

**CITY OF TEMECULA
CITY COUNCIL POLICY**



Title:	Use of Systems, Electronic Communications and Technology Resources
Policy No.	TBD
Approved:	October 24, 2023
Revised:	N/A

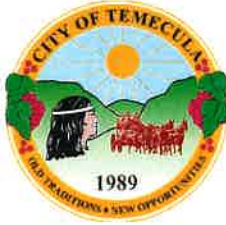
PURPOSE:

The purpose of this City Council policy is to set forth certain expectations for the use of City systems, electronic communications and/or technology resources, regardless of whether the electronic communications and/or technology resources are owned or maintained by the City, to conduct City business. In utilizing systems, electronic communications and/or technology resources, all users are expected to share the obligation of safeguarding and maintaining the City's information and adhering to the relevant policy.

POLICY:

The policy of the City Council with respect to the matter listed in the above-referenced title is attached as Exhibit A.

DRAFT



CITY OF TEMECULA
**INFORMATION TECHNOLOGY &
SUPPORT SERVICES DEPARTMENT**

MEMORANDUM

TO: Aaron Adams, City Manager
FROM: Michael K Heslin, Director of ITSS *mkh*
DATE: June 13, 2023
SUBJECT: Policy Update Approval – User Technology Resources Policy

The attached User Technology Resources Policy is an update to the previously approved Employee Technology Resources Policy on October 30, 2023.

The User Technology Resources Policy includes all definitions of communications (including email and text messaging) and Appropriate Use of Electronic Mail, Retention, and Responsibility of City Officials/Employees. City Attorney's Office has revised this policy to combine all facets of users and technology use into this policy where applicable. This update now combines employees, elected officials and other consultants into one policy and addresses use of personal technology.

Attached is the updated User Technology Resources Policy dated June 13, 2023, that will supersede all other Employee Technology Resources Policies. Attached is the marked-up version for your reference.

Please call me with any questions you may have.


Thank you




CITY OF TEMECULA
INFORMATION TECHNOLOGY
& SUPPORT SERVICES

USER TECHNOLOGY RESOURCES POLICY

DATE: June 13, 2023

DEPARTMENT APPROVAL:  6/13/2023
Department Director Signature Date

CITY MANAGER APPROVAL:  6/14/23
City Manager Signature Date

PURPOSE:

All Users who access City systems or use any Electronic Communications or Technology Resources, regardless of whether the Electronic Communications or Technology Resources are owned or maintained by the City, to conduct City Business are expected to share the obligation for safeguarding and maintaining the City's information, as outlined in the following policy. If a User needs clarification on any of the terms of this Policy, the User should contact the ITSS Department.

SCOPE:

This Policy applies to all Users including those Users affiliated with third parties who access City Technology Resources or Electronic Communications or use any personal or commercial Technology Resources or create Electronic Communications to conduct City Business.

Table of Contents

1	Confidentiality	4
2	Definitions	4
2.1	“User” means all City employees, elected and appointed City officials, members of City commissions and advisory boards, and City consultants and other non-employees utilizing Electronic Communications or Technology Resources for the purpose of conducting City Business, regardless of the User’s location when accessing any Electronic Communications or Technology Resource.	4
2.2	“City” shall mean any entity controlled by the City Council, including but not limited to Temecula Community Services District, Public Financing Authority, Temecula Housing Authority or Successor Agency to the Temecula Redevelopment Agency.	4
2.3	“City Business” is broadly defined to mean those activities or other business, related to the City and its jurisdiction, functions, programs, operations, regulations or regulatory activities, or events relating to the City, or that contain information used by its officials, employees and consultants for the accomplishment of City-related tasks, or are related to the operation of the City, with the exception of limited incidental uses as described in Section 4.2.	4
2.4	“Electronic Communications” includes emails, text messages, voicemails, social media and blog posts, and any other electronic communications, including those developed or implemented in the future, transmitting or maintaining messages, documents, images or other writings via Technology Resources.	4
2.5	“Public Records” include any “writing” (as broadly defined below) containing information relating to the conduct of the City’s business that is prepared, owned, used, or retained by the City, regardless of the physical form and characteristics. Public Records specifically include any recorded and retained communications regarding City Business sent or received by a User through commercial or personal Technology Resources or other Technology Resources not owned by the City or connected to a City computer network. Public Records do not have to be written but may be in another format that contains information such as computer tape or disc, video or audio recording, or email or text message. Public Records are further defined in Section 4.2.2.	4
2.6	“Public Records Request” is a request for Public Records made under the Public Records Act or subpoena duces tecum or discovery request addressed to the City or a User.	4
2.7	“Technology Resources” includes all electronic media and storage devices, software, and means of electronic communication including any of the following: personal computers and workstations; laptop computers; mini and mainframe computers; tablets; computer hardware such as disk drives, tape drives, external hard drives and flash/thumb drives; peripheral equipment such as printers, modems, fax machines, and copiers; computer software applications and associated files and data, including software that grants access to external services, such as the Internet or cloud storage accounts; electronic mail (or email); telephones; mobile phones; smart phones; personal organizers and other handheld devices; and instant messaging and text systems. Technology Resources is also intended to broadly include new or emerging devices, technology, software and means of communications that may be developed or implemented in the future.	4
3	Introduction	5
4	Conditions of Use of City Technology Resources	5
4.1	Code of Conduct in the Use of City Technology Resources	6
4.1.1	Introduction	6
4.1.2	Responsibilities	7
4.1.3	Inappropriate Activities	8
4.2	Appropriate Use of Electronic Communications	11
4.2.1	Introduction	12
4.2.2	Scope	12
4.2.3	Appropriate Use and Responsibility of Users	12
4.2.4	Confidentiality and Security	14
4.3	Password Requirements	15
4.3.1	Password Standards	16
4.4	Appropriate Use of City Technology Resources	16
4.4.1	Public Representations	17
4.4.2	Users must not publicly disclose City internal information via the City Technology Resources that may adversely affect City relations or public image. Care must be taken to properly structure comments and questions posted to mailing lists, public news groups, and related public postings.	17

