Records Maintenance and Release

806.1 PURPOSE AND SCOPE

This policy provides guidance on the maintenance and release of [department/office] records. Protected information is separately covered in the Protected Information Policy.

806.2 POLICY

The Capitola Police Department is committed to providing public access to records in a manner that is consistent with the California Public Records Act (Government Code § 7920.000 et seq.).

806.3 CUSTODIAN OF RECORDS RESPONSIBILITIES

The Chief of Police shall designate a Custodian of Records. The responsibilities of the Custodian of Records include but are not limited to:

(a) Managing the records management system for the [Department/Office], including the retention, archiving, release, and destruction of [department/office] public records.

(b) Maintaining and updating the [department/office] records retention schedule including:

1. Identifying the minimum length of time the [Department/Office] must keep records.

2. Identifying the [department/office] division responsible for the original record.

(c) Establishing rules regarding the inspection and copying of [department/office] public records as reasonably necessary for the protection of such records (Government Code § 7922.525; Government Code § 7922.530).

(d) Identifying records or portions of records that are confidential under state or federal law and not open for inspection or copying.

(e) Establishing rules regarding the processing of subpoenas for the production of records.

(f) Ensuring a current schedule of fees for public records as allowed by law is available (Government Code § 7922.530).

(g) Determining how the [department/office]'s website may be used to post public records in accordance with Government Code § 7922.545.

(h) Ensuring that all [department/office] current standards, policies, practices, operating procedures, and education and training materials are posted on the [department/office] website in accordance with Penal Code § 13650.

(i) Ensuring that public records posted on the [Department/Office] website meet the requirements of Government Code § 7922.680 including but not limited to posting in an open format where a record may be retrieved, downloaded, indexed, and searched by a commonly used internet search application.

(j) Ensuring that a list and description, when applicable, of enterprise systems (as defined by Government Code § 7922.700) is publicly available upon request and posted

in a prominent location on the [Department/Office]'s website (Government Code § 7922.710; Government Code § 7922.720).

806.4 PROCESSING REQUESTS FOR PUBLIC RECORDS

Any [department/office] member who receives a request for any record shall route the request to the Custodian of Records or the authorized designee.

806.4.1 REQUESTS FOR RECORDS

Any member of the public, including the media and elected officials, may access unrestricted records of this [department/office], during regular business hours by submitting a written and signed request that reasonably describes each record sought and paying any associated fees (Government Code § 7922.530).

The processing of requests for any record is subject to the following (Government Code § 7922.530; Government Code § 7922.535):

(a) The [Department/Office] is not required to create records that do not exist.

(b) Victims of an incident or their authorized representative shall not be required to show proof of legal presence in the United States to obtain [department/office] records or information. If identification is required, a current driver's license or identification card issued by any state in the United States, a current passport issued by the United States or a foreign government with which the United States has a diplomatic relationship or current Matricula Consular card is acceptable (Government Code § 7923.655).

(c) Either the requested record or the reason for non-disclosure will be provided promptly, but no later than 10 days from the date of request, unless unusual circumstances preclude doing so. If more time is needed, an extension of up to 14 additional days may be authorized by the Custodian of Records or the authorized designee. If an extension is authorized, the [Department/Office] shall provide the requester written notice that includes the reason for the extension and the anticipated date of the response.

1. When the request does not reasonably describe the records sought, the Custodian of Records shall assist the requester in making the request focused and effective in a way to identify the records or information that would be responsive to the request including providing assistance for overcoming any practical basis for denying access to the records or information. The Custodian of Records shall also assist in describing the information technology and physical location in which the record exists (Government Code § 7922.600).

2. If the record requested is available on the [department/office] website, the requester may be directed to the location on the website where the record is posted. If the requester is unable to access or reproduce the record, a copy of the record shall be promptly provided.

(d) Upon request, a record shall be provided in an electronic format utilized by the [Department/Office]. Records shall not be provided only in electronic format unless specifically requested (Government Code § 7922.570; Government Code § 7922.580).

