Rights

All City computer resources, and all users' accounts, are the properties of the City. All employees must respect the legal protection provided by copyrights, licenses, and federal, state, or local laws and regulations. Copying of City-owned or licensed software or data to another computer system for personal or external use is prohibited without the prior written consent of the Information Services manager. Attempts to damage or disrupt operation of computing equipment, data

communications networks, or data communications lines is prohibited and is subject to disciplinary action, up to and including termination, as already established within the City of Visalia's disciplinary policy.

D. Computer Users

All authorized employees, volunteers, and contractors of the City who use City computer resources shall be defined as "Computer Users." Volunteers, contractors, and non-city employees may be granted access to City computer resources at the discretion of the Information Services Manager or appropriate Department Head. Each computer user will be assigned a network logon and one-time initial password. In general, after the initial password access, each user is responsible for maintaining his/her personal passwords. Where possible and appropriate within the City network, a valid e-mail account, that both sends and receives Internet mail, and access to Internet web sites via a browser will be provided.

E. Security - User ID

1. The City's computer systems require that each user have a unique identity, referred to as a "User ID," typically protected by one or more passwords or security schemes to gain access to the system. Other security mechanisms, such as hardware or software locks, digital signatures, encryption cards, tokens, algorithms, or biometrics testing may be used in lieu of, or in conjunction with, password security. The User ID represents a user in various system activities, provides access to certain software and data based on his/her department-established authorization, and associates his/her own software and data with his/her identity. As such, this User ID is another instrument of identity and its misuse may constitute forgery or misrepresentation. Assuming another person's identity, or assuming an anonymous identity, is expressly prohibited.

2. An employee's User ID and security are unique, identifying him/her as the user accessing a particular workstation or PC. The employee is responsible for any modifications or access to system information made using his/her User ID. Every change to computer information is subject to audit logging with the identification of the person who signed on. Therefore, it is imperative that each user or their designee does not share

passwords, and that no PC, terminal, or workstation is left unattended while logged on. Users should be aware that merely turning a PC off does not always log the user off the system. Users needing assistance with logging off procedures should contact Information Services.

3. Each employee may perform specific functions, as authorized by his/her Department Head, which are identified through use of the User ID. Employees may have access to large volumes of information, much of which may be confidential to the Department or the City. It is important that each employee knows and understands what information may be shared with others in the work unit, in the department, with personnel in other departments, and with the general public. Employees who are uncertain as to the confidentiality of data should request clarification from their supervisor or Information Services immediately.

F. Internet Content

1. Due to the very nature of Internet and on-line services, the City has no control over the content of messages or information postings on those services.

2. The City reserves the right to use available technology to screen out information that may be offensive, as determined by the City. Since new sites are added daily, this technology cannot block all sites that may contain offensive material, nor can the City prevent transmission and/or receipt of offensive e-mail messages.

3. The City reserves the right to log, monitor, and review all system and Internet connection and traffic information. Employees using on-line services and/or Internet access must understand that they may receive unsolicited e-mail/information that may be considered offensive. Due to the nature of the Internet, there is no way to safeguard this activity at this time. Offensive information or sites should be forwarded to Information Services and the immediate supervisor. The City will attempt to minimize this type of activity so as to protect city users from this intrusion.

4. The City has several sanctioned web sites for general city information (www.ci.visalia.ca.us), Visalia Police Department

(www.vpd.ci.visalia.ca.us), Convention Center (www.visalia.org), Convention & Visitor's Bureau (www.cvbvisalia.com), and Economic Development (www.visaliaecondev.com), as well as an internal / intranet site for use by city personnel only. Personal web sites produced, or hosted, and/or linked on City resources are not allowed.

5. The City maintains a dedicated Internet connection with a protective security firewall. This firewall isolates city resources and helps protect the City network from external intrusions. The City's web servers reside behind this firewall to provide some level of security and protection. Internet use is provided through the use of this dedicated connection, the firewall, and a proxy or authorization system. Internet use outside of this configuration is prohibited unless specifically authorized by the Information Services manager and appropriate Department Head.

G. E-Mail Services (e.g. Outlook and/or Internet Mail*)*

1. All electronic mail messages are considered City records. The City reserves the right to access and use for business purposes the contents of all messages sent over its electronic mail systems, including electronic mail sent over the Internet. Employees should not expect or assume any privacy regarding the content of electronic mail communications.