4.4.3	Downloading	17
4.4.4	Contacts	17
4.4.5	Information Security	17
4.5	Software Security	17
4.6	Security	17
4.6.1	Right to Examine	17
4.6.2	Privacy	17
4.7	Reporting Security Problems	18
4.8	Hardware Security	18
5	Appropriate Use of Specific City Technology Resources: City-Issued Cellular Phones and Radios	18
5.1	Introduction	18
5.2	Appropriate Use and Responsibility of Users	19
5.3	Inappropriate Use	19
6	Proximity Keys	20
7	Technology Resource Check Out	20
8	Employee Computer Purchase Program	20
	The City has incorporated a program that allows employees to borrow, at no interest, up to \$2,000 to purchase personal computer/supplies with a loan repayment up to 24-months. This program is available for full-time and part-time City employees. For more information, please visit SharePoint or the ITSS Department	20
9	User Use of Technology Resources Not Owned and/or Controlled by City	20

1 Confidentiality

Material contained in this document is property of the City of Temecula. This document should not be disclosed outside of the City without specific approval from the ITSS Director, and should not be duplicated, used or disclosed for any purpose other than that for which it was intended.

2 Definitions

- 2.1 "User" means all City employees, elected and appointed City officials, members of City commissions and advisory boards, and City consultants and other non-employees utilizing Electronic Communications or Technology Resources for the purpose of conducting City Business, regardless of the User's location when accessing any Electronic Communications or Technology Resource.
- 2.2 "City" shall mean any entity controlled by the City Council, including but not limited to Temecula Community Services District, Public Financing Authority, Temecula Housing Authority or Successor Agency to the Temecula Redevelopment Agency.
- 2.3 "City Business" is broadly defined to mean those activities or other business, related to the City and its jurisdiction, functions, programs, operations, regulations or regulatory activities, or events relating to the City, or that contain information used by its officials, employees and consultants for the accomplishment of City-related tasks, or are related to the operation of the City, with the exception of limited incidental uses as described in Section 4.2.
- 2.4 "Electronic Communications" includes emails, text messages, voicemails, social media and blog posts, and any other electronic communications, including those developed or implemented in the future, transmitting or maintaining messages, documents, images or other writings via Technology Resources.
- 2.5 "Public Records" include any "writing" (as broadly defined below) containing information relating to the conduct of the City's business that is prepared, owned, used, or retained by the City, regardless of the physical form and characteristics. Public Records specifically include any recorded and retained communications regarding City Business sent or received by a User through commercial or personal Technology Resources or other Technology Resources not owned by the City or connected to a City computer network. Public Records do not have to be written but may be in another format that contains information such as computer tape or disc, video or audio recording, or email or text message. Public Records are further defined in Section 4.2.2.
- 2.6 "Public Records Request" is a request for Public Records made under the Public Records Act or subpoena duces tecum or discovery request addressed to the City or a User.
- 2.7 "Technology Resources" includes all electronic media and storage devices, software, and means of electronic communication including any of the following: personal computers and workstations; laptop computers; mini and mainframe computers; tablets; computer hardware such as disk drives, tape drives, external hard drives and flash/thumb drives; peripheral equipment such as printers, modems, fax machines, and copiers; computer software applications and associated files and data, including software that grants access to external services, such as the Internet or cloud storage accounts; electronic mail (or email); telephones; mobile phones; smart phones; personal organizers and other handheld devices; and instant messaging and text systems. Technology Resources is also intended to broadly include new or emerging devices, technology, software and

means of communications that may be developed or implemented in the future.

3 Introduction

This Policy applies to all Users. Users are responsible for complying with this and all other City policies defining computer and network security measures.

It is City Policy that all information created, stored, processed, transmitted or printed by or on behalf of the City is and shall remain City property.

All Users who access or make decisions affecting City information play a role in protecting that information. Accordingly, it is expected that all Users share the obligation to safeguard and maintain the City's information.

All Users are expected to protect the information assets with which they have been entrusted from unauthorized, deliberate, or accidental:

- Access,
- Use,
- Modification,
- Destruction,
- Disclosure, or
- Possession.