(e) When a record contains material with release restrictions and material that is not subject to release restrictions, the restricted material shall be redacted and the unrestricted material released.

1. A copy of the redacted release should be maintained in the case file for proof of what was actually released and as a place to document the reasons for the redactions. If the record is audio or video, a copy of the redacted audio/video release should be maintained in the [department/office]-approved media storage system and a notation should be made in the case file to document the release and the reasons for the redacted portions.

(f) If a record request is denied in whole or part, the requester shall be provided a written response that includes the statutory exemption for withholding the record or facts that the public interest served by nondisclosure outweighs the interest served by disclosure. The written response shall also include the names, titles, or positions of each person responsible for the denial (Government Code § 7922.000; Government Code § 7922.540).

806.5 RELEASE RESTRICTIONS

Examples of release restrictions include:

(a) Personal identifying information, including an individual's photograph; Social Security and driver identification numbers; name, address, and telephone number; and medical or disability information that is contained in any driver license record, motor vehicle record, or any [department/office] record, including traffic collision reports, are restricted except as authorized by the [Department/Office], and only when such use or disclosure is permitted or required by law to carry out a legitimate law enforcement purpose (18 USC § 2721; 18 USC § 2722).

(b) Social Security numbers (Government Code § 7922.200).

(c) Personnel records, medical records, and similar records that would involve an unwarranted invasion of personal privacy except as allowed by law (Government Code § 7927.700; Penal Code § 832.7; Penal Code § 832.8; Evidence Code § 1043 et seq.).

1. Peace officer personnel records that are deemed confidential shall not be made public or otherwise released to unauthorized individuals or entities absent a valid court order.

2. The identity of any officer subject to any criminal or administrative investigation shall not be released without the consent of the involved officer, prior approval of the Chief of Police, or as required by law.

(d) Victim information that may be protected by statutes, including victims of certain crimes who have requested that their identifying information be kept confidential, victims who are minors, and victims of certain offenses (e.g., sex crimes or human trafficking (Penal Code § 293)). Addresses and telephone numbers of a victim or a witness shall not be disclosed to any arrested person or to any person who may be a defendant in a criminal action unless it is required by law (Government Code § 7923.615; Penal Code § 841.5).

1. Victims of certain offenses (e.g., domestic violence, sexual assault, stalking, human trafficking, elder and dependent adult abuse) or their representatives shall be provided, upon request and without charge, one copy of all incident report face sheets, one copy of all incident reports, a copy of any accompanying or related photographs of the victim's injuries, property damage, or any other photographs that are noted in the incident report, and a copy of 9-1-1 recordings, if any, pursuant to the requirements and time frames of Family Code § 6228.
2. Victims of sexual assault, upon written request, shall be provided a free copy of the initial crime report regardless of whether the report has been closed. Personal identifying information may be redacted (Penal Code § 680.2(b)).

(e) Video or audio recordings created during the commission or investigation of the crime of rape, incest, sexual assault, domestic violence, or child abuse that depicts the face, intimate body part, or voice of a victim of the incident except as provided by Government Code § 7923.750.

(f) Information involving confidential informants, intelligence information, information that would endanger the safety of any person involved, or information that would endanger the successful completion of the investigation or a related investigation. This includes analysis and conclusions of investigating officers (Evidence Code § 1041; Government Code § 7923.605).

1. Absent a statutory exemption to the contrary or other lawful reason to deem information from reports confidential, information from unrestricted agency reports shall be made public as outlined in Government Code § 7923.605.

(g) Local criminal history information including but not limited to arrest history and disposition, and fingerprints shall only be subject to release to those agencies and individuals set forth in Penal Code § 13300.

1. All requests from criminal defendants and their authorized representatives (including attorneys) shall be referred to the [District/CountyAttorney], the City Attorney, or the courts pursuant to Penal Code § 1054.5.

