PROVIDENCE POLICE DEPARTMENT

HEADQUARTERS

COLONEL OSCAR L. PEREZ

CHIEF OF POLICE

TYPE OF ORDER	NUMBER/SERIES	ISSUE DATE	EFFECTIVE DATE
General Order	350.05	9/4/2026	9/4/2026
SUBJECT TITLE		**PREVIOUSLY ISSUED DATES**	
Automated License Plate Readers (ALPR)		11/25/2025; 7/27/2022	
REFERENCE		**RE-EVALUATION DATE**	
CALEA 41.3.9		As Needed	
SUBJECT AREA		**DISTRIBUTION**	
Law Enforcement Operations		All Sworn Personnel	

PURPOSE

The purpose of this policy is to provide guidance for the capture, storage, and use of digital data obtained using Automated License Plate Reader (ALPR) technology for criminal investigations.

POLICY

The policy of the Providence Police Department is to utilize ALPR technology to capture and store digital license plate data and images for criminal investigations while recognizing the established privacy rights of the public. All data and images gathered by the ALPR are for the official use of this department. Because such data may contain confidential information, it is not open to public review. The placement of the ALPR shall be determined by crime analysis data and severity in consultation with the vendor providing the ALPR service and shall be law enforcement sensitive. The Chief of the Providence Police Department shall have the exclusive authority for placement of the ALPR.

The ALPR technology, also known as Automated License Plate Recognition (ALPR), allows for the automated detection of license plates along with the vehicle make, model, color and unique identifiers through the Providence Police Department's ALPR system and the vendor's vehicle identification technology. The technology is used by the Providence Police Department to convert data associated with vehicle license plates and vehicle descriptions for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates and missing persons. It may also be used to gather information related to active warrants, electronic surveillance, suspect interdiction, stolen property recovery and active criminal investigations. The ALPR technology shall not be used for traffic violations, outstanding fines or any civil infractions.

DEFINITIONS

Automated License Plate Reader (ALPR): A device that uses cameras and computer technology to compare digital images to lists of known information of interest.
ALPR Operator: Trained Department members who may utilize ALPR system/equipment. ALPR operators may be assigned to any position within the Department, and the ALPR Administrator may order the deployment of the ALPR systems for use in various efforts.

ALPR Administrator: The Chief of Police or their designee, serves as the ALPR Administrator for the Department.

Hot List: A list of license plates associated with vehicles of interest compiled from one or more data bases including, but not limited to, National Crime Information Center (NCIC), Rhode Island Division of Motor Vehicles (RI DMV), Local "Be On The Lookout" (BOLO's), etc.
Vehicles of Interest: Including, but not limited to vehicles which are reported as stolen; display stolen license plates or tags; vehicles linked to missing and/or wanted persons and vehicles flagged by the Department of Motor Vehicle Administration or law enforcement agencies.

Detection: Data obtained by an ALPR of an image (such as a license plate) within public view that was read by the device, including potential images (such as the plate and description of vehicle on which it was displayed), and information regarding the location of the ALPR system at the time of the ALPR's read.

Hit: Alert from the ALPR system that a scanned license plate number may be in the National Crime Information Center (NCIC) or other law enforcement database for a specific reason including, but not limited to, being related to a stolen car, wanted person, missing person, domestic violation protective order or terrorist-related activity.

PROCEDURE

I.

A. ALPR Administrators

The Commanding Officer of the Investigative Bureau or their designee shall be responsible for compliance with the following:

1. Only properly trained sworn officers, and police dispatchers are allowed access to the ALPR system or to collect ALPR information.
2. Ensuring that training requirements are completed for authorized users.
3. ALPR system monitoring to ensure the security of the information and compliance with applicable privacy laws.
4. Maintaining the title and name of the current designee overseeing the ALPR operation.
5. Continually working with the BCI Unit on the retention and destruction of ALPR data.

6. Ensuring this policy, related procedures, and the transparency portal are conspicuously posted on the department's website.

7. Any and all current or future external agencies granted permission to use or review ALPR technology, data, and/or footage shall agree, through a formal written agreement, to the provisions contained in the Providence Code of Ordinances §1, Chapter 18 ½. For those agencies that do not agree, permission to access data in Providence shall be denied.