This document defines City standards and guidelines for the protection of the availability, integrity and confidentiality of the City's Technology Resources and any Electronic Communications stored or transmitted in the furtherance of City Business, regardless of whether on City Technology Resources or other Technology Resources.

4 Conditions of Use of City Technology Resources

All Users utilizing City Technology Resources must respect the integrity of all security controls and abide by all implemented security measures, as well as adhere to all end-user license and contractual agreements associated with City Technology Resources.

1. The City reserves the right to limit permanently or restrict any User's usage of the City Technology Resources. The City reserves the rights to copy, remove or otherwise alter any information or system that may undermine the authorized use of the City Technology Resources. The City may do so with or without notice to the User in order to protect the integrity of the City Technology Resources against unauthorized or improper use, and to protect authorized Users from the effects of unauthorized or improper usage.
2. The City, through authorized individuals or entities, reserves the right periodically to check and monitor City Technology Resources, and reserves any and all other rights necessary to protect them.
3. The City disclaims responsibility and will not be responsible for loss or disclosure of User information or interference with User information resulting from its efforts to maintain the privacy, security and integrity of City Technology Resources and information.

4. The City reserves the right to take emergency action to safeguard the integrity and security of City Technology Resources and information. This includes, but is not limited to, termination of a program, job, or on-line session, or temporary alteration of User account names and passwords. The taking of emergency action does not waive the rights of the City to take additional actions under this Policy.
5. Users utilizing City Technology Resources do so subject to applicable laws and City policies. The City disclaims any responsibility and/or warranties for information and materials residing on non-company computer systems or available over publicly accessible networks, except where such responsibility is formally expressed. Such materials do not necessarily reflect the attitudes, opinions or values of the City or its employees.
6. A Department Director may recommend disciplinary action if after appropriate investigation an employee is found to be in willful violation of any City Policy. Other Users may lose access to City Technology Resources. Acts that may lead to discipline or loss of access include, but are not limited to:
 - Willful physical damage to any City Technology Resources;
 - Obtaining confidential information improperly;
 - Deliberate destruction of information;
 - Intentional interruption of normal services provided by the City Technology Resources;
 - Infringement of any patent or the breach of any copyright;
 - Gaining or attempting to gain unauthorized access to accounts and passwords;
 - Gaining or attempting to gain access to restricted areas without the permission of the appropriate authority; or
 - Inappropriate use of City Technology Resources.

4.1 Code of Conduct in the Use of City Technology Resources

It is City Policy that all Users who use, have access to, or are responsible for any City Technology Resources must recognize and comply with City's "Code of Conduct." Employees violating this Code of Conduct may be subject to disciplinary action, up to and including termination of employment, and legal action. All Users who violate this Code of Conduct may lose access to City Technology Resources.

4.1.1 Introduction

Standards for the use of City Technology Resources derive directly from standards of common sense and common decency that apply to the use of any shared resource. The City depends on a spirit of mutual respect and cooperation to resolve differences and resolve problems that arise from time to time. This Code of Conduct is published in that spirit. Its purpose is to specify User responsibilities and to promote the appropriate use of City Technology Resources for the protection of the City.

4.1.2 Responsibilities

All Users who access or make decisions affecting City information play a role in protecting that information. Accordingly, all users of any City Technology Resources must accept specific responsibilities for the security and confidentiality of the City's information. The following description of City network drives will better organize your documents and minimize the opportunity for losing files.

- 'V' Drive: This is your 'my documents' directory-for draft documents or confidential information. No other User is able to access this directory
- 'P' Drive: This is a Global Directory used for quick transfer of non-confidential files. All network Users have access and may copy, delete, and modify all files. Due to this, it is recommended that you use this directory with caution. ITSS will not restore documents lost or deleted from this directory.
- 'R' Drive: This is your department directory. Only members of your department have access to this directory. It is recommended that files that are shared by others within your department be stored here.
- 'C' Drive: This is your local hard drive on your desktop. City policy requires all data to be stored on the above network drives. Local hard drives are not backed up and will not be recovered in the event of data loss.

4.1.2.1 Disclosure and Disclaimer Statement

All intellectual and proprietary property rights, including copyrights and rights to service marks and trademarks, as to any and all text, material, images and/or content appearing on or accessible through the City websites, belong to their respective owners. Notwithstanding the foregoing, the City owns all intellectual and proprietary property rights, including copyrights and rights to service marks and trademarks, as to the City Seal, all City logos, symbols, emblems, and any and all other images, designs, content and materials created by or on behalf of the City that appear on or are accessible through the City websites.

Any use of any of the City-owned materials, images or other content accessible through, or appearing or stored on the City Technology Resources or City's websites is prohibited without the written permission of the City Manager. The following acts or activities are prohibited without prior, written permission from the City Manager: 1) modification and/or re-use of text, images or other content from a City server; 2) distribution of the City's web content; or 3) "mirroring" of the City's information, materials or data on a non-City server.