(h) Certain types of reports involving but not limited to child abuse and molestation (Penal Code § 11167.5), elder and dependent abuse (Welfare and Institutions Code § 15633), and juveniles (Welfare and Institutions Code § 827).

(i) Sealed autopsy and private medical information concerning a murdered child with the exceptions that allow dissemination of those reports to law enforcement agents, prosecutors, defendants, or civil litigants under state and federal discovery laws (Code of Civil Procedure § 130).

(j) Information contained in applications for licenses to carry firearms or other files that indicates when or where the applicant is vulnerable or which contains medical or psychological information (Government Code § 7923.800).

(k) Traffic collision reports (and related supplemental reports) shall be considered confidential and subject to release only to the California Highway Patrol, Department

of Motor Vehicles (DMV), other law enforcement agencies, and those individuals and their authorized representatives set forth in Vehicle Code § 20012.

(l) Any record created exclusively in anticipation of potential litigation involving this [department/office] (Government Code § 7927.200).

(m) Any memorandum from legal counsel until the pending litigation has been adjudicated or otherwise settled (Government Code § 7927.205).

(n) Records relating to the security of the [department/office]'s electronic technology systems (Government Code § 7929.210).

(o) A record of a complaint, or the investigations, findings, or dispositions of that complaint if the complaint is frivolous, as defined by Code of Civil Procedure § 128.5, or if the complaint is unfounded (Penal Code § 832.7 (b)(9)).

(p) Any other record not addressed in this policy shall not be subject to release where such record is exempt or prohibited from disclosure pursuant to state or federal law, including but not limited to provisions of the Evidence Code relating to privilege (Government Code § 7927.705).

(q) Information connected with juvenile court proceedings or the detention or custody of a juvenile. Federal officials may be required to obtain a court order to obtain certain juvenile information (Welfare and Institutions Code § 827.9; Welfare and Institutions Code § 827.95; Welfare and Institutions Code § 831).

806.6 SUBPOENAS AND DISCOVERY REQUESTS

Any member who receives a subpoena duces tecum or discovery request for records should promptly contact a supervisor and the Custodian of Records for review and processing. While a subpoena duces tecum may ultimately be subject to compliance, it is not an order from the court that will automatically require the release of the requested information.

Generally, discovery requests and subpoenas from criminal defendants and their authorized representatives (including attorneys) should be referred to the District Attorney, City Attorney or the courts.

All questions regarding compliance with any subpoena duces tecum or discovery request should be promptly referred to legal counsel for the [Department/Office] so that a timely response can be prepared.

806.7 RELEASED RECORDS TO BE MARKED

Each page of any written record released pursuant to this policy should be stamped in a colored ink or otherwise marked to indicate the [department/office] name and to whom the record was released.

Each audio/video recording released should include the [department/office] name and to whom the record was released.

806.8 SEALED RECORD ORDERS

Sealed record orders received by the [Department/Office] shall be reviewed for appropriate action by the Custodian of Records. The Custodian of Records shall seal such records as ordered by the court. Records may include but are not limited to a record of arrest, investigation, detention, or conviction. Once the record is sealed, members shall respond to any inquiry as though the record did not exist (Penal Code § 851.8; Welfare and Institutions Code § 781).

When an arrest record is sealed pursuant to Penal Code § 851.87, Penal Code § 851.90, Penal Code § 851.91, Penal Code § 1000.4, or Penal Code § 1001.9, the Records Supervisor shall ensure that the required notations on local summary criminal history information and police investigative reports are made. Sealed records may be disclosed or used as authorized by Penal Code § 851.92.

806.8.1 SEALED JUVENILE ARREST RECORDS

Upon receiving notice from a probation department to seal juvenile arrest records pursuant to Welfare and Institutions Code § 786.5, the Records Supervisor should ensure that the records are sealed within 60 days of that notice and that the probation department is notified once the records have been sealed (Welfare and Institutions Code § 786.5).

