City of Red Bluff
Administrative Policies & Procedures – Personnel Manual

Subject: Employee Use of Technology Policy	**Number:** 22-9
	Effective Date: 6/18/2024
Departments Affected: All	**Supersedes (Number/Date):** 22-9 10/17/2023
Authority: Section 2.82-A. Red Bluff City Code	**File References:**
	Approved: Approved by City Council on: 6/18/2024

Overview: Access to the internet, electronic mail (email), and electronic information systems may be provided to City of Red Bluff employees for the benefit of the City. The City of Red Bluff authorizes employees to use technology owned by the City subject to the conditions and restrictions set forth under the following guidelines

Applicable to: All employees, vendors, or contractors

Guidelines: City technology, including all City electronic information systems, are considered the property of the City of Red Bluff. For the sake of this rule, "City owned, leased, or subscribed to technology" will include electronic information systems that are used to conduct City business and owned by the City, or a State/Federal entity. The City of Red Bluff may authorize employees to use technology owned by the City as necessary to fulfill the requirements of their position. City technology includes, but is not limited to, computers, the City's computer network including servers and wireless computer networking technology (Wi-Fi), the Internet, email, universal serial bus (USB) drives, wireless access points (routers), tablets, smartphones or smart devices, telephones, cellular telephones, fax machines, photocopiers, printers, wearable technology, any wireless communication device including emergency radios, and/or future technological innovations, whether accessed on or off site, or through City owned or personally owned equipment or devices used to access web-based or cloud-based electronic information from the City.

The use of City technology is a privilege permitted at the City's discretion and is subject to the conditions and restrictions set forth. The City reserves the right to suspend access at any time, without notice or reason. The City may place restrictions on employee access to sites, material, and information, including access to systems from personally owned equipment. In addition, any financial obligations which may arise from unauthorized use may be the responsibility of the employee.

Employee Obligations and Responsibilities
City of Red Bluff employees are responsible for the proper use of City technology at all times. System use shall only occur under the individual account assigned. Employees shall not share their account information, passwords, or other

information used for identification and authorization purposes. Employees shall not gain unauthorized access to files or equipment of others, access electronic resources by using another person's name or electronic identification or send anonymous electronic communications. Employees shall not attempt to access any data, documents, email, or programs in any system for which they do not have authorization and a business need to know.

City employees shall use their assigned City email address to conduct City business. Personal or non-City email addresses shall not be distributed to contacts related to City responsibilities.

Documents, data, inventions, programs, training materials, templates, and scripts developed, generated, or provided by employees, consultants, or contractors for the benefit of the City are the property of the City unless covered by a contractual agreement.

Any usage costs associated with personal use will be the responsibility of the employee.

Prohibited Activities

Equipment, software, and data are the sole property of the City. The unauthorized use of these systems is strictly prohibited and may result in discipline. Employees are prohibited from using City technology for improper purposes, including activities prohibited by law, but not limited to, use of City technology to:

- Access, post, display, or otherwise use material, which is discriminatory, defamatory, offensive, obscene, sexually suggestive, harassing, intimidating, threatening, or disruptive, except as required as a result of conducting criminal investigations.
- Disclose, or in any way cause to be disclosed, confidential or sensitive City, employee, customer, or client information without proper authorization.
- Engage in personal, financial, commercial, or other for-profit activities.
- Engage in the use of City technology for political activities.
- Infringement on copyright, license, trademark, patent, or other intellectual property rights.
- Intentionally disrupt or harm City technology or other City operations (such as destroying City equipment, placing a virus on City computers, adding or removing a computer program without permission, moving, disconnecting, or changing settings on shared computers).
- Install or download unauthorized content.
- Engage in online gambling.
- Engage in or promote unethical practices or violate any law or City policy, administrative regulation, or City practice.

De minimis use of technology for non-profit activities may be authorized at the discretion of the Department Head or their designee.

Use of Artificial Intelligence (A.I.) generative software in the workplace

While use of A.I. generative software is not strictly prohibited, it should be used with caution. Employees must ensure that the following considerations are made when using any A.I. generated tasks:

- Ensure discrimination does not take place with A.I. filtering software systems,

including software from third-party vendors.
- Ensure copyright violations and plagiarism do not take place.
- Ensure accuracy of information.
- Ensure proper security to safeguard the City's computer systems are in place.

Confidentiality
A large quantity of information and/or data processed by City of Red Bluff employees is sensitive and/or confidential in nature. Supervisors and managers are responsible for administering controls which adequately protect the security, confidentiality, availability, and integrity of electronic information and/or data processed by City of Red Bluff departments. City of Red Bluff employees are required to exercise a proper level of protection by taking steps to guard information and assets in their direct control. Providing unauthorized access, releasing data, disclosing information considered confidential in nature, providing electronic information or data which adversely impacts the department, or accessing information for which you are not specifically authorized and don't have a business need to know, is considered a violation of this policy and may subject the employee to disciplinary action.