4.1.2.2 Security

City Policy uses access controls and other security measures to protect the confidentiality, integrity and availability of the information handled by City Technology Resources. All Users are responsible to insure the security of City Technology Resources by implementing procedures to:

- Safeguard their data, personal information, passwords and authorization codes, and confidential data;

- Take full advantage of file security mechanisms built into the City Technology Resources;
- Choose their passwords wisely and to change them as required; and
- Follow the security policies and procedures established to control access to administrative data.

4.1.2.3 Confidentiality

All Users using City Technology Resources must comply with all City Policies for the maintenance of confidentiality.

1. Users have an obligation to respect the privacy of other individuals and refrain from:
 - Intentionally seeking information on, obtaining copies of, or modifying files, tapes, or passwords belonging to other individuals or to the City;
 - Representing others, unless authorized to do so explicitly by those individuals; or
 - Divulging sensitive personal data to which they have access concerning staff, customers, vendors or other individuals without explicit authorization to do so.
2. Users are responsible for reporting any information concerning instances in which City Policies or any City standards or Codes of Conduct has been or are being violated. In general, reports about violations should be directed initially to the ITSS Director and/or Human Resource Director.
3. Printers used to produce confidential information should be monitored while printing.
4. Confidential files must be overwritten on fixed disks, tapes, or cartridges.

4.1.3 Inappropriate Activities

All information stored and processed on City Technology Resources and networks is City property and subject to inspection without notice. Non-compliance with City Policy on restricted activities will not be tolerated. Violating employees are subject to disciplinary action, up to and including termination of employment, and all Users, including employees, are subject to loss of access to City Technology Resources and/or legal action.

The following are intended to illustrate some examples of unacceptable actions rather than to exhaustively list every specific behavior that may violate the City Policies. Accordingly, disciplinary or other legal action may occur after other actions if the circumstances so warrant.

4.1.3.1 Illegal Activity

Users are specifically prohibited from accessing, downloading, storing, printing or disseminating anything using City Technology Resources that is considered inappropriate, offensive, illegal, disrespectful to others, or that could instigate legal conflicts, or otherwise harm the City.

4.1.3.2 Objectionable Material

The City's Technology Resources must not be used for the transmission, obtaining possession, demonstration, advertisement or requesting the transmission of objectionable material including, but not limited to:

- Pornography;
- An article or image that promotes hate, crime or violence, or incites or instructs in matters of hate, crime or violence; or
- An article or image that describes or depicts any material, in a manner that is likely to cause offense to a reasonable adult.

4.1.3.3 Restricted Material

City Technology Resources must not be used to transmit or make available restricted material to a minor. City Policy defines restricted material as an article that a reasonable adult—by reason of the nature of the article, or the nature or extent of references in the article—would find offensive as to matters of sex, race, ancestry or native origin, drug misuse or addiction, crime, cruelty, violence would regard as unsuitable for a minor to see, read or hear.

Users should be aware that there are severe penalties for such activities. The police or a person authorized for the purposes under state or federal law may without a warrant, at any reasonable time, enter any place where the operating of a Technology Resource is carried on and inspect any articles and records kept on the premises and may seize anything that the member reasonably suspects is connected with an offense that is found on or in the place. In addition, there are penalties for delaying, obstructing or otherwise hindering the police or authorized person in the performance of their functions and for giving false or misleading statements, which are misleading through the omission of information.

4.1.3.4 Restricted Activities

The City prohibits use of City Technology Resources for the conduct of a business enterprise, participation in activities for profit purposes, or involvement in activities contrary to the spirit of City Policies including, but not limited to:

- Gambling or performing an act of playing for stakes, involving a monetary wager, in the hope of winning (including the payment of a price for a chance to win a prize); including, but not limited to sports betting, poker, blackjack, and casino wagering; or
- Day Trading or involvement in any act involving a monetary wager to broker or act as agent in the buying and selling of stocks and bonds.

4.1.3.5 Restricted Hardware and Software

It is illegal, unethical and contrary to City Policy to use City Technology Resources to generate viruses, worms or any malicious devices to contaminate other Technology Resources. Users should not knowingly possess, give to another person, install on any of the City Technology Resources, or run, programs or other information, which could result in the violation of the City Policy or the violation of any applicable license or contract.

The unauthorized physical connection of monitoring devices to City Technology Resources, which could result in the violation of City Policy or applicable licenses or contracts, is prohibited.

4.1.3.5.1 Copying and Copyrights

The City strongly supports strict adherence to software vendors' license agreements and copyright holders' notices. In particular, Users should be aware of and abide by City Policies on copying and using computer software. Most software that resides on the City Technology Resources is owned by the City or by third parties, and is protected by copyright and other laws, together with licenses and other contractual agreements.

Users are required to respect and abide by the terms and conditions of software use and redistribution licenses. Such restrictions may include prohibitions against copying programs or data for use on the City Technology Resources or for distribution outside the City; against the resale of data or programs, or the use of them for non-City purposes or for financial gain; and against public disclosure of information about programs without the owner's authorization. Users who develop new packages that include components subject to use, copying, or redistribution restrictions have the responsibility to make any such restrictions known to the users of those packages.