806.9 SECURITY BREACHES

The Records Supervisor shall ensure notice is given anytime there is a reasonable belief an unauthorized person has acquired either unencrypted personal identifying information or encrypted personal information along with the encryption key or security credential stored in any [Department/Office] information system (Civil Code § 1798.29).

Notice shall be given as soon as reasonably practicable to all individuals whose information may have been acquired. The notification may be delayed if the [Department/Office] determines that notification will impede a criminal investigation or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

For the purposes of this requirement, personal identifying information includes an individual's first name or first initial and last name in combination with any one or more of the following (Civil Code § 1798.29):

(a) Social Security number

1. Driver license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual
2. Account number or credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account
3. Medical information
4. Health insurance information

5. Information or data collected by Automated License Plate Reader (ALPR) technology
6. Unique biometric data
7. Genetic data

(b) A username or email address, in combination with a password or security question and answer that permits access to an online account

806.9.1 FORM OF NOTICE

(a) The notice shall be written in plain language, be consistent with the format provided in Civil Code § 1798.29 and include, to the extent possible, the following:

1. The date of the notice.
2. Name and contact information for the Capitola Police Department.
3. A list of the types of personal information that were or are reasonably believed to have been acquired.
4. The estimated date or date range within which the security breach occurred.
5. Whether the notification was delayed as a result of a law enforcement investigation.
6. A general description of the security breach.
7. The toll-free telephone numbers and addresses of the major credit reporting agencies, if the breach exposed a Social Security number or a driver license or California identification card number.

(b) The notice may also include information about what the Capitola Police Department has done to protect individuals whose information has been breached and may include information on steps that the person whose information has been breached may take to protect him/herself (Civil Code § 1798.29).

(c) When a breach involves an online account, and only a username or email address in combination with either a password or security question and answer that would permit access to an online account, and no other personal information has been breached (Civil Code § 1798.29):

1. Notification may be provided electronically or in another form directing the person to promptly change either his/her password or security question and answer, as applicable, or to take other appropriate steps to protect the online account with the [Department/Office] in addition to any other online accounts for which the person uses the same username or email address and password or security question and answer.
2. When the breach involves an email address that was furnished by the Capitola Police Department, notification of the breach should not be sent to that email address but should instead be made by another appropriate medium as prescribed by Civil Code § 1798.29.

806.9.2 MANNER OF NOTICE

(a) Notice may be provided by one of the following methods (Civil Code § 1798.29):

1. Written notice.
2. Electronic notice if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 USC § 7001.
3. Substitute notice if the cost of providing notice would exceed $250,000, the number of individuals exceeds 500,000 or the [Department/Office] does not have sufficient contact information. Substitute notice shall consist of all of the following:
   (a) Email notice when the [Department/Office] has an email address for the subject person.
   (b) Conspicuous posting of the notice on the [department/office]'s webpage for a minimum of 30 days.
4. Notification to major statewide media and the California Information Security Office within the California Department of Technology.

(b) If a single breach requires the [Department/Office] to notify more than 500 California residents, the [Department/Office] shall electronically submit a sample copy of the notification, excluding any personally identifiable information, to the Attorney General.

806.10 DECLINE TO FILE NOTIFICATION

Prosecuting office decline to file notifications received by the Department shall be reviewed for appropriate action by the Custodian of Records. The Custodian of Records shall update any criminal information reported to Department of Justice, update local RMS and issue appropriate certificat(s).

806.11 SECURITY INCIDENT RESPONSE PLAN

The Records Supervisor shall ensure the following guidelines are met anytime a computer intrusion is suspected.