B. ALPR USE

Use of an ALPR is restricted to the purposes outlined below:

1. Department members shall not use or allow others to use the equipment or database records for any unauthorized purpose.

2. An ALPR shall only be used for official law enforcement business/criminal investigations.

3. An ALPR may be used in conjunction with any routine patrol operation or criminal investigation; reasonable suspicion or probable cause is not required before using an ALPR.

4. Partial license plates and unique vehicle descriptions reported during major crimes should be entered into the ALPR system to identify suspect vehicles.

5. The officer should verify an ALPR response through the Rhode Island Law Enforcement Telecommunications System (RILETS) before taking enforcement action that is based solely on an ALPR alert unless exigent circumstances exist. Once an alert is received, the operator shall confirm that the observed license plate from the system matches the license plate of the observed vehicle before any law enforcement action is taken because of an ALPR alert, the alert will be verified through a RILETS inquiry via MDT or through Dispatch. Officers will not take any police action that restricts the freedom of any individual based solely on an ALPR alert unless it has been validated. Because the ALPR alert may relate to a vehicle and may not relate to the person operating the vehicle, officers are reminded that they need to have reasonable suspicion and/or probable cause to make an enforcement stop of any vehicle. (For example, if a vehicle is entered into the system because of its association with a wanted individual, officers should attempt to visually match the driver to the description of the wanted subject prior to making the stop or should have another legal basis for making the stop.)

6. Designation of hot lists to be utilized by the ALPR system shall be made by the Chief of Police or their designee. Hot lists shall be obtained or compiled from sources consistent with the purposes of the ALPR system set forth in this policy. Hot lists utilized by the department's ALPR system may be updated by agency sources more

frequently than the department may be uploading them and thus the department's ALPR system will not have access to real time data. Occasionally, there may be errors in the ALPR system's read of a license plate. Therefore, an alert alone shall not be a basis for police action (other than following the vehicle of interest). Prior to initiation of a stop of a vehicle or other intervention based on an alert, officers shall undertake the following:

a. An officer must receive confirmation, from Communications Center or other department computer device, that the license plate is still stolen, wanted, or otherwise of interest before proceeding (absent exigent circumstances).

b. Officers shall visually verify that the license plate of interest matches identically with the image of the license plate number captured (read) by the ALPR, including both the alphanumeric characters of the license plate, state of issue, and vehicle descriptors before proceeding. Officers alerted to the fact that an observed motor vehicle's license plate is entered as a Hot Plate (hit) in a specific BOLO (be on the lookout) list are required to make a reasonable effort to confirm that a wanted person is in the vehicle and/or that a reasonable basis exists before an officer would have a lawful basis to stop the vehicle.

c. Officers will clear all stops from hot list alerts by indicating the positive ALPR Hit, i.e., with an arrest or other enforcement action. If it is not obvious in the text of the call as to the correlation of the ALPR Hit and the arrest, then the officer shall update with the Communications Center personnel and original person inputting the vehicle in the hot list (hit).

d. General Hot Lists will be automatically downloaded into the ALPR system a minimum of once a day with the most current data overwriting the old data.

e. All entries and updates of specific Hot Lists within the ALPR system will be documented by the requesting department member within the appropriate general offense report. As such, specific Hot Lists shall be approved by the ALPR Administrators or designee before initial entry within the ALPR system. The updating of such a list within the ALPR system shall thereafter be accomplished pursuant to the approval of the department member's immediate supervisor. The hits from these data sources should be viewed as informational; created solely to bring the officers attention to specific vehicles that have been associated with criminal activity.

f. All Hot Plates and suspect information entered into the ALPR system will contain the following information at a minimum:

    1) Entering department member's name;

    2) Related case number; and

3) Short synopsis describing the nature of the originating call.

7. No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.

8. To ensure proper operation and facilitate oversight of the ALPR system, all users will be required to have individual credentials for access and use of the systems and/or data, which can be fully audited.

C. Communications

The Communications Center shall be responsible for monitoring the ALPR system. All hits received will sound an alert in the Communications Center. Upon receiving an alert, on-duty dispatch personnel will immediately verify the captured plate (photo) with the wanted/suspect plate number displayed as the wanted plate from either NCIC, RILETS or the department Hotlist. Upon visual verification of the plate/tag the dispatcher will manually verify the wanted plate with NCIC to determine if it is still outstanding as wanted.