4.1.3.6 Harassment

City policy prohibits sexual and discriminatory harassment. City Technology Resources are not to be used to libel, defame, or harass any other person. Computer harassment is exemplified by, but not limited to:

- Intentionally using a City Technology Resource to annoy, harass, terrify, intimidate, threaten, offend or bother another person by conveying obscene language, pictures, or other materials or threats of bodily harm to the recipient or the recipient's immediate family;
- Intentionally using any City Technology Resource to contact another person repeatedly with the intent to annoy, harass, or bother, regardless of whether any actual message is communicated, and/or where no purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease;
- Intentionally using any City Technology Resource to contact another person repeatedly regarding a matter for which one does not have a legal right to communicate, once the recipient has provided reasonable notice that he or she desires such communication to cease (such as debt collection); or
- Intentionally using any City Technology Resource to invade the privacy, academic or otherwise, of another or the threatened invasion of the privacy of another.

The display of offensive material in any publicly accessible area is likely to violate City harassment policies. There are materials available on the Internet and elsewhere that some members of the City will find offensive. One example is sexually explicit graphics. The City can restrict the availability of such material if it considers its display in a publicly accessible area to be inappropriate. Public display includes, but is not limited to, publicly accessible computer screens and printers.

4.1.3.7 Wasting Technology Resources

One role of ITSS is to educate Users about proper usage of City Technology Resources. Every effort will be made to help Users understand how to use City Technology Resources properly.

It is inappropriate to deliberately perform any act that will impair the operation of any part of the City Technology Resources or deny access by legitimate Users to any part of them. This includes, but is not limited to, wasting resources, tampering with components or reducing the operational readiness of the City Technology Resources.

Wastefulness includes, but is not limited to, passing chain letters, willful generation of large volumes of unnecessary printed output or disk space, willful creation of unnecessary multiple jobs or processes, or willful creation of heavy network traffic. In particular, the practice of willfully using City Technology Resources for the establishment of frivolous and unnecessary chains of communication is an inappropriate waste of resources.

The sending of random mailings (for example, "junk mail") is not permitted. It is poor etiquette at best, and potentially harassment, to send unwanted mail messages to strangers deliberately. Recipients who find junk mail objectionable should mark as junk or delete. If the junk mail continues, the recipient should contact ITSS helpdesk.

4.1.3.8 Game Playing

The City Technology Resources are not to be used for recreational or competitive game playing. The intention of this policy is to prohibit game playing with programs and other software that may adversely impact others, violate other provisions of this Policy or damage City ability to process City Business transactions promptly.

4.1.3.9 Commercial Use

City Technology Resources are provided for the support of the City's mission. Except where expressly permitted, it is inappropriate to use City Technology Resources for:

1. Commercial gain or placing a third party in a position of commercial advantage;
2. Any non-City related activity, including non-company related communications; and
3. Commercial advertising or sponsorship except where such advertising or sponsorship is clearly related to or supports the City's mission or the service being provided.

4.1.3.10 Use for Personal Business

City Technology Resources may not be used in connection with compensated outside work or for the benefit of organizations not related to the City, except where expressly permitted.

4.2 Appropriate Use of Electronic Communications

City Technology Resources are limited to use for City Business. All Electronic Communications transmitted over or by means of any City Technology Resource shall be limited to those which involve City functions, activities or

other business, or that contain information essential to its officials, employees and consultants for the accomplishment of City-related tasks.

Electronic Communications access, including Internet and Intranet access, is provided to authorized Users as a communication tool for appropriate internal and external City Business. Implementation of this Policy and its directives are essential to protecting vital City resources and interests. Accordingly, City Policies including, but not limited to, those addressing copyright, confidentiality, harassment and compliance with equal employment laws; applicable federal, state and local laws; and the corporate code of conduct govern use of any Electronic Communications access.

4.2.1 Introduction

All Users who use Electronic Communications are expected to conduct their use with the same integrity as in face-to-face or telephonic business operations. Any use perceived to be illegal, harassing, and offensive or in violation of other City Policies may be the basis for disciplinary action up to and including termination for employees and/or loss of use or legal action for all Users.

4.2.2 Scope

This Policy applies to all Users. Users must be aware of the following restrictions that have been placed on use of Electronic Communications:

- Electronic Communications on City Technology Resources are intended for City-related business purposes with other limited incidental uses. All Electronic Communications on city Technology Resources are the property of the City, just as are hard copies of City records. The City reserves the right to retrieve and make proper and lawful use and/or disclosure of any and all Electronic Communications transmitted through any City Technology Resource.
- Electronic Communications determined to be Public Records shall be retained in electronic folders or, as described above, in hard copy. Such Electronic Communications shall be retained for the period described in the City's Records Retention Schedule or expiration of a Litigation Hold or resolution of a Public Records Act Request.

4.2.3 Appropriate Use and Responsibility of Users

City guidelines and standards for appropriate and responsible use of Electronic Communications are derived directly from the same standards of common sense and decency that apply to the use of any City Technology Resource. All usage inconsistent with these objectives is considered inappropriate use.

All Users must recognize and comply with standards and guidelines for the appropriate use of Electronic Communications.

1. No Electronic Communications should be unethical, be perceived to be a conflict of interest with the City's interests, or be inconsistent with City Policies.

