CITY OF CLOVIS

TECHNOLOGY USERS POLICY AND AGREEMENT

December 13, 2024

TABLE OF CONTENTS

I. PURPOSE AND DEFINITIONS.

A. Purpose. This Policy and Agreement ("Policy") is designed to provide employees, volunteers, contractors, elected officials, agents, vendors, and other Users of City Technology Resources with definitive guidelines of acceptable and unacceptable use of City Technology Resources for the protection of both the City and the Users.

B. Definitions:

For the purposes of this Policy, unless otherwise specified, the following definitions apply:

1. City Technology Resources. A Technology Resource acquired and owned by the City, regardless of who uses or is provided that resource.

2. Personal Technology Resources. A Technology Resource acquired and owned by an individual. The receipt of a City stipend towards the use of a cell phone or other electronic device does not change the ownership of the device.

3. Posts or postings. Information, articles, pictures, videos or any other form of communication posted on a Social Media site.

4. Social Media. Content created by individuals, using accessible, expandable, and upgradable publishing technologies, through and on the internet. Examples of Social Media include, but are not limited to, Facebook, Twitter, Blogs, RSS, YouTube, LinkedIn, Delicious, and Flickr. City Social Media site(s) means Social Media which the City establishes and has proprietary rights to control.

5. Technology Resources. Includes, but is not limited to the following:

   - Internet/Intranet/Extranet-related systems.
   - Computer hardware and software.
   - Wi-Fi.
   - Cameras and video recording equipment.
   - Electronic devices, such as computers, tablets, smart phones and cell phones.
   - Telephone and data networks.
   - Operating systems.
   - Storage media.
   - Network accounts.
   - Email systems.
   - Electronically stored data.
   - Websites, web applications and mobile applications.

6. User. User or Users are individual(s) whether full or part-time, active or inactive, including, but not limited to employees, interns, volunteers, contractors, consultants, vendors, agents, elected officials, etc. who have been given access to and granted permission(s) to use City Technology Resources.

7. Multi-factor Authentication ("MFA"): An electronic authentication method in

which a User is granted access to a website, system or application only after successfully presenting two or more pieces of evidence to an authentication mechanism (i.e., a username/password combination, and at minimum, a second authenticator not based on user credentials, such as a passcode, certificate or token that is provided to the User).

II. PERSONALLY OWNED TECHNOLOGY RESOURCES.

A. Personnel Rules. The use of Personal Technology Resources at the workplace is subject to the City's Personnel Rules and Regulations.

B. City Business. Employees must check with their supervisor and the Information Technology ("IT") Deputy Director regarding the use of Personal Technology Resources to conduct City business. Personal Technology Resources used for City business are subject to the Public Records Act (See Section XI below). When using Personal Technology Resources to conduct City business, the User shall comply with the etiquette rules in Section X below.

C. Loss or Damages. The City accepts no responsibility for loss or damage to Personal Technology Resources.

III. TECHNOLOGY USERS AGREEMENT.

The Technology Users Agreement attached to this Policy shall be signed prior to all new employees, volunteers, contractors, elected officials, agents, vendors, or other users utilizing City Technology Resources. Employees currently using City Technology Resources (Users who currently have a login and password) will be required to sign the Agreement within fifteen (15) days of receipt of this Policy or risk the loss of access and City Technology Resources privileges.

IV. PRIVACY AND CONFIDENTIALITY.

A. No Expectation of Privacy. There is no expectation of personal privacy in any use of City Technology Resources, including personal e-mail, text messages, photos, social media posts, and voice messages.

B. City Technology Resources are Subject to Monitoring, Inspection and Disclosure.
All information and data viewed, created, saved, accessed, or stored on City Technology Resources are subject to monitoring, inspection, review, copying, modification, deletion, audit, disclosure and discovery.

The City reserves the right to monitor, record, search, and seize all use of City Technology Resources, including, but not limited to, access to the Internet or Social Media, communications sent or received from City Technology Resources, or other uses within the jurisdiction of the City. Such monitoring, recording, search, and seizure may occur at any time without prior notice for any legal purposes including, but not limited to, maintenance, inspections, updates, upgrades, audits, and record retention and distribution, all of which necessarily occur frequently and without notice. Such monitoring, recording, search, and seizure may specifically be used for the investigation of improper, illegal, or prohibited activity and as evidence in a legal or disciplinary matter.

