

Protected Information

609.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the access, transmission, release and security of protected information by employees of the Yolo County Probation Department. This policy addresses the protected information that is used in the day-to-day operation of the Department and not the public records information covered in the Records Maintenance and Release Policy.

609.2 AUTHORITY

This policy is established pursuant to the mandate of the Regulations Regarding Security of Criminal Offender Record Information in California, Title 11, California Code of Regulations. Other authority includes Penal Code section 11105, which delineates who has access to Criminal Offender Record Information (CORI), and Penal Code sections 11140 through 11144, which establishes penalties for the improper use of rap sheets.

609.3 RESPONSIBILITIES

The Chief Probation Officer shall select an employee of the Department to coordinate the use of protected information.

The responsibilities of this position include, but are not limited to:

- (a) Ensuring employee compliance with this policy and with requirements applicable to protected information, including requirements for the National Crime Information Center (NCIC) system, National Law Enforcement Telecommunications System (NLETS), Department of Motor Vehicle (DMV) records and California Law Enforcement Telecommunications System (CLETS).
- (b) Developing, disseminating and maintaining procedures that adopt or comply with the U.S. Department of Justice's current Criminal Justice Information Services (CJIS) Security Policy.
- (c) Developing, disseminating and maintaining any other procedures necessary to comply with any other requirements for the access, use, dissemination, release and security of protected information.
- (d) Developing procedures to ensure training and certification requirements are met.
- (e) Resolving specific questions that arise regarding authorized recipients of protected information.
- (f) Ensuring security practices and procedures are in place to comply with requirements applicable to protected information.

609.4 ACCESS TO PROTECTED INFORMATION

Protected information shall not be accessed in violation of any law, order, regulation, user agreement, Yolo County Probation Department policy and training. Only those employees who

Yolo County Probation Department

Policy Manual

Protected Information

have completed applicable training and met any applicable requirements, such as a background check, may access protected information, and only when the member has a legitimate work-related reason for such access.

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

609.4.1 RELEASE OF CONFIDENTIAL OFFENDER RECORD INFORMATION (CORI)

Only the persons listed below are authorized to release CORI:

- (a) Agency CLETS Coordinator
- (b) CLETS Security Officer
- (c) Chief Probation Officer or designee
- (d) Division Manager or designee
- (e) Superintendent of the Juvenile Detention Facility or designee.

Each authorized person releasing CORI is responsible for ensuring that each request granted appears legitimate and the requester is an authorized recipient with a right and need to know.

*Reference CORI Procedures

609.5 RELEASE OR DISSEMINATION OF PROTECTED INFORMATION

Protected information may be released only to authorized recipients who have both a right to know and a need to know.

An employee who is asked to release protected information that should not be released should refer the requesting person to a Supervisor for information regarding a formal request.

Unless otherwise ordered or when an investigation would be jeopardized, protected information maintained by the Department may generally be shared with authorized persons from other law enforcement agencies who are conducting a related investigation. Any such information should be released through the Records Section to ensure proper documentation of the release (see the Records Maintenance and Release Policy).

Protected information, such as Criminal Justice Information (CJI), which includes Criminal History Record Information (CHRI), should generally not be transmitted by radio, cellular telephone or any other type of wireless transmission to members in the field or in vehicles through any computer or electronic device, except in cases where there is an immediate need for the information to further an investigation or where circumstances reasonably indicate that the immediate safety of officers, other Department employees or the public is at risk.

Nothing in this policy is intended to prohibit broadcasting warrant information.

Protected Information

609.5.1 REVIEW OF CRIMINAL OFFENDER RECORD

Individuals requesting to review their own California criminal history information shall be referred to the Department of Justice. (Pen. Code § 11121.)

Individuals shall be allowed to review their arrest or conviction record on file with the Department after complying with all legal requirements regarding authority and procedures in Penal Code sections 11120 through 11127. (Pen. Code § 13321)

609.6 SECURITY OF PROTECTED INFORMATION

The Chief Probation Officer will select employees of the Department to act as a CLETS Agency Administrator and a CLETS Security Officer to oversee the security of protected information.

The responsibilities of these positions include, but are not limited to:

- (a) Developing and maintaining security practices, procedures and training
- (b) Ensuring federal and state compliance with the CJIS Security Policy and the requirements of any state or local criminal history records systems
- (c) Establishing procedures to provide for the preparation, prevention, detection, analysis and containment of security incidents including computer attacks
- (d) Tracking, documenting and reporting all breach of security incidents to the Chief Probation Officer and appropriate authorities

* Reference Media Protection Procedures and Media Disposal Procedures

609.6.1 CUSTODIAN(S) OF CRIMINAL RECORDS

The Custodian(s) of Criminal Records shall be responsible for the security, storage, dissemination and destruction of criminal records, and will serve as a primary contact for the California Department of Justice for any related issues. The Chief Probation Officer may appoint other Department employees to the role of Custodian of Criminal Records, who will share the same responsibilities regarding criminal records.

The Chief Probation Officer or designee will ensure that he or she makes the appropriate applications and notifications to the California Department of Justice regarding the Department's Custodian of Criminal Record appointments, per the requirements of Penal Code section 11102.2

This subsection is not intended to interfere with any other employee acting as a custodian of records for other statutory purposes but is narrowly tailored to address issues of criminal history records.

609.6.2 EMPLOYEE RESPONSIBILITIES

Employees accessing or receiving protected information shall ensure the information is not accessed or received by persons who are not authorized to access or receive it. This includes leaving protected information, such as documents or computer databases, accessible to others when it is reasonably foreseeable that unauthorized access may occur (e.g., on an unattended table or desk; in or on an unattended vehicle; in an unlocked desk drawer or file cabinet; on an unattended computer terminal).

Protected Information

609.7 TRAINING PROGRAM

All personnel authorized to process or release CORI shall be required to complete a training program prescribed by the California Department of Justice. The assigned training officer and/or designee shall coordinate the course to provide training in the proper use, control, and dissemination of CORI.

609.8 PENALTIES FOR MISUSE OF RECORDS

Penal Code sections 11140 and 11144 make it a misdemeanor to furnish, buy, receive, or possess Department of Justice rap sheets without authorization by a court, statute, or case law.

Any person authorized by law to receive a Department of Justice rap sheet or information obtained from a rap sheet who knowingly furnishes the rap sheet or information to a person who is not authorized by law to receive such a rap sheet or information is guilty of a misdemeanor under Penal Code section 11142.

Title 11, California Administrative Code section 702 provides that authorized persons or agencies violating the Regulations Regarding the Security of Criminal Offender Record Information in California may lose direct access to CORI maintained by the California Department of Justice.

Divulging the content of any criminal record to anyone other than authorized personnel is a violation of Policy Manual section 336.4.6.

Employees who obtain, or attempt to obtain, information from the department files other than that to which they are entitled in accordance with their official duties is a violation of Policy Manual section 336.4.6.

Employees who violate any portion of this section shall be subject to discipline up to and including termination.

609.9 CALIFORNIA RELIGIOUS FREEDOM ACT

Employees shall not release personal information from any agency database for the purpose of investigation or enforcement of any program compiling data on individuals based on religious belief, practice, affiliation, national origin or ethnicity. (Govt. Code § 8310.3.)