2. Users must take particular care not to disseminate confidential City information or personal information to unauthorized users. Users should refrain from leaving messages containing confidential or personal information on answering machines or voice-mail systems.
3. Electronic Communications must be able to withstand scrutiny without causing embarrassment to the City, its employees or citizens. Because Electronic Communications deleted by a User may still be present, either in another person's mailbox, or on a file server or back-up file of a User. Care must be taken to ensure the accuracy and professionalism of all Electronic Communications.
4. Users must not send messages prohibited or restricted by government security laws or regulations. Emailing copies of documents in violation of copyright laws or licensing agreements is also prohibited.
5. Users should consider Electronic Communications to be the electronic equivalent of a postcard. Users must recognize their responsibility for the content, dissemination and management of the messages they send. Electronic Communications should:
 - Be courteous and polite;
 - Be consistent with City standards of conduct;
 - Protect others' right to privacy and confidentiality; and
 - Contain an accurate, appropriate and informative signature.
6. Users should secure access to their email and voice mailboxes through the use of passwords and other security devices and should not leave the system on and available to unauthorized users.
7. Users may not reveal any confidential internal email names and passwords of the City's email or voicemail users to anyone including other Users or people who request such information over the telephone and seem to have a legitimate reason for asking. All such requests must be referred to the Records Department.
8. City policy prohibits use of profanity, obscenities, or derogatory remarks in Electronic Communications referencing other individuals. Such remarks, even when made in jest, may create legal problems.
9. Users are prohibited from sending or forwarding any Electronic Communications that a reasonable person would consider to be defamatory, harassing or explicitly sexual. Users are also prohibited from sending or forwarding Electronic Communications via City Technology Resources that would be likely to offend on the basis of race, gender, national origin, sexual orientation, religion, political beliefs, disability or other protected characteristics.
10. Users must not use an Electronic Communication account assigned to another individual either to send or receive messages. If there is need to access another's Electronic Communications, such as while the other person is out ill, message forwarding and other resources must instead be used. Contact ITSS Director and/or Human Resource Director to arrange such access.

11. Users must not disclose credit card numbers, passwords, research and development information, and other sensitive data via any Electronic Communication.
12. Users must not unnecessarily or frivolously overload the Electronic Communications system including, but not limited to, spamming and junk mailing.
13. City Electronic Communications may not be used for commercial purposes unless authorized by City Manager in writing in advance.
14. Internal telephone books must not be distributed to third parties without specific authorization of a Department Manager.

4.2.4 Confidentiality and Security

Users should be aware that Electronic Communications are not a confidential means of communication. The City cannot guarantee that Electronic Communications will be private. Users should be aware that Electronic Communications could, depending on the technology, be forwarded, intercepted, printed, and stored by others. Users should also be aware that, once Electronic Communications are transmitted, they might be altered. Deleting an Electronic Communication from an individual workstation will not eliminate it from the various systems it has been transmitted across. Therefore, Users should have no personal expectation that their Electronic Communications using City Technology Resources are private.

The City reserves the right to review all Electronic Communications stored or transmitted on City Technology Resources. Although, the City does not intend to monitor the contents of Electronic Communications routinely, Users should expect that System Administrators with or without the permission of the User might access Electronic Communications. However, no other individuals may monitor or access Electronic Communications of another User unless proxy rights have been delegated by the System Administrators and approved by ITSS Director and/or Human Resource Director.

All Users must accept and abide by management directives to ensure information security, including, but not limited to:

- Users must verify the integrity of their password and abide by City Policy on password security (see section on Password Requirements);
- Users are prohibited from sending confidential material through any Electronic Communications system unless it is marked confidential or otherwise protected;
- Users must take extreme care that confidential information be redirected only where there is a need and with the permission of the originator, where possible;
- Users should recognize that Electronic Communications can be forged. Therefore, if an Electronic Communication is suspect, Users must verify its authenticity via telephone, or personally; and
- It is recommended that personal confidential material not be stored on or sent through Electronic Communications using City Technology Resources.

Unauthorized access of Electronic Communications is a violation of the City Policy and grounds for potential employee discipline or other repercussions for both employees and other Users.

4.3 Password Requirements

It is City policy that information must be protected in a manner commensurate with its sensitivity, value and criticality. To ensure the security of the City Technology Resources, all authorized users must be uniquely identified and authenticated before being granted access to Electronic Communications. User identification and authentication will be authorized through the use of User identification (User ID) unique to each User. To insure the security of the City Technology Resources, such access must be authorized, logged and periodically reviewed.

Identification Password Management

Passwords are a primary defense mechanism on many City Technology Resources. Careful selection of passwords improves security. Users are responsible for the robustness and maintenance of their own passwords. Accordingly, the following standards for password use shall apply:

- Passwords must be used where possible;
- Passwords and User IDs must be unique to each authorized User and must never be shared with anyone else;
- Passwords must not be easily associated with a particular User;
- Passwords must be memorized and never written down with other account information such as an account name;
- Passwords must not be stored in readable form in batch files, automatic log-in scripts, software macros, terminal function keys, in City Technology Resources without access control, or in other locations where unauthorized persons might discover them;
- Passwords must be changed every 90 days, or immediately if compromised or suspected of compromise;
- To prevent the compromise of multiple systems, Users must employ different passwords on each of the systems to which they have been granted access;
- The display and printing of passwords must be masked, suppressed, or otherwise obscured so that unauthorized parties will not be able to observe or subsequently recover them;
- Passwords must consist of a minimum of eight alphanumeric characters one of which is upper case and a special character.
- Any User who suspects that a password has been compromised must report it to ITSS immediately through the IT Help Desk.

