

**RIVERSIDE COUNTY SHERIFF'S DEPARTMENT
STAN SNIFF, SHERIFF**

TO: All Personnel

DATE: November 21, 2018

FROM: Stan Sniff, Sheriff

**Department Directive #18-132
Supersedes DD#10-019, #15-059, and #16-074**

**RE: Automated License Plate Reader (ALPR) Technology Usage and
Privacy Protection**

The use of Automated License Plate Reader (ALPR) technology is a valuable law enforcement tool that can be beneficial in several ways, including assisting with identifying stolen or wanted vehicles, vehicles associated with missing or wanted people, and stolen license plates. ALPR systems and information are also useful to capture license plates and vehicle images in or near crime scenes, identify locations and patterns where wanted vehicles were located or frequent, and are an effective investigative resource. However, ALPR systems also inadvertently gather data related to vehicles that are not directly related to a law enforcement purpose, so adequate safeguards need to be followed to prevent data from being misused and ensure privacy is properly protected. Therefore, appropriate protocols must be followed in the gathering, storage and use of ALPR data to ensure its integrity, maintain community confidence, and comply with applicable laws.

The use of ALPR systems and information is restricted to official and legitimate law enforcement purposes only. Department members shall not use, or allow others to use, the ALPR equipment or related database for any unauthorized purpose.

1. ALPR systems and information databases shall only be utilized by personnel employed by the Department in conjunction with their assigned duties.
2. Department members shall verify ALPR alerts with CLETS or Dispatch before taking any enforcement action.
3. No Department member may operate ALPR systems or access ALPR information without first completing a Department-approved online training course. The Ben Clark Training Center is responsible for establishing and maintaining this training course, which will be administered through DocRead. The training will be automatically distributed to employees based on their rank, classification, station/facility, or division. At a minimum, this training will cover general ALPR use, legal requirements, privacy issues, and ALPR data retention and destruction guidelines. At the conclusion of the training course, each participant's unique ALPR system username and password will be activated.

4. In the event that the Department utilizes an independent contractor to operate ALPR systems on the Department's behalf, then such personnel shall first be required to complete training that at a minimum covers ALPR access and use, legal requirements, privacy issues, and ALPR data retention and destruction guidelines.
5. Department members shall only use their own assigned username and password when accessing any ALPR system. Username and passwords are specific to each authorized Department member and shall not be shared. When searching ALPR information, Department members must document a justification for the inquiry (preferably a file number or other clear identifier linking the access to a legitimate use). The Technical Services Bureau (TSB) may conduct random audits to ensure compliance with justification for the query.
6. ALPR information may be released to other authorized and verified law enforcement officials and agencies for legitimate law enforcement purposes only. ALPR information gathered and retained may be used and shared with prosecutors or others as required for criminal filings, discovery, court proceeding, or other legal purpose. Under no circumstance may the Department, or any Department member, sell, share or transfer ALPR data to anyone except another public safety agency, and only as otherwise permitted by law.
7. Any printed ALPR information must be destroyed using a secure method (station and facility specific). ALPR information shall not be disposed of in a regular trash or recycling bin.
8. Public record requests for ALPR related information shall be routed to CPRA@Riversidesheriff.org for disposition in accordance with the California Public Records Act.
9. Electronic data gathered during ALPR usage is the property of the Riverside County Sheriff's Department. The approved ALPR vendor will maintain responsibility for adherence to protocols involving information security in accordance with FBI CJIS security policy. The approved vendor will also be responsible for executing retention and/or deletion routines of electronically stored data as specified by the Riverside County Records Management and Archive Policy and in compliance with applicable laws.
10. Any information sharing will be done in accordance with applicable laws and policies of the Department. Any compromise in the ALPR system will immediately be reported to the Chief Deputy of Support Services.
11. Department members using ALPR systems shall report errors they encounter by sending an electronic mail to ALPR@riversidesheriff.org. The email should include, at a minimum, the vehicle license plate number, file number or case information used to access the ALPR information, a description of the incorrect data, and how the information can be corrected.

12. Authorized Department vendors with access to systems containing ALPR data shall maintain reasonable security procedures and practices, including operational, administrative, technical, and physical safeguards, to protect ALPR information from unauthorized access, destruction, use, modification, or disclosure.
13. Sheriff's TSB will ensure a copy of this policy is appropriately placed on the Department's website where it can be viewed by the public. This requirement remains in effect as long as the Department uses any ALPR system.
14. Sheriff's TSB will require that ALPR login and query records are retained for a period of two years unless the information has been requested for investigative or other legal reasons. Any records retained must contain, at a minimum, the following information:
 - a) The date and time ALPR information was accessed;
 - b) The username of the person who accessed the information;
 - c) The license plate number or other data elements used to query the ALPR system;
 - d) The stated purpose for accessing the information.

EDP Code for ALPR Incidents:

To assist in identifying incidents where ALPR systems directly lead to the recovery of vehicles or the arrest of suspects, an EDP code has been created. Effective immediately, the following EDP code is to be utilized when reporting ALPR-related incidents: 25T1-N

The ALPR EDP code shall be used as a secondary EDP and is required on any written report where this technology was effectively utilized during an investigation. For example, if an abandoned stolen vehicle is located via a notification from the ALPR system, the recovery should be documented as a Stolen Vehicle Recovery and the corresponding EDP for the recovery should be first on the Form A. On the second line of the Form A, "ALPR" should be entered in the offense section and 25T1-N should be entered in the EDP code section. This practice will ensure proper identification of ALPR-related incidents and crime trends.

Example:

<small>10. OFFENSES - CODE SECTION</small> 10851(a) CVC	<small>CRIME</small> Stolen Vehicle Recovery	<small>COUNTS</small> 01	<small>11.EDP CODE</small> 15B1-N
<small>12. OFFENSES - CODE SECTION</small> ALPR	<small>CRIME</small>	<small>COUNTS</small>	<small>13.EDP CODE</small> 25T1-N

Retention of ALPR Information:

ALPR records retained by the Department will be maintained, safeguarded, and purged according to all applicable laws and policies. Consistent with Government Code § 26202 and Riverside County Records Management and Archive Policy A-43, raw ALPR information will be retained for a period of two years and then be deleted. ALPR data that may be needed for active or probable litigation, is the subject of an active public records request, or is needed for auditing purposes shall be maintained until the underlying matters are fully resolved before being deleted. ALPR information documented in criminal and/or

administrative reports will follow the same retention period as the report. ALPR information placed in evidence will remain secured as evidence until destroyed per Department policy. Deletion of ALPR data will follow the steps specified pursuant to Board of Supervisors policy and in accordance with the Sheriff Department's records retention schedule.

Official Custodian/ Owner of ALPR System and Information:

The Commander of TSB, acting on behalf of the Riverside County Sheriff's Department, is responsible for implementing the provisions of this usage and privacy policy as the official custodian/owner of the ALPR system, and ALPR information covered herein.

Public Hearing:

Before implementing an ALPR program within Riverside County or any local jurisdiction, an opportunity for public comment will be set at a regularly scheduled public meeting of the appropriate local governing body. Once held, the dates and locations of these public comment opportunities will be posted on the Sheriff's website for historical reference.

SS: jp