2. When communicating with individuals, groups, or institutions, employees do so as a representative of the City. Thus, all actions should be conducted in a professional manner. Users of City-provided e-mail systems are expected to use these systems in a professional manner.

3. Users and their designees agree to represent themselves according to their true and accurate identities in all electronic messages, files and transactions at all times.

4. Confidential, restricted, or proprietary data should not be sent via the Internet without appropriate encryption safeguards. This includes specific strategies, major directions, and working files not completed for public dissemination; confidential or restricted data as defined by local, state, or federal laws; data of other businesses or persons with respect to which the City is under an obligation of confidentiality.

5. E-mail messages regarding policies, decision-making, contracts, or other information that should be a part of the official City business records should be printed and retained by the sender or receiver of such e-mail. Therefore, employees are responsible for retaining and archiving those e-mail messages that serve as official records of City business.

6. In order to use system resources efficiently, general interest work-related announcements will be posted on the e-mail system in an appropriate area established by Information Services. Incidental and occasional personal use of electronic mail is permitted within the City, but such messages will be treated the same as other messages. All messages will be deleted according to the schedule maintained by the City's Information Services (IS) division.

H. Computer Virus Issues

1. The City desires to protect its computing resources from both the intentional and unintentional introduction or promulgation of any computer virus, which is a violation of the law. Therefore, the City maintains a site license for anti-viral products for use on all City computers. Network servers, incoming Internet mail and the e-mail server are continuously scanned for viruses. Individual desktop or laptop PCs are also equipped with this anti-viral software.

2. While the City makes every effort to control the spread of computer viruses, there are no absolute guarantees against computer viruses on any computer system. Therefore, employees must also take responsibility by practicing safe computing. The following are some safe computing guidelines: Computer users are to leave the anti-virus software running on their computer (there are a few exceptions to this, where certain software will not run with the anti-virus software resident – check with Information Services). Great care must be used when receiving Internet e-mail or outside files on diskette, particularly if the originator is unknown. Finally, report any suspicions of viruses to Information Services.

I. Remote Access and Use of Modems

1. Modem access either in or out of the City network must be authorized by Information Services. Most users will utilize a "modem bank" that restricts and logs activity. Due to security risks, standalone modems and remote access software (e.g., Carbon Copy or PC Anywhere) are allowed only with written authorization from the IS Manager and appropriate Department Head.

2. Remote access services will be allowed for those users specifically authorized to work at home, away from the office, or at City facilities lacking network communications upon written request from the appropriate Department Head.

3. The City will not be responsible for any damages, licensing issues, hardware or software configuration issues, delays, nondeliveries, or service interruptions that may occur due to use of personal equipment at home for City business.

4. Users may not run or otherwise configure software or hardware to intentionally allow access by unauthorized users.

J. System Administration Access and Monitoring

1. A System Administrator (i.e., the person responsible for the technical operations of a particular machine or system) may access others files for the maintenance of networks, computers, and storage systems, such as to create backup copies of media. IS staff operating computers and networks may routinely monitor and log usage data, such as network session connection times and source and destination, CPU and disk utilization for each user, security audit trails, network loading, etc.

2. The contents of electronic messages may be viewed by a system administrator or supervisor in the course of routine maintenance, or as needed for City administrative purposes, including investigation of possible violations of this policy, or other disciplinary action.

3. IS staff may review this data for evidence of violation of law or policy, and other purposes and is responsible to report violations or abuse of privileges

if made aware of them. Violations will be confidentially reported to Personnel.

4. The City will cooperate appropriately, upon the advise of legal counsel, with any local, state, or federal officials investigating an alleged crime committed by an individual affiliated with a City computer resource, and may release information to such officials without the knowledge or consent of the user. This includes any violation of Police Department operating procedures and use/misuse of law enforcement systems.

5. When necessary, management staff may monitor all the activities of, and inspect the files of, specific users on their computers and networks. Any person who believes such monitoring or inspection is necessary must obtain concurrence from the Personnel division.

6. In all cases, individuals' privileges and reasonable expectation of personal privacy are to be preserved to the greatest extent possible.

K. Purchasing and Upgrade Processes

1. To provide the most cost-effective and efficient service, Information Services has established standard hardware and software configurations and purchasing guidelines.

2. All hardware and software acquisitions, whether new or upgrades, must be authorized by both the requesting department and Information Services (IS) before purchases are made.

