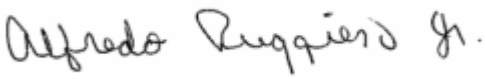





# NORTH PROVIDENCE POLICE DEPARTMENT



## GENERAL ORDER 350.11

<b>SUBJECT: AUTOMATED LICENSE PLATE READERS (ALPR)</b>		
Issue Date: <b>09/25/25</b>	Effective Date: <b>09/25/25</b>	Distribution: <b>All Sworn Personnel</b>
Subject Area: <b>INVESTIGATION</b>		CALEA Standard: <b>41.3.9</b>
Amends/Rescinds: <b>NONE</b>		Review Date: <b>As Needed</b>   Pages: <b>9</b>
<b>Per order of the Chief of Police:</b>  		<b>Approved by the Director of Public Safety:</b>  
<i>This General Order is for departmental use only and does not apply in any criminal or civil proceeding. This General Order should not be construed as creation of a higher legal standard of safety or care in an evidentiary sense with respect to third party claims. Violations of this General Order will only form the basis for departmental administrative sanctions. Violations of law will form the basis for civil and criminal sanctions in a recognized judicial setting.</i>		

### I. PURPOSE

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

### II. POLICY

The policy of the North Providence Police Department is to utilize ALPR technology to capture and store digital license plate/vehicle description data, and images 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 the public review.

### III. DISCUSSION

The ALPR technology, also known as License Plate Recognition (LPR), allows for the automated detection of license plates along with the vehicle make, model, color and unique identifiers through the North Providence Police Department's ALPR system and the vendor's vehicle identification technology. The technology is used by the North 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, homeland security, electronic surveillance, suspect interdiction, stolen property recovery, and active criminal investigations.

#### IV. DEFINITIONS

- A. **ALPR ADMINISTRATOR:** A designee assigned by the Chief of Police who serves as the ALPR Administrator for the Department.
- B. **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 investigations.
- C. **ALERT:** A visual and/or auditory notice that is triggered when the ALPR system receives a potential hit on a license plate.
- D. **ALERT DATA:** Information captured by an ALPR relating to a license plate that matches the license plate on a Hotlist.
- E. **ALPR DATA:** Data captured by the ALPR cameras of an image (such as license plate and description of a vehicle on which it is displayed) within public view that was read by the device, including GPS coordinates and date and time information of the ALPR system at the time of the ALPR's read.
- F. **ALPR DATA QUERY LOGS:** A record of a search or query of ALPR data.
- G. **AUTOMATIC LICENSE PLATE RECOGNITION (ALPR):** Technology that uses high-speed cameras combined with sophisticated computer algorithms capable of converting the images of license plates and vehicles to electronically readable data. The ALPR System captures an image of a license plate and converts it to a text file using Optical Character Recognition (OCR) technology. The technology also compares the digital images of license plates to the CJIS-NCIC Hot file database. The ALPR System is configured as either fixed, mobile, or portable.
- H. **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.
- I. **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.
- J. **HOTLIST:** License plate numbers of vehicles of interest, such as: stolen vehicles, vehicles owned by persons of interest, vehicles associated with AMBER Alerts, Missing Child Alerts, Missing College Student Bulletins, Silver Alerts, Be On Look Out (BOLO), Attempt to Locate (ATL), and Wanted or Missing Person broadcasts or bulletins in which a license plate number is included, or other license plate numbers of interest entered by the Department or an authorized officer.

- K. **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.

**V. ALPR ADMINISTRATOR**

- A. A designee assigned by the Chief of Police who shall be responsible for compliance with the following:
1. Only properly trained personnel 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. Continually working with the Administrative Services Division on the retention and destruction of ALPR data; and
  5. Ensuring this policy, related procedures, and the transparency portal are clearly posted on the department's website.
- B. Personnel will report any damage to department ALPR equipment, via the chain of command, to the ALPR Administrator who will coordinate any necessary repairs.
- C. Repairs or modifications to the ALPR systems hardware or software, shall only be made by authorized sources or employees as determined by the ALPR administrator.

**VI. PROCEDURES**

A. ALPR USE

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

1. An ALPR shall only be used for official law enforcement purposes.
2. Department members shall not use or allow others to use the equipment or database records for any unauthorized purpose.
3. No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.
4. 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.

5. ALPR operators shall not use personal devices to take or upload images to the ALPR system.
6. An ALPR may be used in conjunction with routine patrol operations or criminal investigations; reasonable suspicion or probable cause is not required before using the ALPR system.
7. Partial license plates and unique vehicle descriptions reported during major crimes should be entered into the ALPR system to identify suspect vehicles.
8. If practicable, the officer shall verify an ALPR alert through the Rhode Island Law Enforcement Telecommunications System (RILETS) before taking enforcement action that is based solely on an ALPR alert. 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. The alert will be verified through a RILETS inquiry via MDT or through Dispatch. Officers shall 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).
9. When Department members utilize ALPR data to assist in the identification of a suspect or vehicle linked to criminal activity, the ALPR data shall be downloaded from the system and attached to the report as evidence.