Users should be aware that, in most instances, their use of City Technology Resources

cannot be erased or deleted. Accordingly, any such information may be accessed by the City and may potentially be subject to subpoena, discovery in litigation, or responsive to a Public Records Act request.

C. Electronic Communications Privacy Act Notice.
Pursuant to the Electronic Communications Privacy Act of 1986 (18 USC 2510, et seq.), notice is hereby given that there are no facilities, sources, or equipment provided by the City for sending or receiving private or confidential electronic communications. System Administrators have access to all e-mail and may monitor messages. Messages relating to or in support of illegal or inappropriate activities will be reported to the appropriate authorities and/or City Administration.

D. Specific Consent to Search and Seize City Technology Resources. Users consent to the search and seizure of any City Technology Resource in the User's possession by the City, or the City's authorized representative, at any time of the day or night and by any reasonable means. This consent is unlimited and shall apply to any City Technology Resource that is in the possession of the User, whenever the possession occurs, and regardless of whether the possession is authorized. The User waives any rights that may apply to searches of City Technology Resources under California SB 178 (2015) as set forth in Penal Code sections 1546 through 1546.4.

E. Personal Technology Resources Using City Wi-Fi.
The use of a Personal Technology Resource to access City Wi-Fi may be filtered and monitored, but is not subject to the inspection, disclosure, and search and seizure provisions of this section. Users shall comply with the City's Personnel Rules and Regulations and follow the etiquette rules set forth in Section X below.

F. Permissions and Accessibility Rights. The City reserves the right to set permissions and accessibility rights to all City Technology Resources as necessary. Rules prohibiting theft or vandalism apply to software and data as well as to physical equipment. All software, data, reports, messages (voice and data) and information stored on local and network hard drives, as well as other products created using City Technology Resources, are the property of the City of Clovis and access to them may not be obtained without prior authorization by the user/creator or the City Manager or designee.

G. Confidentiality. Most communication among City employees is not considered confidential. However, certain communications, including but not limited to police investigations, employee records, and communications with the City Attorney's office or other attorneys representing the City, may be confidential or contain confidential information. Questions about whether communications are confidential should be raised with the employee's supervisor.

1. Confidential information must be stored in the confines of a secured network drive or folder.
2. Confidential information may not be transmitted to individuals or entities not authorized to receive that information nor to other City employees not directly involved with the specific matter.
3. Employees shall exercise caution in sending confidential information through email and text messages given the ease with which such information may be retransmitted. Employees shall ensure information is not inadvertently sent to unintended recipients. In particular, exercise care when using distribution lists to make sure all addressees are

appropriate recipients of the information.

V. SECURITY - USER ID.

A. User ID. Each User shall have a unique identity, referred to as a "User-ID", protected by a "password" in order to gain access to the system. The User ID identifies a User in various system activities, provides access to certain software and data that is based on his/her department-established authorization, and associates his/her own software and data with his/her identity.

B. Passwords. Users shall use passwords associated with a particular City information system only on that system.

When setting up an account on a different information system that will be accessed using the Internet or other on-line service, choose a password that is different from the ones used on City information systems. Do not use the same password for both local and remote systems accessed via the Internet or another on-line service.

Local System Password Requirements:

- Passwords should not be so obvious so that others could easily guess them.
- Passwords must be changed if there is evidence of compromise, including malware infection, spam testing campaign or cybersecurity breach/incident.
- Passwords must be a minimum of nine (9) characters long.
- Passwords shall not contain a username or any part of your full name.
- Passwords shall not contain three (3) repetitive or sequential characters (e.g. 'aaa', '123', 'abc').
- Passwords shall not match any known to have been directly or indirectly compromised or breached.
- Passwords shall not contain context-specific words, such as 'Clovis', 'city', 'police', etc. and derivatives thereof (e.g. `'Cl0v1s', c!ty, 'p0l1c3'`).
- City User accounts will be locked for 30 minutes after five (5) failed login attempts.

C. City-issued Multi-factor Authentication ("MFA") will be required for all Users

D. Employee Responsibility. An employee's password and User-ID 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 technology information is logged with the identification of the person who signed on. Users shall not share account information, usernames, passwords, passcodes, pins or any other personal authentication tools or data with others. No PC, terminal, or workstation shall be left unattended while logged on (i.e. Users should either logoff or lock their workstations). Users should be aware that merely turning a PC or monitor off does not always log the user off the system. Users needing assistance with logging off procedures or locking their workstation should contact the IT Division at Ext. 2150.