Safeguarding of Information Assets
All information maintained by the City of Red Bluff is considered a City asset and shall be protected from damage, loss, misuse, or inappropriate disclosure. Department Heads, or their designee, are responsible for administering adequate controls to ensure the security, confidentiality, and integrity of information. Furthermore, all City employees are required to maintain proper levels of protection for information assets.

City technology is intended for use in conducting City business. Employees, contractors, consultants, and other workers should not have an expectation of privacy when using City electronic systems and information assets. All messages created, sent, or retrieved on any City electronic system are the property of City of Red Bluff and may be subject to the Public Records Act. Government Code Sections 6252 and 6254 define the term "public record" for purposes of the Act's disclosure requirements. "Public record" includes most information maintained electronically. Much of the data processed by City of Red Bluff employees is of a sensitive and/or confidential nature. Each City employee must become familiar with the distinctions between the information assets of the employee's department which must be disclosed to the public and those which are exempt from disclosure. Any employee having a question concerning the possible confidentiality of information assets should question their Department Head, or their designee, before releasing any information. Further, any citizen inquiries concerning the department's procedures for processing data should be referred to the Department Head or their designee, who should, when necessary, consult with the City Attorney. Providing access to production data or information without an authorized work related need to know is in direct violation of this policy and could subject the employee to disciplinary action.

The Department Head or their designee reserves the right to monitor and record all use of City technology, including, but not limited to, access to the Internet or social media, communications sent or received from City technology including electronic messages originating outside of the City, or other uses within the jurisdiction of the City. Such monitoring or recording may occur at any time without prior notice for any

legal purposes, record retention and distribution, and/or investigation of improper, illegal, or prohibited activity. Any review or audit of electronic systems and information assets may be conducted by authorized individuals as directed by the Department Head, or their designee, and/or the City Manager, or their designee.

Employees should be aware that their use of City technology cannot be erased or deleted. All files, including emails, remain in the system and can be retrieved even if “deleted”. Employees who access, disclose, alter, or willfully destroy information which adversely impacts the City's services or who violate copyright laws, are and will be subject to applicable federal, state and local criminal laws as well as to disciplinary action pursuant to City policies and procedures.

Computers should be electronically locked when unattended. Where possible, all PCs, laptops, and workstations must be secured with a password-protected screen saver with the automatic activation feature set at 10 minutes or less, or by logging off when unattended. All personal devices must be secured in a manner that requires dual authentication whenever the device is powered on.

All passwords created for or used on any City technology are the sole property of the City. Employees must ensure their passwords are secure and/or protected from disclosure to unauthorized users at all times. The creation or use of a password by an employee on City technology does not create a reasonable expectation of privacy.

If an employee uses a personally owned device to access City technology or conduct City business, the guidelines for use and prohibited activities outlined within this policy will apply. Any such use of a personally owned device may subject the work-related contents of the device and any work-related communications sent or received on the device to disclosure pursuant to lawful subpoena or public records request.

Employees must use extreme caution when opening email attachments. Email attachments may contain viruses, email bombs, or other malicious code. If an employee becomes aware of a security concern, a virus is detected, or misuse of City technology, they shall inform the appropriate city personnel when the user's software does not appear to be functioning correctly. The malfunction - whether accidental or deliberate - may pose an information security risk. If the user, or the user's manager or supervisor, suspects a computer virus infection these steps should be taken immediately:

- Stop using the computer.
- Do not carry out any commands, including commands to save data.
- Do not close any of the computer's windows or programs.
- Do not turn off the computer or peripheral devices.
- If possible, physically disconnect the computer from networks to which it is attached.
- Inform the appropriate personnel or technology provider as soon as possible. Write down any unusual behavior of the computer (screen messages, unexpected disk access, unusual responses to commands) and the time when they were first noticed.
- Write down any changes in hardware, software, or software use that preceded the malfunction.
- Do not attempt to remove a suspected virus.

Those in the department responsible for managing technology should monitor the resolution of the malfunction or incident and report the result of the action with recommendations on action steps to avert future similar occurrences.

Remote Access

An employee working remotely may be responsible for ensuring the security and confidentiality of all City work and information at their remote work site. All information provided by the City for working remotely or used by the employee for job purposes must be protected from unauthorized or accidental access, use, modification, destruction, or disclosure.

The City has an unrestricted right of access to, and disclosure of all data and software being used in connection with working remotely on any City furnished equipment. The information generated or placed into personally owned personal computers being used on City time or undertaken on behalf of the City outside of any City worksite and/or work hours shall be made available for review at the request of appropriate City officials.

Files and online data that belong to the City of Red Bluff can only be accessed from personal computers with permission from the Department Head.

Software Copyrights and Licensing

There is a significant financial liability to the City if software that has not been legally obtained is used on City-owned or leased equipment. All employees and other users of City computers shall adhere to computer software copyright statutes when on City-owned or controlled property. Copyright infringement is a felony. The City will not condone nor contribute to the commission of a felony. Only licensed copies of copyrighted software may be installed on the City's PCs, laptops, servers, or other electronic storage devices.

Consequences for Violation

Violations of any guidelines listed in this policy or laws may result in revocation of an employee's access to City technology and/or discipline, up to and including termination. Violations of the law may be reported to law enforcement.