Computer intrusion is defined as a compromise to any computer system by gaining unauthorized access.

a. The person who suspects or discovers the incident must contact the Police Records Supervisor. If the Police Records Supervisor is unavailable, the Police Captain or Chief of Police will be contacted. The following is a list of possible sources that may discover incidents requiring contact information:

- City IT
- Current Assistant to City Manager
- Police Sergeants, Police Officers or other Police Staff
- Records Division Personnel

· Netcom / Santa Cruz County Regional 9-1-1

· Santa Cruz County Sheriff's Department IT Division and/or Records Supervisors

Each of the above listed sources has been provided this Incident Response Plan

b. Regardless of whether the person discovering the incident is a member of the IT Department or not, in the order listed, one of the following people will be immediately contacted:

· Capitola Police Records Manager: (831) 212-4063 24/7

· Capitola Police Captain: (831) 471-1141 24/7

· Capitola Police Chief: (831) 471-1141 24/7

c. Whomever is contacted in section b, will contact City IT and the effected department(s). If the Police Records Supervisor is contacted, she/he will also notify the Police Captain and/or Chief of Police. The contacted person, along with City IT will document the following information:

· The name of the caller.

· Time of the call.

· Contact information about the caller.

· The nature of the incident.

· What equipment or persons were involved?

· Location of equipment or persons involved.

· How incident was detected.

· When the event was first noticed that supported the idea that the incident occurred.

· Is the equipment affected business critical?

· What is the severity of the potential impact?

· Name of system being targeted, along with operating system, IP address, and location.

· IP address and any information about the origin of the attack.

· A team will be formed with the affected departments and will meet or discuss the situation over the telephone and determine a response strategy.

· Is the incident real or perceived?

· Is the incident still in progress?

· What data or property is threatened and how critical is it?

· What is the impact on the business should the attack succeed? Minimal, serious, or critical?

· What system or systems are targeted, where are they located physically and on the network?

· Is the incident inside the trusted network?

· Is the response urgent?

· Can the incident be quickly contained?

· Will the response alert the attacker and do we care?

· What type of incident is this? Example: virus, worm, intrusion, abuse, damage.

d. The incident will be categorized into the highest applicable level of one of the following categories:

· Category one - A threat to public safety or life

· Category two - A threat to sensitive data

· Category three - A threat to computer systems

· Category four - A disruption of services

e. The team will use forensic techniques, including reviewing system logs, looking for gaps in logs, reviewing intrusion detection logs, and interviewing witnesses and the incident victim to determine how the incident was caused. Only authorized personnel should be performing interviews or examining evidence, and the authorized personnel may vary by situation and the organization.

f. The team will recommend changes to prevent the occurrence from happening again or infecting other systems.

· Upon management approval, the changes will be implemented.

· Team members will restore the affected system(s) to the uninfected state. They may do any or more of the following:

· Re-install the affected system(s) from scratch and restore data from backups if necessary. Preserve evidence before doing this.

· Make users change passwords if passwords may have been sniffed.

· Be sure the system has been hardened by turning off or uninstalling unused services.

· Be sure the system is fully patched.

· Be sure real time virus protection and intrusion detection is running.

· Be sure the system is logging the correct events and to the proper level.

g. Documentation—the following shall be documented:

· How was the incident discovered?

· The category of the incident.

· How the incident occurred, whether through email, firewall, etc.

· Where the attack came from, such as IP addresses and other related information about the attacker.

· What the response plan was.

· What was done in response?

· Whether the response was effective.

· Evidence Preservation—make copies of logs, email, and other communication.

· Keep lists of witnesses.

· Keep evidence as long as necessary to complete prosecution and beyond in case of an appeal.

h. Notify proper external agencies—Police documentation and other appropriate agencies if prosecution of the intruder is possible. See below contact information.

· Criminal Prosecution – Santa Cruz County District Attorney (831) 454-2400

· State of California Attorney General's Office: https://oag.ca.gov

i. Assess damage and the cost to the organization.

· Estimate both damage to equipment and containment efforts.

j. Review response and update policies as needed to take preventative steps so the intrusion can't happen again. Document responses for the following:

· Consider whether an additional policy could have prevented the intrusion.

· Consider whether a procedure or policy was not followed which allowed the intrusion, and then consider what could be changed to ensure that the procedure or policy is followed in the future.

