

City of Red Bluff  
Administrative Policies & Procedures – Personnel Manual

<b>Subject:</b>  Employee Responsibility to Maintain Confidentiality		<b>Number:</b> 22-10
		<b>Effective Date:</b> 10/17/2023
<b>Departments Affected:</b> All		<b>Supersedes (Number/Date):</b>
<b>Authority:</b>  Section 2.82-A. Red Bluff City Code	<b>File References:</b>	
	<b>Approved:</b> Approved by City Council on: 10/17/2023	

**Overview:** Legal obligations and privacy laws require employers to establish processes and procedures to secure and safeguard sensitive employee data against unauthorized access or use. When working with confidential information, employees take on the responsibilities to identify, protect, communicate, and maintain the confidentiality of the information.

**Applicable to:** All employees and contractors with access to confidential information

**Guidelines:** Employees and contractors entrusted with sensitive employee and client information must understand the importance of maintaining confidentiality and privacy in matters including, but not limited to:

- Hiring information – job applications, names of job applicants, resumes, interview notes, employment history, employment assessments, background checks, reference checks, I-9 forms, criminal records, drug test results, physical exams, and Live Scan results.
- Performance and disciplinary documents – reviews, warnings, disciplinary notices, conduct problems, reasonable suspicion drug testing.
- Payroll – direct deposit (banking) information, authorization for deductions, deferred compensation accounts, tax forms, pay garnishments, and financial records.
- Attendance – dates and specific reasons for absences, time off, and leave.
- Personal information - Social Security numbers, address, date of birth, marital status, ethnicity, gender, education level, financial matters, birth certificates, marriage certificates, beneficiaries, home address, phone numbers, and dependents.
- Workplace investigations – complaints of harassment, discrimination, retaliations, threats, witness statements, meeting notes, written summaries of incidents, names of people involved, and other documentation.
- Workplace injury reports – illnesses and injuries, worker’s compensation records.
- Health-related information – medical exam information, statutory leave certifications and medical documentation, leave dates, reasonable accommodations, doctor notes, drug test results, past/present/future

## City of Red Bluff

### AP&P 22-10 Employee Responsibility to Maintain Confidentiality Policy

physical/mental health conditions, and qualifying events.

- Subsequent (after hire) arrests.
- Driving records associated with the Employee Pull Notice or Department of Transportation (medical exams, random drug testing).
- Confidential information of citizens that employees may have access to, including but not limited to contact information, financial and criminal data.

#### **Protecting Confidential Information & Sensitive Data**

All confidential information must be cared for with the appropriate level of physical and electronic security. Confidential information or sensitive data may be stored in emails, electronic documents, printed information, files, computers, laptops, electronic devices, and removable media.

Information must be protected against unauthorized access, unauthorized use, loss, or damage. Some examples of recommended practices include, but are not limited to:

- Not sharing, disclosing, or utilizing another's user identification or passwords or other forms of electronic authorization with other individuals.
- Granting appropriate access to information only to those who "need to know."
- Maintaining up to date security software updates in all computer workstations.
- Password protecting confidential information.
- Keeping portable equipment, storage devices, and removable storage media in a secure location.
- Not leaving computer equipment unattended with sensitive data in view of others or positioning monitors so that others cannot see or obtain sensitive data.
- Logging out, shutting down, or locking the system when leaving your computer unattended for a period of time.
- Storing confidential information, personnel files, medical files, and official/working files in locking filing cabinets or locked storage areas.
- Transporting confidential information, personnel files, and medical files in locking/secure mailbags, briefcases, etc.
- Changing locks, keys, passwords, etc. used to secure confidential information when someone's access authorization changes or a key is lost.
- Placing fax machines or printers which may produce sensitive data in a secure location or, if in a common area, be present at the device to retrieve information when produced.
- Labeling electronic files, hard files, or sealed envelopes as "confidential."
- Removing confidential information from view in office spaces (or turning it over) when those who are not authorized are present.
- Not removing confidential information from premises except as authorized.
- Before sending out emails containing confidential information, confirm names entered are the intended recipients and are in "need-to-know" status.
- Closing office doors or finding a private area to discuss confidential matters.
- Shredding documents when no longer needed.
- Training employees to understand the responsibility and expectation to follow appropriate procedures for the protection of confidential information.
- Reporting any possible unauthorized access, use, or loss of information.

## City of Red Bluff

### AP&P 22-10 Employee Responsibility to Maintain Confidentiality Policy

Confidential and sensitive data may not be provided to prospective employers without consent from the employee or unless otherwise allowed by law.

#### **Department Confidentiality**

Many City employees and contractors are privy to personal information of its citizens on a regular basis. It is paramount that each employee exercise caution in the handling of this information to retain trust from our citizens. Each employee should refer to their own Department's specific confidentiality requirements and adhere to them at all times. Violations of confidentiality should be reported immediately to the Department Head and/or Human Resources to maintain and protect the privacy of our citizens.

A confidentiality agreement shall be signed by each employee upon hire with the City of Red Bluff.

#### **Health Information**

HIPAA, ADA, GINA, and statutory leaves impose very strict rules for handling health-related information obtained through medical examinations and inquiries. Medical and benefit records should be kept separate from personnel files and may be revealed with employees' permission only to certain individuals on a legitimate "need-to-know" basis as defined by specific statutes.

#### **Workplace Investigations**

When conducting investigations, Human Resources and Department Heads or their designee should balance preserving confidentiality and conducting a fair and complete investigation. Human Resources and Department Heads or their designee cannot promise complete confidentiality because other individuals may need to be involved. Detailed information gathered in an investigation will not be divulged other than needed. Instead, employees should be reassured that their issue will be taken seriously and dealt with in a fair and appropriate manner.

Human Resources and Department Heads and their designees will monitor access to confidential information and sensitive data within their department and ensure employee information is protected. Any unauthorized access or breach of confidentiality will be addressed with the offending employee.

**References:** Americans with Disabilities Act; Genetic Information Nondiscrimination Act; Family and Medical Leave Act; Health Insurance Portability and Accountability Act; Penal Code 632.