E. Terminating Sessions. Users shall log off or execute an alternate termination procedure

when finished using any technology system or program, especially the Internet and other external technology systems. This will help prevent a potential breach of security.

F. Unencrypted E-Mail. Unencrypted e-mail sent or received on Technology Resources cannot be expected to be secure. Users should always be aware that the sender has no control over what the recipient does with the message and that the message may be sent to the wrong address or intercepted by hackers.

VI. INTERNET.

A. Use. The use of the Internet is provided to City employees as a tool to assist employees in performing official duties.

B. Content and Monitoring. The City has no control over the content of messages or information postings on external Internet sites. The City reserves the right to monitor Internet sites visited, accessed, or commented on by employees using City technology devices. The City also reserves the right to use available technology to screen out inappropriate and offensive information. This technology cannot block all sites that may contain inappropriate/offensive material. If such a site is not blocked, contact the IT Deputy Director or designee.

VII. E-MAIL.

A. Use. The City's e-mail system is provided to City employees as a tool to assist employees in performing official duties.

B. Privacy. Users should not expect or assume any personal privacy regarding the content of electronic mail communications, including personal e-mails. Employees who make incidental use of the e-mail system for personal e-mails should not expect the content to be protected from review or deletion by the City.

C. Monitoring. The City reserves the right to access and use the contents of all messages sent over City e-mail systems, including e-mail sent using City Technology Resources and messages sent over the Internet.

D. Work Related Announcements. General interest work-related announcements should be posted to the "City Information Bulletin Board" known as the Clovis Chalkboard, not sent to individual addresses or mailing lists.

E. Signature Block Usage. The use of the email signature block shall be limited to either the City standard signature block, or the Department approved signature block. Employees shall not deviate from the approved signature blocks which will include only the sender's name (including approved City relative post-nominal initials), pronouns (if desired), City title, City of Clovis, department, address, telephone, City website, City or department logo, City or department social media account links, City or department mission statement, and City disclaimer. This information must comply with the City's standard signature block style or the approved department signature block style. The email signature block shall not

contain any information not expressly authorized under this policy which shall include, but not be limited to, personal details, personal quotation, graphics (other than approved City or department graphics), or other information unrelated to City business.

F. Medium of Communication. It is the City's policy that City e-mails and e-mail systems are intended to be a medium of communication. Routine e-mail messages are comparable to telephonic communications and are not intended to be retained in the ordinary course of City business. The informational content of such communications is neither necessary nor intended to be preserved for future City use or reference. Messages in the "Deleted Items" folder will be purged after 90 days and messages in the "Sent Items" folder will be purged after two (2) years. An e-mail is considered destroyed as soon as it has been deleted from a User's mailbox, even though it is temporarily stored in the trash folder before being purged from the e-mail system.

G. Records. City e-mail systems are not intended to be, and shall not be used for, the electronic storage or maintenance of City records. Upon removal from the e-mail system, the messages will be disposed of in the City's ordinary course of business. However, until removed, e-mails will constitute public records, unless otherwise exempt by law, and may be disclosable under specified circumstances. In addition, certain e-mails will have to be retained as set forth in the City's Records Retention Policy.

The following guidelines apply:

1. E-mail messages and attachments comparable to hard copy documents that would be retained under the Records Retention Policy must be printed in hardcopy or converted to the appropriate electronic format and retained for the required time period as outlined in the Records Retention Policy.

2. It is the responsibility of individual employees and their department heads to determine if an e-mail is an official City record that must be retained in accordance with the City's Record Retention Policy. The City Clerk will assist you in making such a determination. You should keep in mind, however, that preliminary drafts, notes or interagency or intra-agency memoranda, which are not retained by the City in the ordinary course of business are generally not considered to be official City records subject to retention or disclosure. Generally, the City employee who sends the e-mail should be the person responsible for printing and filing it accordingly, but persons responsible for a particular program or project file shall be responsible for retaining all e-mail they send or receive related to that program or project.