3. All established purchasing procedures (see Purchasing Policy) are to be followed. In order to insure compatibility and avoid possible problems, all purchases and installation will be made with the assistance of IS and competent departmental staff. In general, physical software licenses and disks should be stored with IS.

4. Under no circumstances are unauthorized individuals to install any hardware or software on City computers or the network, or to relocate equipment.

III. CITY RESPONSIBILITIES

A. The City has the responsibility to develop, implement, maintain, and enforce appropriate security procedures to ensure the integrity of individual and City information, however stored, and to impose appropriate penalties when privacy or security is purposefully abridged.

B. The City has the responsibility to develop, implement, maintain, and enforce appropriate procedures to discourage harassment by use of its computers or networks, and to impose appropriate penalties when such harassment takes place.

C. The City has the responsibility to uphold all copyrights, laws governing access and use of information, and rules of organizations supplying information resources to the City.

D. Each supervisor has the responsibility of communicating and enforcing this policy, providing for security in their areas, controlling physical access to equipment, providing a proper physical environment for equipment, and providing safeguards against fire, flood, theft, etc.

E. Each supervisor has the responsibility to provide appropriate training in the use of computer equipment and applications. That training may come from internal City resources or through contracted training classes.

IV. EMPLOYEE RESPONSIBILITIES

A. Users of computer services provided by the City shall abide by the following:

1. Make a reasonable effort to inform themselves of these access guidelines and definitions of acceptable and unacceptable uses of City computer systems, the Internet and other on-line services in general. The burden of responsibility is on the user to inquire as to acceptable and unacceptable uses prior to accessing the system. Compliance with applicable use restrictions is mandatory.

2. Respect the rights of others. Conduct which involves the use of City computing resources to violate another user's rights includes, but is not limited to: a) invading the privacy of an individual by using electronic

means to ascertain confidential information; b) copying, or altering another user's software or data which has been obtained by illegal means; c) abusing or harassing another user through electronic means; d) assuming another user's or an anonymous identity.

3. Respect the legal protection provided to programs and data by all copyrights, licenses, and laws. Users may not copy City-owned or licensed software or data to another computer system for personal or external uses without prior written approval of the City's IS manager. Software from home may not be installed or copied to city owned computers without prior written authorization from the IS manager.

4. Respect the integrity of computing systems connected to the City network, the Internet and other on-line services. Be aware of network or computer capacity and the impact that complex graphic and video files have on the City system.

5. Know and follow the generally accepted etiquette of e-mail, the Internet and other on-line services. For example, use civil forms of communication as outlined in this policy.

6. Avoid uses that reflect poorly on his/her department, the City, or Government in general.

7. Users should remember that existing and evolving rules, regulations, and guidelines on ethical behavior of government employees and the appropriate use of government resources also apply to the use of electronic computing and communications systems supplied by the City.

B. Acceptable Computer and Internet Uses

1. Communication, research, and information exchange directly related to the City or Department mission, or to the User's work tasks.

2. Communication and exchange for professional development, to obtain training or education, or to discuss issues related to the user's governmental activities.

3. Use in applying for or administering grants or contacts for City programs.

4. Use for advisory, standards, research, analysis and professional society activities related to governmental tasks and duties.

5. Announcement and/or tracking of new laws, procedures, policies, rules, services, programs, information, or activities.

6. Any other governmental administrative communications not requiring a high level of security.

C. Unacceptable Computer and Internet Uses

Use of City's computer resources for purposes other than those identified in this policy is not permitted. Users are specifically prohibited from using the City's computer resources in any manner identified in this section. Users who violate this section of the Policy by engaging in inappropriate use of the City's computer resources shall be subject to revocation or suspension of user privileges, disciplinary action up to and including termination as already established within the City of Visalia's disciplinary policy, and may also be subject to criminal or civil sanctions permitted by law. Specific exemption to these unacceptable uses may be made for Police Department investigations with the approval of the Chief or his designees. Such violations include, but are not limited to:

1. Use of City computer systems, the Internet or any other on-line service for any purposes, which violate the law.

2. Destruction or damage to equipment, software, or data belonging to the City or others.

3. Use for any for-profit activities unless specific to the mission or duties of the user's department.

4. Use for purposes not directly related to the mission or work tasks of the user during normal work hours.

5. Use for private business, including commercial advertising and sending or replying to "chain letters."

6. Use of City computing resources for external consulting is prohibited.

7. Sending or soliciting sexually oriented messages or images; accessing internet sites which are "adult-oriented in nature, or which require the user to be over the age of 18 years, or which offer gambling services, or which contain obscene content of any nature.