· Was the incident response appropriate? How could it be improved?

· Was every appropriate party informed in a timely manner?

· Were the incident-response procedures detailed and did they cover the entire situation? How can they be improved?

· Have changes been made to prevent a re-infection? Have all systems been patched, systems locked down, passwords changed, anti-virus updated, email policies set, etc.?

· Have changes been made to prevent a new and similar infection?

· Should any security policies be updated?

What lessons have been learned from this experience?

806.12 DIGITAL MEDIA HANDLING & PROTECTION

Only Personnel who meet DOJ/FBI security requirements shall be allowed to perform the following:

a. When any type of computer, cell phone, copier, scanner, printer or other types of electronic devices containing any information defined by California Department of Justice or FBI standards as being confidential or otherwise prohibited from any other type of use not law enforcement related is retired or otherwise no longer being used or housed in a secure area as defined by DOJ and FBI, shall be thoroughly sanitized, that is overwriting at least three times or degauss electronic media (degaussing destroys the data by disrupting the magnetic field) before disposal or release for reuse by unauthorized individuals to make sure that the information remains protected.

b. Any type of digital storage device, including but not limited to flash, jump, or other types of portable storage containing any information defined by California Department of Justice or FBI standards as being confidential or otherwise prohibited from any other type of use, not law enforcement related shall be thoroughly sanitized, that is overwriting at least three times or degauss electronic media (degaussing destroys the data by disrupting the magnetic field), shredded by cross-cut shredder, smashed or incinerated prior to leaving the custody of the police department to make sure the information remains protected.

The Capitola Police Department has the following policies for the protection of information:

- Secure doors to get into the building
- Code access to secured areas
- Police Department staff members escort all non-Police and city employees who have not completed or are out of compliance in completing the mandatory biannual Security Awareness Training, throughout the building
- Information handling protection and destruction
- Documents are kept in locked drawers when not in use by the Officer
- 24/7 camera surveillance

The Capitola Police Department personnel shall, for their area of responsibility, receive, disseminate, document, and react to validated security alerts and bulletins in compliance with the CJIS Security Policy. Any relevant alerts shall be forwarded to the agency SPOC by the appropriate supervisor. Based upon the information contained in the alerts or bulletins, the information will be disseminated to appropriate Capitola Police Department personnel. Based upon the information contained in the alerts or bulletins, appropriate actions will be taken by the IT Division staff.

806.13 DESTRUCTION OF CRIMINAL HISTORIES

Upon summarization of criminal history in a police report, or upon conclusion of the use of a criminal history for other authorized purposes, the employee who is using the criminal history shall be responsible for its immediate destruction.

As a means of making sure compliance with this policy, when criminal histories are encountered in the Police Department files and determined to no longer be in use as part of an ongoing investigation. Part of ongoing police investigations (Generally, in police investigations where a

statute of limitations has expired), the employee shall immediately remove it from the file and destroy it.

Criminal history printouts shall be destroyed in such a manner to render them completely unreadable and impossible to reconstruct, and in a manner that renders it impossible for an unauthorized person to glean any information from them. This generally means shredding them with an approved, cross-cut shredder.

806.14 RELEASE OF AUDIO OR VIDEO RECORDINGS RELATED TO CRITICAL INCIDENTS

Video and audio recordings related to critical incidents shall be released upon a proper public record request and subject to delayed release, redaction, and other release restrictions as provided by law (Government Code § 7923.625).

For purposes of this section, a video or audio recording relates to a critical incident if it depicts an incident involving the discharge of a firearm at a person by an officer, or depicts an incident in which the use of force by an officer against a person resulted in death or in great bodily injury (as defined by Penal Code § 243(f)(4)) (Government Code § 7923.625).

The Custodian of Records should work as appropriate with the Chief of Police or the Internal Affairs Unit supervisor in determining what recordings may qualify for disclosure when a request for a recording is received and if the requested recording is subject to delay from disclosure, redaction, or other release restrictions.