3. Any e-mail messages that relate to a claim or a potential claim against the City must be preserved. Likewise, any e-mail messages that may relate to a lawsuit filed against the City, even if a subpoena or court order for such e-mail messages has not yet been issued, must be preserved. The City has a duty to preserve any relevant data when there is even a hint of possible litigation. Therefore, when City employees become aware of a potential claim, an actual claim, or a lawsuit against the City, they must preserve any e-mail messages and attachments that have any information relevant to that matter. Your department head can provide you with guidance on these issues.

4. Litigation Hold: From time to time you may receive a litigation hold notice. If such

notice is received, you shall create a separate folder of all items mentioned in the hold until otherwise directed by the City Attorney's office. This will help avoid the accidental destruction of records.

5. The City receives requests for inspection or production of documents pursuant to the Public Records Act, as well as demands by subpoena or court order for documents. In the event a records request or court-issued demand is made for e-mail, the employees having control over such e-mail, once they become aware of the request or demand, shall use their best efforts, by any responsible means available to temporarily preserve any e-mail which is in existence until such time as it is determined whether such e-mail is subject to preservation, public inspection, or disclosure.

H. Disclaimer Notice in City Email.

The following disclaimer will be added to each outgoing email:

"This e-mail may contain confidential and privileged material for the sole use of the intended recipient. Any review, use, distribution or disclosure by others is strictly prohibited. If you are not the intended recipient (or authorized to receive for the recipient), please contact the sender by reply e-mail and delete all copies of this message". However, permission to distribute or forward as appropriate may be given in the body of an email.

VIII. CITY SOCIAL MEDIA.

A. General. This Section establishes guidelines for the establishment and use of City Social Media sites as a means of conveying information to members of the public. The intended purpose of City Social Media sites is to disseminate information from the City about the City's mission, meetings, activities, and current issues to members of the public.

The City has an overriding interest and expectation in protecting the integrity of the information posted on its City Social Media sites and the content that is attributed to the City and its officials.

The City's official website at cityofclovis.com (or any domain owned by the City) will remain the City's primary means of internet communication.

Approved City Social Media sites shall bear the name and/or official logo of the City and, where applicable, of the Department.

B. Requirements.

1. All content on City Social Media sites shall be reviewed, approved, and administered by the Department head or Social Media designee.
2. The City's Public Affairs and Information Supervisor shall monitor content on City Social Media sites to ensure adherence to the Use Policy and the interest and goals of the City.
3. Adequate oversight of City Social Media must occur for the protection of the public health, safety and welfare of the community.

4. Whenever possible, City Social Media sites shall link back to the City's official website for forms, documents, online services and other information necessary to conduct business with the City.

5. City Social Media sites shall be managed consistent with the Brown Act. Members of the City Council, Commissions and/or Boards shall not use a City Social Media site to engage in serial meetings. Members of the City Council, Commissions and/or Boards are expected to use good judgment when using personal Social Media so that statements of personal opinion are not misinterpreted as official City policy.

6. The City reserves the right to terminate any City Social Media site at any time without notice.

7. City Social Media sites shall comply with usage rules and regulations required by the site provider, including privacy policies.

8. All City Social Media sites shall adhere to applicable federal, state and local laws, regulations and policies.

9. Any employee authorized to post items on any of the City's Social Media sites shall review, be familiar with, and comply with the Social Media site's use policies and terms and conditions.

10. Employee use of City Social Media shall be subject to Section IX of this Policy setting forth the Rules Governing the Use of Technology Resources and the City's Personnel Rules and Regulations.

C. Use Policy. The use of City Social Media shall be subject to the following:

1. The content of City Social Media sites shall only pertain to City-sponsored or City-endorsed programs, services, and events. Content includes, but is not limited to, information, photographs, videos, and hyperlinks.

2. The City shall have full permission or rights to any content posted by the City, including photographs and videos.

3. Any employee authorized to post items on any of the City's Social Media sites shall not express his or her own personal views or concerns through such postings. Instead, postings on any of the City's Social Media sites by an authorized City employee shall only reflect the views of the City.

4. Postings must contain information that is freely available to the public and not be confidential as defined by any City policy or state or federal law.

5. Postings to City Social Media sites shall NOT contain any of the following:

- Comments that are not topically related to the particular posting being commented upon.
- Comments in support of, or opposition to, political campaigns, candidates or ballot measures.
- Profane language or content.
- Content that promotes, fosters, or perpetuates discrimination on the basis of race, creed, color, age, religion, gender, marital status, or status with regard to public assistance, national origin, physical or mental disability or sexual

orientation, as well as any other category protected by federal, state, or local laws.