8. Libelous, offensive, or harassing statements, including disparagement of others based on their race, national origin, sex, sexual orientation, age, disability, religious or political beliefs.

9. Use of City's computer resources to defraud, threaten, libel or harass others.

10. Impersonation of any person or communication under a false or unauthorized name.

11. Transmission of any unsolicited advertising, promotional materials, or other forms of solicitation.

12. Using City resources for commercial purposes or personal financial gain, without written permission from the City Manager or his/her designee.

13. Inappropriate mass mailing, "spamming" or "mail bombing".

14. Tampering with any software protections or restrictions placed on computer applications or files.

15. Knowingly or maliciously introducing any invasive or destructive programs (i.e., viruses, worms, Trojan Horses) into City computers or networks.

16. Attempting to circumvent local or network system security measures.

17. Use for access to and distribution of computer games, except for incidental and occasional use of legally obtained games which come pre-installed

with the computer's operating system, as approved by the user's supervisor.

18. Use of the City of Visalia provided computer systems, the Internet or other on-line services so as to interfere with or disrupt network users, services or equipment.

D. Users of computer services provided by the City of Visalia shall refrain from:

1. Intentionally seeking out information on, obtaining copies of, modifying, or divulging files, reports, and other data which is private, confidential or not open to public inspection or release unless specifically authorized to do so once the legal conditions for release are satisfied.

2. Intentionally copying or printing any software, electronic file, program or data using City provided computer systems, Internet or other, on-line services without a prior, good faith determination that such copying or printing is, in fact, permissible. Any efforts to obtain permission should be adequately documented.

3. Intentionally seeking information or security access rights on, obtaining copies of, or modifying files or data without proper authorization. Seeking passwords of others or the exchanging of passwords is prohibited, without proper designation and approval by the immediate supervisor.

4. Intentionally representing themselves electronically as others, either on the City network or on the Internet or other on-line services unless explicitly authorized to do so by those other Users. Users shall not circumvent established policies defining eligibility for access to information or systems.

5. Intentionally developing programs designed to harass other users or infiltrate a computer or computing system and/or damage or alter the software components of same.

6. Using City computer resources for fundraising, partisan politics or public relations activities not specifically related to City activities.

7. Attempting to modify City-owned or licensed software or data files without prior written approval by the city's Information Services Manager.

8. Attempting to damage or disrupt operation of computing equipment or telecommunication equipment lines. If a user is not familiar with the ramifications of the changes he/she is attempting to make on his/her computer, call Information Services before making any changes.

9. Using city computing resources for purposes other than those intended by the Department authorizing access, including allowing access by unauthorized persons, even if they are members of the community or city staff.

Computer and Internet Use Policy
Informational Addendum

Internet Etiquette

By Stan Horwitz (stan@vm.temple.edu)

The Internet is a vast community of people from all over the world. In this global electronic community, the only impression other people have of you is based on what you say through your writing and how well you say it. A thorough knowledge of E-mail etiquette will help prevent misunderstandings. The following tips apply to sending any information you write over the Internet (i.e., Usenet, Listserv, and E-mail): Use mixed case text in your writing.. Uppercase text denotes shouting so you may offend some people by typing in all uppercase text. All uppercase text is also hard to read.

Never send chain letters via the Internet. Sending a chain letter can annoy recipients and cause hostility. Some recipients will return so many copies of the letter to you (mail bombing) that it could crash the system you use for E-mail. Other people will report you to your local system administrator who might suspend your Internet access privileges.

Include a subject heading in each E-mail message you send. Be sure that your subject heading is brief and clearly indicates exactly what you intend to write about. This helps people organize and prioritize their incoming E-mail. Many people will ignore a message if it does not have a subject indicated or if it is vague. They feel that any message which does not include a clearly written subject isn't worth reading. Additionally, if you reply to a message, make sure your reply is relevant to the subject of the original message. If not, the thoughts you intend to convey in your message won't match up with what the subject says it should be about. This will confuse your readers.

Don't post the same message to many different Usenet groups. Posting the same message on several Usenet groups at once is called crossposting. Many people read several groups and they get annoyed when they see the same message appear in different places. Crossposting also wastes network resources and people's time. Post your messages only to the minimum number of groups necessary. Don't post a message on a group unless the topic of your message pertains to the topic of discussion on that group. For instance, don't post a question about a computer problem on a group that talks about science fiction movies. Before you post a message to any discussion group, read through that group's postings to be sure you know what the group's discussion is all about. If you're not sure about the topic, ask on the group.

