Information Technology Services
Technology Resource
Usage Policy
Revision 2.0

February 24, 2004

Access to the information technology resources owned and operated by the City of Caldwell imposes certain responsibilities and obligations and is granted subject to City of Caldwell policy and the applicable local, state and federal laws. Use of City of Caldwell technology resources implies that the user has agreed to comply with and be subjected to these policies.

The following policies define appropriate use of the City of Caldwell network, telephones, computers, all related peripherals, software, electronic communications and Internet access. They apply to the access of the City’s network and use of computing technology resources at any location, from any device, via wired or wireless connection. They apply to all users of City technology resources regardless of employment status. Access to all networks and related resources require that each user be familiar with these policies and associated work rules. The City of Caldwell authorizes the use of computing and network resources by City staff, contractors, volunteers and others, as assigned by City staff, to carry out legitimate City business. All users of City computing and network resources must be consistent with the intent and requirements of all City policies and work rules. Technology resources may not be used to facilitate operation of a personal business or for personal gain.

Technology resources may be used for incidental personal needs as long as such use does not result in additional cost or liability, interfere with business, productivity or performance, pose additional risk to security, reliability or privacy or conflict with the intent or requirements of any City policy or work rule. Personal usage should generally be communicated with and approved by the department Supervisor. This document does not attempt to address every possible situation that may arise. Etiquette and common sense should be exercised while using City technology resources. This document provides policies and general rules for appropriate uses of these resources.

1. Information Technology Security

The City of Caldwell incorporates several methods for securing technology resources from intrusion, virus infection and other similar threats. Any attempts to avoid, bypass or defeat the restrictions and/or systems that provide these methods of protection is considered a violation of City policy.

All authorized users of City technology resources will be issued a username and password. Authorized users will take reasonable care to ensure the integrity and security of all systems they are authorized to use, including taking precautions to ensure that their passwords remain secure.

Employees should never:

a. Reveal a password, except to their authorized computer support professionals.
b. Leave a written record of their password in an obvious location such as under the keyboard, taped to the monitor, etc.
c. Leave their computer or other system logged in and accessible when the user is not present.
d. Log in on behalf of another person so that person can access the system.

e. Never execute a program sent to you unless you know what it does and completely trust the source. By no means shall any unauthorized executable program from an external site be executed on the City network. PC software should be scanned for viruses and/or Trojan code. For instruction in virus protection methods, contact the Information Technology Services staff.

2. Software Management

Software will be installed on City of Caldwell technology resources by authorized Information Technology Services staff only. This ensures proper licensing compliance, virus detection and appropriate configuration as necessary for use within City technology resources.

3. Expectations of Privacy

There should be no expectation of privacy for any user on any City technology resource. All information stored on any City system, including but not limited to email, voicemail, network file servers (even in personal home directories), local hard drives or their workstations, personal digital assistants (PDA's), City issued digital cameras and City owned removable media, belongs to the City. Any information can be viewed, read or used at any time by authorized Information Technology Services staff members or City authorized agent(s), with or without notice to the employee. The existence or use of passwords does not create privacy due to the fact that authorized City Information Technology Services staff, when necessary, can change user password and access information; similarly, deleting information or documents does not ensure privacy because the City maintains backups which may be accessed in order to review data. If users wish to retain truly private information, they should not store it anywhere on City technology resources.

Authorized Information Technology Services staff may utilize active or passive systems for monitoring activity or data on any City technology resource. The City can, may and will change or add such systems at any time, with or without notice. These systems are used primarily to help monitor system performance, detect system problems and help in troubleshooting problems when they occur.