- Sexual content or links to sexual content.
- Solicitations of commerce.
- Conduct or encouragement of illegal activity.
- Information that may tend to compromise the safety or security of the public or public system.
- Content that violates a legal ownership interest of any other party.

6. The contents of this Use Policy shall be displayed to users or made available by hyperlink with the following disclaimers:

   - "City Social Media sites may contain content, including but not limited to, advertisements or hyperlinks over which the City has no control. The City does not endorse any hyperlink or advertisement placed on City social media sites by the social media site's owners, vendors, or partners."
   - "The City reserves the right to change, modify, or amend all or part of this policy at any time."
   - "The City reserves the right to terminate any City Social Media site at any time without notice."

D. Department Policies. Each Department that chooses to have a Social Media presence shall comply with this Section. The Department shall identify the purpose of the Social Media presence prior to establishing a Department Social Media account.

E. City Social Media Supplemental. City Social Media shall supplement, and not replace, the City's required notices and standard methods of communication.

IX. RULES GOVERNING USE OF CITY TECHNOLOGY RESOURCES.

A. Use of Hardware, Software, Subscription Services, and Similar.

1. Users shall comply with all copyright laws and licensing agreements including but not limited to:

   a. Proprietary Software is not to be reproduced, modified or inappropriately accessed unless authorized under the license agreement.

   b. Not copying any City-owned or licensed software or data to another technology system for personal or external use.

   c. Each piece of proprietary software must have a valid registration and be covered by a Client Access License (CAL).

   d. Having the appropriate documentation to substantiate the legitimacy of the software.

2. Users shall not install or use non City-owned software or hardware with City Technology Resources without prior authorization from the IT Deputy Director or designee.

3. Users shall not take or use City-owned hardware for use at home without prior

authorization from the Department Head or designee.

4. Users shall not install free, purchased, fee-based or subscription on-line services, e-mail software, Internet services, etc. on City Technology Resources without prior approval by the City Manager or designee.

5. Users shall not download data, music, games or videos, whether free or for purchase, with or on City Technology Resources, except when work related and authorized.

6. Users shall not attempt to modify City Technology Resources, software or data files without prior written approval by the City Manager or designee.

7. Users shall report lost or stolen mobile devices, smartphones or other City Technology Resources immediately. The City, at its choosing, may remotely wipe all data, files, images, etc. from these lost or stolen devices.

B. Americans with Disabilities Act (ADA) and Web Content Accessibility Guidelines (WCAG) standards. To create ADA-compliant emails, documents, social media posts and other publicly available content, employees shall follow the WCAG guidelines including but not limited to:

1. Using a legible sans-serif font (e.g., Arial, Calibri, Helvetica) and keeping text at a reasonable size (11 or 12pt).
2. Breaking up text into short paragraphs.
3. Using plain language.
4. Writing descriptive link text.
5. Ensuring sufficient color contrast.
6. Including alt text for images.

The city reserves the right to use available technology to scan and verify compliance with ADA and WCAG standards.

C. Confidential Reports. Users shall not intentionally seek out information on, obtain copies of, modify, or divulge files, reports, and other data, which is private, confidential or not open to public inspection, or release such information unless specifically authorized to do so when the legal conditions for release are satisfied.

D. Copying and Printing. Users shall not intentionally copy or print any software, electronic file, program or data without a prior, good faith determination that such copying or printing is, in fact, permissible. Any efforts to obtain permission shall be documented.

E. Authority, Passwords and Identity. Users shall not:

1. Intentionally seek information on, obtain copies of, or modify files or data without proper authorization. Seeking passwords of others, or the exchange of passwords, is prohibited.

2. Intentionally represent themselves electronically as another user, either on the City network or on the Internet or other on-line services, unless explicitly authorized to do so by the City Manager or designee. Users shall not circumvent established policies defining eligibility for access to information or systems.

3. Allow an unauthorized individual to use the User's identity or use another person's User ID, even if they are City employees, volunteers, or contractors.

F. Disruption of Operations. Users shall not:

1. Intentionally develop programs designed to infiltrate a technology or computing system, and/or damage or alter software components or hardware.