1. Verified RILETS/NCIC hits will result in an immediate dispatch to the post car as a priority call.

    a. Stolen License Plates – On all stolen license plate hits, dispatch personnel will check the stolen plate through DMV records. Should the stolen plate come back to a vehicle with the same make, model, and color of the vehicle that the stolen plate is currently being displayed on, the dispatched units shall be immediately advised of that fact. Officers should be advised that the plate may be the secondary license plate and not stolen.

2. Hotlist Alerts may include specific instructions to field personnel. Those instructions will also be relayed to on - duty personnel at the time of dispatch. i.e., “stop only with probable cause and identify occupants.”

3. Communications personnel shall be responsible for notification of the NCIC/RILETS information submitting jurisdiction of the recovery of wanted stolen vehicles and the status of any arrests. Notification shall be as per NCIC/RILETS protocols.

D. Officers

Patrol Officers shall be responsible for monitoring ALPR cameras on their assigned beat. Upon receipt of an ALPR notification, on duty personnel will respond to the area of the capture and look for the suspect vehicle. If the vehicle is located, proper traffic stop procedures shall be followed based upon the type of hit, officer observations and other factors present. The first officer identifying the wanted vehicle should wait for appropriate back-up before initiating a traffic stop or engaging the vehicle. If a felony car stop is conducted, it will be in accordance with *General Order 350.05 Traffic Enforcement.*

Investigative Personnel Responsibilities

1. Investigating personnel shall utilize ALPR data to assist in the identification of suspects involved in criminal activity in the City of Providence.

2. Investigating personnel shall have search access enabling them to search the database for vehicles and/or persons of interest.

3. When Investigating personnel utilize ALPR data to assist in identification of a suspect or vehicle linked to criminal activity, the ALPR data shall be downloaded from the system and attached to the investigative report as evidence.

E. Permitted/Impermissible Uses

The ALPR system, and all data collected, is the property of the Providence Police Department. Department personnel may only access and use the ALPR system for official and legitimate law enforcement purposes consistent with this policy. The following uses of the ALPR system are specifically prohibited:

1. **Invasion of Privacy:** Except when done pursuant to a court order such as a search warrant, it is a violation of this policy to utilize the ALPR to record license plates except those of vehicles that are exposed to public view (e.g., vehicles on a public road or street, or that are on private property but whose license plate(s) are visible from a public road, street, or a place to which members of the public have access, such as the parking lot of a shop or other business establishment).

2. **Harassment or Intimidation:** It is a violation of this policy to use the ALPR system to harass and/or intimidate any individual or group.

3. **Use Based on a Protected Characteristic:** It is a violation of this policy to use the ALPR system or associated scan files or hot lists solely because of a person’s, or group's race, gender, religion, political affiliation, nationality, ethnicity, sexual orientation, disability, or other classification protected by law.

4. **Personal Use:** It is a violation of this policy to use the ALPR system or associated scan files or hot lists for any personal purpose.

5. **First Amendment Rights:** It is a violation of this policy to use the ALPR system or associated scan files or hot lists for the purpose or known effect of infringing upon First Amendment rights.

6. It is a violation of this policy and local ordinance to use the ALPR technology to engage in targeted electronic surveillance to collect or retain information about the lawful activities of targeted individuals or groups without reasonable suspicion that such activities relates to criminal activity or a judicial warrant is obtained specific to the time, place, and target of the surveillance.

7. It is a violation of this policy and local ordinance to use the ALPR technology to enforce, comply, or assist with federal immigration enforcement, or collect or retain information regarding a person's demographic identity, such as race and/or ethnicity, unless presented with a judicial warrant.

8. It is a violation of this policy and local ordinance to grant federal immigration authorities access to any facial recognition technology used, utilized or managed by law enforcement, unless presented with a judicial warrant naming a specific person or evidence sought.

9. Anyone who engages in an impermissible use of the ALPR system or associated scan files, or hot lists may be subject to criminal prosecution, civil liability, and/or administrative sanctions pursuant to and consistent with the collective bargaining agreement and department policies.