806.14.1 DELAY OF RELEASE

Disclosure of critical incident recordings during active criminal or administrative investigations may be delayed as follows if disclosure would substantially interfere with the investigation, such as by endangering the safety of a witness or a confidential source:

(a) Disclosure may be delayed up to 45 days from the date the [Department/Office] knew or reasonably should have known about the incident.

(b) Delay of disclosure may continue after the initial 45 days and up to one year if the [Department/Office] demonstrates that disclosure would substantially interfere with the investigation.

(c) Any delay of disclosure longer than one year must be supported by clear and convincing evidence that disclosure would substantially interfere with the investigation (Government Code § 7923.625).

806.14.2 NOTICE OF DELAY OF RELEASE

When there is justification to delay disclosure of a recording, the Custodian of Records shall provide written notice to the requester as follows (Government Code § 7923.625):

(a) During the initial 45 days, the Custodian of Records shall provide the requester with written notice of the specific basis for the determination that disclosure would substantially interfere with the investigation. The notice shall also include the estimated date for the disclosure.

(b) When delay is continued after the initial 45 days, the Custodian of Records shall promptly provide the requester with written notice of the specific basis for the determination that the interest in preventing interference with an active investigation outweighs the public interest in the disclosure, and the estimated date for the disclosure. The Custodian of Records should work with the Chief of Police in reassessing the decision to continue withholding a recording and notify the requester every 30 days.

Recordings withheld shall be disclosed promptly when the specific basis for withholding the recording is resolved.

806.14.3 REDACTION

If the Custodian of Records, in consultation with the Chief of Police or the authorized designee, determines that specific portions of the recording may violate the reasonable expectation of privacy of a person depicted in the recording, the [Department/Office] should use redaction technology to redact portions of recordings made available for release. The redaction should not interfere with the viewer's ability to fully, completely, and accurately comprehend the events captured in the recording, and the recording should not otherwise be edited or altered (Government Code § 7923.625).

If any portions of a recording are withheld to protect the reasonable expectation of privacy of a person depicted in the recording, the Custodian of Records shall provide in writing to the requester the specific basis for the expectation of privacy and the public interest served (Government Code § 7923.625).

806.14.4 RECORDINGS WITHHELD FROM PUBLIC DISCLOSURE

If the reasonable expectation of privacy of a person depicted in the recording cannot adequately be protected through redaction, and that interest outweighs the public interest in disclosure, the [Department/Office] may withhold the recording from the public, except that the recording, either redacted or unredacted, shall be disclosed promptly, upon request, to any of the following (Government Code § 7923.625):

(a) The person in the recording whose privacy is to be protected, or the person's authorized representative.

(b) If the person is a minor, the parent or legal guardian of the person whose privacy is to be protected.

(c) If the person whose privacy is to be protected is deceased, an heir, beneficiary, designated immediate family member, or authorized legal representative of the deceased person whose privacy is to be protected.

If the [Department/Office] determines that this disclosure would substantially interfere with an active criminal or administrative investigation, the Custodian of Records shall provide the requester with written notice of the specific basis for the determination and the estimated date of disclosure (Government Code § 7923.625).

The [Department/Office] may continue to delay release of the recording from the public for 45 days with extensions as provided in this policy (Government Code § 7923.625).

806.14.5 ACCESS TO PROTECTED INFORMATION

All employees and volunteers of the police department who have physical access to any protected or criminal history information must be fingerprinted and fingerprints must be submitted to DOJ before they have physical access to and the viewing of criminal history information. This includes, but is not limited to peace officer staff, support staff, volunteer staff, and part-time staff.

No employee or volunteer of the Police Department who has a felony conviction shall have physical access to or view criminal history information.

Unauthorized access, including access for other than a legitimate work-related purpose, is prohibited and may subject a member to administrative action pursuant to the Personnel Complaints Policy and/or criminal prosecution.