2. Attempt to damage or disrupt the operation of City Technology Resources or telecommunication equipment lines.

G. Acceptable Uses. The following is a non-exclusive representative list of acceptable uses for City Technology Resources:

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

2. Communication and exchange of information for professional development, to obtain training or education, or to discuss issues related to the User's official job duties.

3. Use in applying for, or administering, grants or contracts for City programs.

4. Use to obtain advisory information, standards, research data, analysis, and professional society activities related to official job duties.

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

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

7. For City-related business, communication with professional associations, public agencies, universities, research, and/or continuing education.

H. Unacceptable Uses. The following is a non-exclusive representative list of unacceptable uses for City Technology Resources, unless otherwise a part of your official duties:

1. Use for any purpose that violates local, State or Federal laws or regulations, including, for example, downloading or distributing pirated software or data.

2. Deliberately generating and/or disseminating any virus or any other destructive programming, or experimenting with malicious computer code, such as worms and viruses.

3. Use for purposes not directly related to the mission or work tasks of the User's department during normal business hours unless otherwise permitted in this policy.

4. Use for private business, including commercial advertising, and sending or replying to "chain letters." Use of City computing resources for external consulting is prohibited.

5. Use for any for-profit activities.

6. Accessing, sending, or soliciting sexually oriented messages or images.

7. Libelous, offensive, or harassing statements, including disparagement of others based on their race, national origin, sex, sexual orientation, age, disability, religious, political beliefs, veteran's status, family status, or union affiliation.

8. Use that interferes with, or disrupts, network users, services, or equipment.

9. Use for fund raising, partisan politics, or public relations activities outside of the User's official duties.

10. Use of any Technology Resources while driving. Hands free use while driving should be restricted to business related calls or calls of an urgent nature, and only when absolutely necessary.

11. Transmission of communications or messages which promote unethical practices or violates City or Department Policies, or applicable software licenses agreements, including but not limited to, infringing on copyright, license, trademark, patent, trade secret or other intellectual property rights and laws.

12. Any participation in illegal activities.

13. Using Technology Resources to gain unauthorized access to any electronic communications system, network or file.

14. Transmission of confidential information to unauthorized recipients.

15. Intentionally or negligently disclosing a User's password or account number to any other person who does not have authorization to view that password or account number.

16. Significant consumption of City Technology Resources for non-business related activities (such as video, audio or downloading large files) or excessive time spent using City Technology Resources for non-business purposes (e.g., shopping, personal social networking, or sports-related sites).

17. Knowingly or carelessly performing an act that will interfere with or disrupt the normal operation of computers, terminals, peripherals, or networks, whether within or outside of City Technology Resources (e.g., deleting programs or changing icon names) is prohibited.

I. Accountability.

Users are prohibited from anonymous usage of City Technology Resources. In practice, this means Users must sign-on with their uniquely assigned City User ID before accessing/using City Technology Resources. Similarly, "Spoofing" or otherwise modifying or obscuring a User's IP Address, or any other User's IP Address, is prohibited. Circumventing User authentication or security of any host, network, or account is also prohibited.

J. Personal Use.

City Technology Resources are provided solely for the conduct of City business. However, the City realizes and is aware of the large role technology (especially the Internet and e-mail) plays in the daily lives of individuals. In this context, the City acknowledges that a limited amount of personal use of City Technology Resources is acceptable. This use must not interfere with the User's job responsibilities; it cannot involve any activities expressly prohibited by this or any other City policy; and it should be limited to designated break periods and/or the User's lunch break.

K. Disclaimer.

The City cannot be held accountable for the information that is retrieved via the network. The City will not be responsible for any damages you may suffer, including loss of data resulting from delays, non-deliveries, or service interruptions caused by the City's Systems, System Administrators or User own errors or omissions. Use of any information obtained is at User's own risk. The City makes no warranties (expressed or implied) with respect to: (a) the content of any advice or information received by a User; (b) any costs or charges incurred as a result of seeing or accepting any information; (c) any costs, liability, or damages caused by the way the User chooses to use his or her access to the network; or (d) injuries or damages resulting from exposure to inappropriate, offensive, harmful or controversial materials, whether User initiated or otherwise.

L. Revocation of Authorized Possession.

The City has sole discretion to determine appropriate use and may deny, revoke, suspend, or close any User account at any time. The City reserves the right, at any time, for any reason or no reason, to revoke a User's permission to access, use, or possess City Technology Resources.