City management reserves the right to revoke the privileges of any User at any time. Conduct that interferes with the normal and proper operation of City Technology Resources, which adversely affects the ability of others to use

these City Technology Resources, or which is harmful or offensive to others, will not be permitted.

4.3.1 Password Standards

The following are standards for password construction:

- Passwords must never be related to a User's job or personal life. Details such as spouse's name, license plate, social security number, and birthday must not be used unless accompanied by additional unrelated characters;
- Passwords must not be the same as User IDs or given name;
- Users must not construct passwords that are identical or substantially similar to passwords that Users had previously employed;
- Must never use the default password for any software or hardware product;
- "Blank" passwords are prohibited;
- Passwords must never be derived from User's association with the City of Temecula; and
- Passwords must never consist of a word from a dictionary. Most basic cracking programs contain over 120,000 words, and plenty of variations.
- Users are encouraged to have a password to include numbers and mixed case letters.

4.4 Appropriate Use of City Technology Resources

City Technology Resources offer extensive capabilities, but also expose risks and threats. All Users are expected to be familiar with and to comply with this Policy.

1. City Technology Resources should not be used for personal purposes. Although incidental use of City Technology Resources for personal use is permissible, use of City Technology Resources for these types of activities consumes City Technology Resources and could potentially result in poor technology performance or even system failure.
2. Any use perceived to be illegal, harassing, offensive, in violation of other City Policies, or any other uses that would reflect adversely on the City can be the basis for disciplinary action up to and including termination for employees and other repercussions including legal action for all Users, including employees. Users are expected to conduct their use of City Technology Resources with the same integrity as in face-to-face or telephonic business operations.

4.4.1 Public Representations

4.4.2 Users must not publicly disclose City internal information via the City Technology Resources that may adversely affect City relations or public image. Care must be taken to properly structure comments and questions posted to social media, mailing lists, public news groups, and related public postings.

4.4.3 Downloading

Software should not be downloaded without approval of ITSS. All software used on City Technology Resources can only be installed by ITSS, following all licensing agreements and procedures. All software downloaded from non-City sources must be screened with virus detection software prior to being installed by ITSS and may require testing on a stand-alone (not networked), non-production machine.

4.4.4 Contacts

Contacts made over the Internet should not be trusted with City information unless reasonable steps have been taken to ensure the legitimacy of the contacts. This applies to the release of any City internal information.

4.4.5 Information Security

Login passwords, User IDs and other parameters that can be used to gain access to City Technology Resources, is confidential information and must not be sent over any Technology Resource in readable form. This information must not be posted on electronic bulletin boards, listed in telephone directories, placed on business cards, or otherwise made available to third parties without the advance written permission of the ITSS Director. Telephone numbers, fax numbers, and email addresses of a User may be disclosed by the User.

4.5 Software Security

The City strongly supports strict adherence to software vendors' license agreements. Adherence to these agreements is subject to random audits by these vendors or the Software Publishers Association (SPA). When City Technology Resources are employed, copying of software in a manner that is not consistent with the vendor's license is strictly forbidden. Users must not use any externally provided software from a vendor other than those approved by ITSS.

4.6 Security

4.6.1 Right to Examine

At any time and without prior notice, City management reserves the right to examine Electronic Communications including personal Electronic Communications, web browser cache files, web browser bookmarks, and other information stored on or passing through City Technology Resources. Such management access assures compliance with internal policies, assists with internal investigations, and assists with the management of City Technology Resources. Every attempt will be made to ensure that the User's privacy is respected.

4.6.2 Privacy

Users using City Technology Resources should realize that their communications are not automatically protected from viewing by third parties.

Unless encryption is used, Users should not send information over the Internet if they consider it to be private.

4.7 Reporting Security Problems

It is the responsibility of all Users to report any known or suspected breach of security, such as passwords or other system access control mechanisms to the ITSS Department.

The ITSS Director must be notified immediately when:

1. Sensitive or confidential City information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties;
2. Unauthorized use of City Technology Resources has taken place, or is suspected of taking place;
3. Passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed; or
4. There is unusual system behavior such as missing files, frequent system crashes and misrouted messages, as these types of system behavior may be related to virus infections or other security problems and must be promptly reported and investigated.

4.8 Hardware Security

To ensure that computer systems are used in an effective and productive way, City Technology Resource hardware must be physically secured and the integrity of operating systems maintained.

