City of Dinuba
Acceptable Use Policy
For Network Services and the Internet

I. Introduction

This acceptable use policy governs the use of computers and networks owned by the City of Dinuba. All users of these resources are responsible for reading and understanding this document. This document protects the consumers of computing resources, computing hardware and networks, and system administrators. The City Manager will appoint a system administrator to administer these policies and to manage the City's networks and mainframe computers.

II. Rights and Responsibilities

Computers and networks can provide access to many resources as well as the ability to communicate with other users worldwide. Such open access is a privilege and requires that individual users act responsibly. Users must respect the rights of other users, respect the integrity of the systems and related physical resources, and observe all relevant laws, regulations, and contractual obligations. Since electronic information is volatile and easily reproduced, users must exercise care in acknowledging and respecting the work of others through strict adherence to software licensing agreements and copyright laws.

Access to computer systems and networks owned or operated by the City of Dinuba imposes certain responsibilities and obligations on City employees and officials (hereinafter termed "users") and is subject to state, federal, and municipal laws. Acceptable use is always ethical, reflects honesty, and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of information, system security mechanisms, and the individual's rights to privacy and freedom from intimidation, harassment, and unwarranted annoyance.

III. Existing Legal Context

All existing laws (federal and state) and City Ordinances, Resolutions, and Policies apply, including not only those laws and regulations that are specific to computers and networks, but also those that may apply generally to personal conduct.

Users do not own accounts on City computers, but are granted the privilege of exclusive use. Under the Electronic Communications Privacy Act of 1986 (Title 18 U.S.C. section 2510 et. Seq.), users are entitled to privacy regarding information contained in these accounts. This act, however, allows system administrators or other authorized City employees to access user files in the normal course of their employment when necessary to protect the integrity of computer systems or the rights or property of the City. For example, system administrators may examine or make copies of files that are suspected of unauthorized use or misuse or that have been corrupted or damaged. User files may be subject to search by law enforcement agencies under court order if such files contain information which may be used as evidence in a court of law.

There is no expectation of personal privacy in the use of City computing resources, the internet, or e-mail. 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.

Use of network services provided by the City of Dinuba may be subject to monitoring for security and/or network management reasons. Users of these services are therefore advised of this potential monitoring and agree to this practice.

Misuse of computing, networking or information resources may result in the loss or restriction of computing and/or network access privileges. Additionally, misuse can be prosecuted under applicable statutes. Users may be held accountable for their conduct under any applicable City policies, procedures, or collective bargaining agreements. Illegal production of software and other intellectual property protected by U.S. copyright law is subject to civil damages and criminal punishment including fines and imprisonment.

Other organizations operating computing and network facilities that are reachable via the City's network may have their own policies governing the use of those resources. When accessing remote resources from City facilities, users are responsible for obeying both the policies set forth in this document and the policies of the other organizations.

Users should also be aware that their "deletion" of electronic information from any computer equipment will often not erase such information from the system's storage until it is overwritten with other data and it may, in any case, still reside in the City's network either on various back-up systems or other forms, and, even if erased, may still exist in the form of print-outs.

Users should also be aware that electronic mail, whether or not created or stored on City equipment, may constitute a City record subject to disclosure under the California Public Records Act or other laws as a result of litigation. However, the City does not

automatically comply with all requests for disclosure, but evaluates all such requests against the precise provisions of the Act, other laws concerning disclosure and privacy, or other applicable law. The California Public Records Act and other similar laws jeopardize the ability of the City to guarantee complete protection of personal electronic mail resident on City equipment.

IV. Internet Content

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.

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.

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 system administrators or other appropriate authority.

V. Personal Use

City computer resources exist for conducting City business. Mindful of this goal, employees may use City computer resources for personal use if all of the following requirements are met:

1. All other requirements of this policy are adhered to.
2. Use time is personal time before or after normal work hours and not City time.
3. Use does not interfere with normal City business or City computer operations.
4. Use does not interfere with performance of duties and responsibilities.
5. Printed output is minimal.
6. Approval has been granted from the immediate supervisor.