## B. CUSTOM HOTLISTS

1. Entries into Custom Hotlists can be completed by the Criminal Investigative Division and Supervisors. The Hotlist groups are defined as “Criminal Investigative Division Hotlist” (restricted access) and “Department Wide Hotlist.”
2. All entries and updates of specific Hotlists within the ALPR system will be documented by the requesting department member within the appropriate offense report. Entries by the Patrol Division into the Hotlist will be completed by the officer’s immediate supervisor or Officer in Charge (OIC). Hits from these data sources are informational and are intended to alert officers to vehicles that have been associated with criminal activity.
3. All Hot Plates and suspect information entered into the Hotlist will contain the following information at a minimum:
  - a. Requesting Department member’s name;
  - b. Authorizing Supervisor;

- c. Related case number; and
  - d. Short synopsis describing the nature of the originating call.
4. The ALPR Administrator designates approved Hotlists, which must align with the system's purposes under this policy. Hotlists may be updated by external sources more frequently than the department uploads them, so data is not real-time. Errors in plate reads may occur; therefore, an alert alone cannot justify police action beyond following the vehicle of interest. Before initiating a vehicle stop or other action based on an alert, officers shall:
- a. Receive confirmation from the Communications Center or from the MDT, that the license plate is still stolen, wanted, or otherwise of interest before proceeding (absent exigent circumstances).
  - b. 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. Document all Hotlist stops by recording the ALPR hit and resulting enforcement action. If the link between the hit and the action is unclear in the call record, officers shall update Communications and notify the originating agency that entered the vehicle on the Hotlist.

## C. COMMUNICATIONS

The Communications Center shall monitor the ALPR system. When a hit alert sounds, dispatch personnel shall verify the captured plate image against the wanted plate in NCIC, RILETS, or the Department Hotlist, and then confirm the plate remains listed as wanted.

- 1. Verified RILETS/NCIC hits will result in an immediate dispatch of the beat officer 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 ID occupants.”

3. Communications personnel shall notify the originating NCIC/RILETS jurisdiction when a wanted or stolen vehicle is recovered and when any related arrests are made. Such notifications shall be made in accordance with established NCIC/RILETS protocols.

#### D. PATROL OFFICER RESPONSIBILITIES

1. Patrol officers shall have access to receive alerts and view shared Hotlists.
2. Patrol Officers will monitor ALPR cameras in their assigned area. Upon receipt of an ALPR alert, on duty personnel (if available) 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.

#### E. INVESTIGATIVE PERSONNEL/ SUPERVISOR RESPONSIBILITIES

1. Criminal Investigative personnel and Supervisors shall utilize ALPR data to assist in the identification of suspects involved in criminal activity in the town of North Providence.
2. Criminal Investigative Personnel and Supervisors shall have search access enabling them to search the database for vehicles and/or persons of interest.
3. Criminal Investigative Personnel and Supervisors shall have access to add, edit, and/or update custom Hotlists.

#### F. PERMITTED/IMPERMISSIBLE USES

The ALPR system, and all data collected, is the property of the North 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, associated scan files, or Hotlists 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, associated scan files, or Hotlists for any personal purpose;
5. **First Amendment Rights:** It is a violation of this policy to use the ALPR system, associated scan files, or Hotlists for the purpose or known effect of infringing upon First Amendment rights; and
6. Anyone who engages in an impermissible use of the ALPR system, associated scan files, or Hotlists may be subject to criminal prosecution, civil liability, and/or administrative sanctions pursuant to and consistent with the [Law Enforcement Officers' Due Process, Accountability, and Transparency Act](#) (sworn personnel), associated collective bargaining agreements, and department policies (all personnel).

#### G. DATA COLLECTION AND RETENTION

1. The ALPR Administrator shall be responsible for ensuring systems and processes are in place for the proper collection and retention of ALPR data.
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 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. The ALPR vendor, Flock Safety, will store and secure data in their servers and automatically purge it after 30 days. This does not prevent the North Providence Police Department from retaining any relevant vehicle data beyond 30 days in accordance with the State of Rhode Island's established retention schedule, or outlined elsewhere.
4. ALPR data gathered, stored, or retained by the North Providence Police Department shall not be sold, accessed, or used for any purpose other than legitimate law enforcement or public safety purposes.

#### H. ACCOUNTABILITY AND SAFEGUARDS

All data will be closely safeguarded and protected by both procedural and technological means. The North 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 or department related civil or administrative action.
4. ALPR data may be released to other authorized and verified law enforcement officials and agencies for legitimate law enforcement purposes only.
5. Every ALPR detection browsing inquiry (search) shall be documented with an associated North Providence Police case/incident number, and the reason for the inquiry (stolen vehicle, missing person, domestic violence...etc.) must be included.
6. The North 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. Hotlist hits;
  - b. Data retention;
  - c. Number of operational cameras;
  - d. Number of total plate reads in a 30-day period; and
  - e. Number of searches in a 30-day period.

#### I. ALPR DATA DETECTION BROWSING AUDITS

1. The Office of Professional Standards (OPS) or the Chief of Police's designee shall conduct a quarterly audit of ALPR detection browsing inquiries. The audit will randomly review at least 10 inquiries from the preceding period to ensure each complies with authorized uses outlined in policy.
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 OPS.

#### J. 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 requesting agency must submit 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 must be reviewed by the Chief of Police or their designee and approved before the request is fulfilled.
  3. North Providence Police Department does not permit the sharing of ALPR data gathered by the Department 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. All approved requests shall be retained on file in accordance with appropriate records retention schedules.
  5. Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will not be processed.

**K. TRAINING**

1. The ALPR Administrator shall ensure that members receive department-approved training for those authorized to use or access the ALPR system.