1. On City Technology Resources, Users must never change operating system configurations, upgrade existing operating systems, or install new operating systems. If such changes are required Users should contact ITSS and ITSS administrators will perform them.
2. Users must not bring their own computers, computer peripherals, or computer software into City facilities without prior written authorization from their Department Head. Personal computers must be labeled clearly with the name of the owner. Desktop PCs, laptops, mobile devices, and City Technology Resources must not leave City offices unless authorized in writing by a department manager.

Printers used to produce sensitive and confidential information should be monitored and sensitive files must be overwritten on fixed disks, tapes, or cartridges.

5 Appropriate Use of Specific City Technology Resources: City-Issued Cellular Phones and Radios

Technology can significantly enhance local service delivery. Cellular telephones and radios are often practical and economical for safety services and emergency communications, and can enhance productivity. In all cases, the issuance of cellular phones or radios to Users is a privilege, not a right or an entitlement. Failure to abide by the procedures set forth in this Policy may result in the loss of use of the cellular phones or radios and in certain circumstances, may result in possible disciplinary action for employees.

5.1 Introduction

It is the intent of the City to provide each Department with effective communication devices, within the constraints of available resources. The City recognizes the need of City-owned cellular telephones and radios, and by this Policy establishes procedures for their authorization, deployment, and use in order to contain costs, ensure Departmental accountability, personal responsibility, and prevent improper use. It is important that each User assume personal responsibility for the prudent use of City-owned communication devices.

5.2 Appropriate Use and Responsibility of Users

City-owned cellular phones or radios are to be viewed as an asset provided to further assist Users in effectively completing their areas of responsibility for the City. The issuance of such communication equipment is also to be considered a vital resource in the event of an emergency. It is a goal, to ensure that City vehicles are configured with emergency (800 MHz) radios for two-way communications.

Users are responsible for maintaining adequate physical protection of the communication equipment issued to them by the City. Users shall immediately notify their Department Head or designee, who in turn shall notify the ITSS Director, if any City-owned cellular phone or radio is damaged, lost or stolen. Cellular phone and radio logs are Public Records.

Any communication equipment purchased by the City is owned by the City and must be returned to the City when the User separates from service or the need of such communication equipment no longer exists.

No User shall record any telephone call, without the knowledge and consent of all parties to the call.

The City reserves the right to terminate cellular service privileges of any User for any reason.

5.3 Inappropriate Use

City issued communication equipment are not considered a User's personal device. California law prohibits drivers from using a cellular phone while operating a vehicle without a hands-free device, e.g. wired headset (ear buds), speaker, or Bluetooth headset. It is City policy to comply with California law when using a City-owned cellular phone while operating in any vehicle. The ITSS Department provides wired headsets (ear buds) for all City-owned cellular phones. In order to further define inappropriate use, the following list is provided. Prohibited uses of cellular phones and radios include, but are not limited to:

- Any illegal use or activity
- Threats
- Slander/Libel
- Defamation
- Obscene, suggestive or offensive messages or communications
- Political endorsements or activities

6 Proximity Keys

Internal entrance to City Hall areas is extended to employees by the City. Proximity keys are issued to all Regular, Part-Time, Temporary, Project Employees, and Interns. Interns' access will be automatically disabled every 30 days unless otherwise noted by related department manager.

The City prohibits the sharing of proximity keys.

Users are required to notify ITSS immediately if proximity keys or readers are lost, damaged or stolen.

7 Technology Resource Check Out

The City understands the need occasionally to check out technology resources for work related issues. City Technology Resources such as: laptops, projectors and digital cameras are available for check out through the ITSS Department. Users in need of the equipment must have proper approval from department manager. A request in advance for the use of such City Technology Resource is necessary. If the City Technology Resource is available, Users must sign for receiving and return of any City Technology Resource on loan.

Users are responsible for maintaining adequate physical protection of the City Technology Resource issued to them by the City. Users shall also immediately notify their department head or designee, who in turn shall notify the ITSS Director, if any City-owned communications equipment is damaged, lost or stolen.

8 Employee Computer Purchase Program

The City has incorporated a program that allows employees to borrow, at no interest, up to \$2,000 to purchase personal computer/supplies with a loan repayment up to 24-months. This program is available for full-time and part-time City employees. For more information, please visit SharePoint or the ITSS Department.

9 User Use of Technology Resources Not Owned and/or Controlled by City

Users should not store Electronic Communications that involve City Business on any Technology Resources that are not owned, issued and/or controlled by the City. When Users are using Technology Resources that are not owned, issued and/or controlled by the City to conduct City Business, Users should be aware and must acknowledge and agree that any Electronic Communication that is stored or transmitted through such Technology Resource is considered a Public Record and is subject to the same terms as any Electronic Communication stored or transmitted on City Technology Resources. Should the City receive a Public Records Request, or otherwise require access to Electronic Communications related to City Business stored or transmitted on or by personal or commercial Technology Resources, the User shall provide access to such Electronic Communications immediately upon request of the City. Additionally, User shall not delete any Electronic Records related to City Business prior to the expiration of the period described in the City's Records Retention Schedule or expiration of a Litigation Hold or resolution of a Public Records Act Request. The City may require that a User execute an affidavit confirming that the User has thoroughly searched its personal or commercial Technology Resource and has provided all responsive Electronic Communications.