Don't be afraid to post a message on a discussion group if you think the message is appropriate for the group. No one will bite you for posting a message as long as you don't consciously try to

offend anyone. Electronic discussion groups work best when a large number of people contribute to the discussion. This free exchange of information or opinion is what helps to make the Internet a dynamic global community. As you begin to learn about the Internet and its various discussion groups, you will probably want to try your hand at posting messages to some groups. The best way to learn about this is to send a test message to a group, however, people who have been participating in that group (particularly busy groups) hate to see test messages interfere with the flow of the discussion on there group. For that reason, a few groups were set up just for testing purposes. On listserv, you're welcome to try your hand at posting messages to test@vm.temple.edu if you're on the Internet or test@templevm if you're on BITNET. For Usenet groups, there's alt.test, misc. test. Most Usenet group hierarchies have a test group within them. Please use these groups for your testing attempts.

Be careful in what you say and how you say it. E-mail is faceless. Unintentionally offending someone is easy because your facial expressions cannot be seen and the emotion in your voice cannot be heard. If you're joking, say so or use a smilie face symbol. For example, use :) to denote a humorous smile. A list of smilie faces is available via anonymous ftp on ftp.temple.edu and on many Gopher servers. If you receive a lot of E-mail, which you requested, you are responsible to read it on a timely basis. Don't let your account overflow with E-mail. This can easily happen with some busy Listserv groups. If you don't regularly read E-mail from a particular list, sign off it. Many discussions have archives, which can be retrieved from the appropriate Listserver. If you go away for a while and cannot check your E-mail, suspend your Listserv subscriptions until you return.

The Internet is neither private nor secure. Some people can look at almost anything you send through the Internet, even private E-mail. Don't send confidential information (i.e., social security numbers, credit card numbers, etc.) to anyone else via the Internet.

COMPUTER AND INTERNET USE POLICY 408

Computer Use Agreement for City of Visalia

I have read the Computer and Internet Use Policy, including all attachments, and understand its provisions. I understand that use of the City's computer system in any capacity is a privilege and not a right. I understand that I have absolutely no right to privacy in any of the City's computer systems, User ID's, files, etc., and that any materials that I have created, saved, downloaded, erased, etc. are subject to search and review by my employer.

I accept responsibility for the appropriate use of City computer resources, which include all computer systems, networks, Internet and intranet web site or other data processing equipment owned by the City, as well as remote computers, or computer systems when used to access the City computer resources, as outlined in the Computer and Internet Use Policy and attachments.

I understand that use of the City computer resources in violation of the Computer and Internet Use Policy may result in employee discipline as already established within the City of Visalia's disciplinary policy, up to and including termination, and/or the cancellation or restriction of user privileges.

I agree to report any use which is in violation of the Computer and Internet Use Policy to the Information Services Manager or appropriate employee supervisor.

Employee (Print Name):_____

Employee Signature_____Date_____

Witnessed by _____
Name Title

Department Head Signature_____Date_____

(To be filed with Personnel, copy to Information Services)

COMPUTER AND INTERNET USE POLICY 408

Personal Computer Use Authorization

I hereby request permission to use the City of Visalia's personal computer resources for my personal use.

Included in the City's Computer and Internet Use Policy is Section II, Policy / Procedure, subsection B, which specifically refers to personal use and is as follows:

> City computer resources exist for conducting City business. Mindful of this goal, employees may use City computer resources for personal business if:
> - All other requirements of this policy are adhered to;
> - Use time is personal time before or after normal work hours and not City time;
> - Personal use does not interfere with normal City business or City computer operations;
> - Personal files are saved on a removable media and not stored on City devices;
> - Printed output is minimal and paper is provided by the employee;
> - Written approval has been granted from the immediate supervisor.

I agree to adhere to the computer use policy and procedures as they relate to personal use and unacceptable computer use. I understand that violation of this policy and its provisions may result in the restriction or complete removal of access for personal use and may also include employee discipline as already established within the City of Visalia's disciplinary policy, up to and including termination.

Employee (Print Name):_____

Employee Signature_____Date_____

Witnessed by _____
Name Title

Supervisor Signature _____Date_____
(To be filed with Personnel, copy to Information Services)