M. Restriction of Use.

The City reserves the right, at any time, for any reason or no reason, to limit the manner in which a User may use City Technology Resources in addition to the terms and restrictions already contained in this Policy.

N. Third-Party Technology.

Connecting unauthorized equipment to City Technology Resources, including the unauthorized installation of any software (including shareware and freeware), is prohibited. Only IT personnel or someone authorized by the IT Department may install, troubleshoot, or configure software or hardware.

O. Reporting.

If an Employee becomes aware of any security problem (such as any compromise of the confidentiality of any login or account information) or misuse of City Technology Resources, he/she shall immediately report such information to the Department Head, City Manager, or designee. If you identify or perceive a security problem on the network, notify the City's IT Department; do not demonstrate the problem to others.

P. Enforcement.

1. Record of Activity: User activity with City Technology Resources may be logged by System Administrators. Usage may be monitored or researched in the event of suspected improper City Technology Resources usage or policy violations.

2. Blocked or Restricted Access: The City has sole discretion to determine whether a site, service or protocol will be blocked to Users. User access to specific Internet Resources, or categories of Internet Resources, deemed inappropriate or non-compliant with this Policy may be blocked or restricted. A particular website that is deemed acceptable for use may still be judged a risk to the City (e.g., it could be hosting malware, etc.), in which case it may also be subject to blocking or restriction. Any attempt to circumvent or disable Internet blocking will result in immediate termination of technology privileges.

   The City also retains sole discretion to use hardware or software that screens e-mails for harmful or potentially dangerous content. E-mail messages that contain harmful or potentially dangerous content will not be delivered to or from Users.

X. ETIQUETTE RULES.

The following rules apply to the use of City Technology Resources and the use of Personal Technology Resources while conducting City business.

A. Generally Accepted Standards.

Users must follow generally accepted business practices and current laws regarding the use of e-mail, the Internet, and other on-line services. Users must avoid uses that reflect poorly on their Department, the City, or government in general.

B. City Representation.

The public may perceive a User's postings and e-mail as official City policy. When using e-mail, the Internet, and other on-line services provided by the City, Users should remember that they represent the City. Users shall avoid making statements of personal opinion that may be misinterpreted as official City policy. Users must recognize that anything they put in writing may become a public record, regardless of the original intent of the message.

C. Relationship With Others.

Users must respect the rights of other Users and the Public. Users shall not use City Technology Resources or Personal Technology Resources to invade the privacy of another person, ascertain confidential information, or abuse or harass another person.

D. Ethical Rules and Regulations.

Rules, regulations, guidelines, and case law on ethical behavior of government employees and the appropriate use of government resources apply to the use of City Technology Resources or Personal Technology Resources when conducting City business.

XI. CALIFORNIA PUBLIC RECORDS ACT AND SEARCHING DEVICES AND ACCOUNTS FOR DISCLOSABLE RECORDS.

The California Public Records Act Request ("CPRA") (Government Code section 6250, et seq.) is a law that requires inspection and/or disclosure of governmental records to the public upon

request. E-mails sent by Users, unless otherwise exempt by law, are subject to inspection and disclosure under the CPRA by any person making such a request. Furthermore, e-mails may also be subject to discovery and disclosure as a result of pending litigation involving the City, the City's Employees and elected or appointed officers or officials.

Employees and Users using Personal Technology Resources to send or receive communications constituting City-related business may be required to search their Personal Technology Resources for potentially disclosable records pursuant to a request made under the CPRA. Communications constituting City-related business are those communications that relate in a substantive way to the conduct of the City's business. Communications that are primarily personal in nature or that contain no more than incidental mentions of the City's business may not constitute City-related business communications.

Searches of Personal Technology Resources by an employee shall be conducted during the employee's regular work hours and as otherwise directed by the employee's supervisor.

The City Clerk or designee shall promptly notify an employee or User of the City's receipt of a CPRA request that may implicate City records located on the employee's or User's Personal Technology Resources and shall provide the employee or User with instructions for conducting such searches that identify the specific type and nature of records for which the employee or User is required to reasonably search and collect, as well as the specific type and nature of records that may be withheld because they are not City-related business.