Incidental and occasional personal use of electronic mail is permitted if it does not otherwise violate this policy. Such messages will be treated the same as all other electronic information on the system.

VI. Conduct

Conduct which violates this policy includes, but is not limited to, the activities in the following list:

1. Unauthorized use of a computer account.
2. Using the City Network to gain unauthorized access to any computer systems.
3. Connecting unauthorized equipment to the City network.
4. Installing unauthorized or personally-owned software on a City computer or network.
5. Installing City-owned software on a non-City computer.

6. Unauthorized attempts to circumvent data protection schemes or uncover security loopholes. This includes creating and/or running programs that are designed to identify security loopholes and/or decrypt intentionally secure data. It also includes attempting to gain access to software or services for which the individual user is not specifically authorized, e.g., internet access.
7. Knowingly or carelessly performing an act that will interfere with the normal operation of computers, terminals, peripherals, or networks.
8. Knowingly or carelessly running or installing on any computer system or network, or giving to another user a program intended to damage or to place excessive load on a computer system or network. This includes, but is not limited to, programs known as computer viruses, Trojan Horses, and worms.
9. Knowingly or carelessly 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.
10. Deliberately wasting/overloading computing resources, such as printing too many copies of a document.
11. Violating terms of applicable software licensing agreements or copyright laws.
12. Violating copyright laws and their fair use provisions through inappropriate reproduction or dissemination of copyrighted text, images, etc.
13. Using City resources for commercial activity or personal financial gain, such as creating products or services for sale.
14. Using electronic mail to harass or threaten others. This includes sending repeated, unwanted e-mail to another user.
15. Initiating or propagating electronic chain letters.
16. Inappropriate mass mailing. This includes multiple mailings to newsgroups, mailing lists, or individuals, e.g. "spamming," "flooding," or "bombing." The City also reserves the right to refuse mail and other connections from outside hosts that send unsolicited, mass or commercial messages, or messages that appear to contain viruses, and may filter or discard such messages.
17. Forging the identity of a user or machine in an electronic communication.
18. Transmitting or reproducing materials that are slanderous or defamatory in nature, or that otherwise violate existing laws or City policies.
19. Attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner.
20. Using the equipment and/or networks for partisan political purposes, fundraising or public relations activities not specifically related to City activities.

Certain activities listed above will not be considered misuse when performed by system security officials for security or performance testing.

VII. Enforcement

Minor infractions of this policy, when accidental, such as consuming excessive resources or overloading computer systems, will generally be resolved informally by the system administrator. This may be done through electronic mail or in-person discussion and education.

Repeated minor infractions or misconduct which is more serious may result in the temporary or permanent loss of computer access privileges or the modification of those privileges. More serious violations include, but are not limited to: unauthorized use of computer resources; attempts to steal passwords or data; unauthorized use or copying of licensed software; repeated harassment; or threatening behavior. In addition, offenders may be referred to the Human Resources Division for further action.

Any offense which violates local, state, or federal laws may result in the immediate loss of all City computing privileges and will be referred to appropriate law enforcement authorities.

Use of City computer resources in any other manner as provided or identified in this policy is prohibited. Users who violate this policy 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 set forth in the City of Dinuba's Personnel Policies and Practices, and may also be subject to criminal or civil sanctions as permitted by law. Specific exemption to violations of this policy may be made for Police Department investigations with the approval of the City Manager, Chief of Police, or appropriate designees.

VIII. Conclusion

Users agree to read and abide by this policy and its administrative interpretation as they may be amended from time to time. The City Manager or his designee is responsible for providing administrative interpretation, which will be modified periodically in light of experience gained and legal and administrative developments. Users are responsible for reviewing this policy and its administrative interpretation on a routine basis.