4. Individual Responsibilities

a. Users are responsible for any use or misuse of their logins or other authorizations by themselves or others. User should never leave equipment unattended once they have logged on and should never logon using another user's authorization. Accounts and passwords are to be used only by the authorized user.
b. Passwords and authorization codes shall be kept confidential by all users and should never be written down. Computer passwords should contain a combination of letters and numbers and should be changed regularly (at least every six months).
c. Users shall respect the confidentiality of other users data; specifically, users shall not intentionally seek information about, obtain copies of, or modify files or passwords belonging to other users unless explicitly authorized to do so by those users. This includes taking printer or facsimile output belonging to others.
d. Disk space is a limited resource to be used for City business only. All redundant files and electronic mail should be periodically removed from the system.
e. Computer users shall refrain from engaging in wasteful practices which consume excess amounts of computing resources (cpu, memory, disk, paper) such as, excessively large on-line compiles and generating large printer listings. When such extensive resources are required, they should be scheduled with Information Technology Services staff to be completed at an appropriate time that does not have an impact on other users or systems. Connectivity is also a limited resource and users should remain logged in or connected to resources only while actively using them.

f. The City performs regular backups of network systems but users are responsible for backing up PC- based files. It is therefore recommended that all users store their information on their designated network storage location. The City and Information Technology Services staff is not responsible for files or information that is lost on a local computer or other technology resource.

5. Acceptable Uses

a. Communication and transmission of information, within the agency, directly related to the task and/or duties outlined in the position held and/or related to the assigned task at hand.
b. Communication and transmission of information, to the public or other agency, directly related to the task and/or duties outlined in the position held and/or related to the assigned task at hand.
c. Research, studies and/or information gathering directly related to the activities of the City and/or related to the assigned task at hand.
d. Application for and/or transmission of information now available online directly related to the position held by the person and/or related to the assigned task at hand.
e. All activities, which are designated by the City of Caldwell to be the reason for which the tools were initially intended to be used.

6. Unacceptable Uses

It is unacceptable to knowingly or intentionally submit, publish, display, transmit, retrieve or store on City technology resources, any information and/or image which:

a. Violates or infringes on the rights of any person;
b. Contains defamatory, false, inaccurate, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive or otherwise biased, discriminatory or illegal material;
c. Violates government regulations prohibiting sexual harassment;
d. Restricts or inhibits other users from using the system or the efficiency of the computer systems;
e. Encourages the use and/or uses the system for the purpose of criminal intent;
f. Contains incendiary statements which might incite violence or describe or promote terrorist activities;
g. Uses the system for any illegal purpose;
h. Solicit the performance of any activity that is prohibited by law;
i. Transmit materials, information, images and/or software in violation of any local, state or federal law;
j. Engage in any activity for personal gain or personal business transactions;
k. Make any unauthorized purchases;
l. Download, disseminate, store or print copyrighted materials, including articles and software, in violation of copyright laws.

Section 6 – Unacceptable Uses, continued…

It is also unacceptable, without the express written consent of the immediate supervisor, for a City employee to use the provided facilities and capabilities of the technology resources to:

m. Conduct any non-approved business;
n. Conduct any political activity;
o. Conduct any non-government-related fund raising or public relations activities;
p. Use any and all games on City provided computer equipment;
q. Use unauthorized screen savers and background images (the City does not allow the use of any background images or screen savers unless first authorized by the Information Technology Services department);
r. Use and /or install any and all software without prior permission of the Information Technology Services staff;
s. Place advertisements for commercial enterprises including but not limited to goods, services and/or property;
t. Abuse electronic voice and mail privileges (An occasional note to another person, similar to a quick telephone call is acceptable);
u. Promote or advertise any non-profit charitable organization or event;
v. Store information on the network or on any technology resource in a location not expressly approved by the Information Technology Services staff;
w. "Hack" the network, any system or computer on the network, and/or any technology resource;
x. Use any portion of the City technology resources to "hack" into any other system and/or technology resource related to or unrelated to the City systems.

As with any set of policies or guidelines, exceptions will be granted and documented on a case-by-case basis. These require authorization from the Department involved as well as from the Information Technology Services staff.

Any employee who observes or suspects a violation of these policies and guidelines, particularly those that relate to security of the City's technology resources, systems and data, should immediately report these concerns to their Supervisor and to the Information Technology Services Help Desk.

Violations of this policy are subject to disciplinary action as deemed appropriate by the Department Head or Supervisor and as outlined by City policy in the City of Caldwell Employee Handbook.