Following an employee's or User's reasonable search of their Personal Technology Resources the employee or User shall be required to sign an affidavit reporting the results of the search, and attesting, under penalty of perjury, that the employee or User has reasonably searched for and collected all potentially disclosable records pursuant to the relevant CPRA request, and that all other information set forth in the affidavit is true and correct.

Alternatively, an employee or User may choose to have the City Attorney perform the search of the employee's or User's Personal Technology Resources to search for records related to City Business that may be disclosable.

XII. VIOLATIONS.

The right to use City Technology Resources is a revocable privilege and a failure to comply with this Policy may result in loss of access to some or all City Technology Resources. In addition, the individual may be subject to disciplinary action, up to and including termination.

TECHNOLOGY USERS AGREEMENT

I, the undersigned, have received and read a copy of City of Clovis Technology Users Policy And Agreement (as revised December 2024) ("Policy"). I understand I have no expectation of privacy regarding my use of City Technology Resources, as defined in the Policy. I understand that messages transmitted over the City's computer network on the Internet and e-mail, as well as my use of all computer files, should be City business-related and that the City's security software may record for management use the Internet address of any site that I visit and keep a record of any network activity in which I transmit or receive any kind of file or message on City Technology Resources, as defined in the Policy.

I further acknowledge that all records on City Technology Resources, as defined in the Policy, and on Personal Technology Resources, as defined in the Policy, and used for City business, may be subject to record retention laws and the California Public Records Act. The City reserves the right to access, audit, and disclose, for whatever reason or purpose, all computer files or messages sent through or in storage on City Technology Resources, as defined in the Policy, or maintained by third-party carriers as applied to City Technology Resources. I further acknowledge that if it is related to City Business and sent, received, or stored on Personal Technology Resources, as defined in the Policy, that I agree to search my Technology Resources for any public records and sign the appropriate documentation for such a search. Alternatively, I acknowledge that I may have the City Attorney's office search my Personal Technology Resource.

I consent to the search and seizure of any City Technology Resources, as defined in the Policy, in my possession, by the City, or the City's authorized representative, at any time of the day or night and by any reasonable means. This consent is unlimited and shall apply to any City Technology Resources that are in my possession, whenever the possession occurs, and regardless of whether the possession is authorized. I waive any rights that may apply to searches of City Technology Resources, as defined in the Policy, under California SB 178 (2015) as set forth in Penal Code sections 1546 through 1546.4.

I recognize that the law and associated policy regarding the use of Technology Resources are continually changing. Therefore, I understand that my regular review of the City policies is required. I agree to abide by and adhere to this Technology Users Policy and understand that failure to comply with this Policy may result in disciplinary actions, up to and including termination.

Employee Signature	Date
Print Employee Name	Print Employee ID Number
Print Department and Division	Print Name of Supervisor
Witness Signature	Date
Print Witness Name	Title

AFFIDAVIT OF SEARCH OF PERSONAL TECHNOLOGY DEVICE

The California Public Records Act Request ("CPRA") (Government Code section 6250, et seq.) is a law that requires inspection and/or disclosure of governmental records to the public upon request. _____ may have used Personal Technology Resources to send or receive communications constituting City-related business and has been asked to search their Personal Technology Resources for records related to _____ in accordance with a request made under the CPRA made by _____ on _____.

In accordance with the above, I, _____, hereby certify and declare as follows:

1. I conducted a search of _____ device(s) for records pertaining to the above CPRA request.
2. The Search was conducted at _____, Clovis, CA. 93612, on _____ at _____a.m./p.m.
3. The result of my search(es) were as follows:

☐ Having conducted a thorough and exhaustive search of the above identified device(s), I found no records related to the CPRA request above.

☐ Having conducted a thorough and exhaustive search of the above identified device(s), I found records related to the CPRA request above, as further described below.

These records are: (Please check all that apply)

☐**Photographic Images** ☐**E-mail** ☐**Text Message** ☐ **Other:**_____

The enclosed records are comprised of the following:

_____

_____

_____

To the best of my knowledge, all of the records referred to above were compiled by me and received at or near the time of the acts, conditions or events recorded. I have delivered all of the records/items requested to _____ _____.

I hereby declare, under penalty of perjury, that the statements made herein are true and correct to the best of my knowledge. I am a witness for the above referenced records provider. I have responded to the request with this affidavit for ALL of the records under my control and custody pertaining to the above request.

_____ _____

Print Name Signature

_____

Date