F. Data Collection and Retention

1. The Commanding Officer of the Investigative Bureau or their designee shall be responsible for ensuring systems and processes are in place for the proper collection and retention of ALPR data. Data will be transferred from vehicles to the designated storage in accordance with department procedures.

2. All ALPR data downloaded to the server should be stored for no longer than thirty (30) days and in accordance with the established Rhode Island Records Retention Schedule (LG6) in accordance with the Secretary of State's Office. Thereafter, ALPR data should be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a discovery request or other lawful action to produce records. In those circumstances the applicable data should be downloaded from the server onto portable media and logged into evidence in accordance with department policy.

3. ALPR vendor, Flock Safety, will store the data (data hosting) and ensure proper maintenance and security of data stored in their data towers. Flock Safety will purge their data at the end of the 30 days of storage. However, this will not preclude Providence Police Department from maintaining any relevant vehicle data obtained from the system after that period pursuant to the established City of Providence retention schedule mentioned above or outlined elsewhere.

4. Information gathered or collected, and records retained by Flock Safety cameras or any other CPD ALPR system will not be sold, accessed, or used for any purpose other than legitimate law enforcement or public safety purposes. It shall be exclusively used for criminal investigations by law enforcement departments.

G. Accountability and Safeguards

All data will be closely safeguarded and protected by both procedural and technological means. The Providence Police Department will observe the following safeguards regarding access to and use of stored data:

1. All non-law enforcement requests for access to stored ALPR data shall be processed in accordance with applicable law.

2. All ALPR data downloaded to a mobile device, computer or MDT shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date, and time.

3. Persons approved to access ALPR data under these guidelines are permitted to access the data for official law enforcement purposes when the data relates to a specific criminal investigation.

4. ALPR data may be released to other authorized and verified law enforcement officials and agencies for legitimate law enforcement purposes.

5. Every ALPR Detection Browsing Inquiry must be documented by either the associated Providence Police case number or incident number, and/or a reason for the inquiry.

6. For records release, refer to General Order 410.01 -Central Records Systems

7. The Providence Police Department will create a transparency portal available to the public which will outline the APLR policy and metrics of the system to include:

    a. Hot List sources;

    b. Data retention;

    c. Number of operational cameras;

    d. Organizations with access to cameras;

    e. Number of total plate-reads in a 30-day period; and

    f. Number of searches in a 30-day period.

H. ALPR Data Detection Browsing Audits

1. It is the responsibility of the Office of Professional Standards (OPS) or the Chief of Police's designee to ensure that an audit is conducted of ALPR detection browsing inquiries on a quarterly basis. The department will audit a sampling of the ALPR system utilization from the prior period to verify proper use in accordance with the above authorized uses. The audit shall randomly select at least 10 detection browsing inquiries conducted by department employees during the

preceding period and determine if each inquiry meets the requirements established in policy section.

2. The audit shall be documented in the form of an internal department memorandum to the Chief of Police. The memorandum shall include any data errors found so that such errors can be corrected. After review by the Chief of Police or their designee, the memorandum and any associated documentation shall be filed and retained by the Office of Professional Standards.

I. Releasing ALPR Data

1. The ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law. The agency makes a written request for the ALPR data that includes:

   a. The name of the agency;

   b. The name of the person requesting; and

   c. The intended purpose of obtaining the information.

2. The request is reviewed by the Chief of Police or their designee and approved before the request is fulfilled.

3. Providence Police Department does not permit the sharing of ALPR data gathered by the city or its contractors/subcontractors for purpose of federal immigration enforcement, these federal immigration agencies include Immigrations and Customs Enforcement (ICE) and Customs and Border Patrol (CPB).

4. The approved request is retained on file by the Providence Police Department. Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed in accordance with applicable law.

J. Training

The Commanding Officer of the Investigative Bureau or their designee and the Training Academy shall ensure that members receive department-approved training for those authorized to use or access the ALPR system.

K. Oversight

The Providence Police Department will provide monthly reports to the Providence City Council for one (1) year and will thereafter provide annual quarterly reports.

The Providence External Review Authority (PERA) will be provided audit reports, quarterly reports and the ability to access the system for the

purpose of auditing for compliance in the LPR program provided, however, that specific information shall not be made public.

APPROVED:

COLONEL OSCAR L. PEREZ
CHIEF OF POLICE