NORTH PROVIDENCE POLICE DEPARTMENT

GENERAL ORDER 350.11

SUBJECT: **AUTOMATED LICENSE PLATE READERS (ALPR)**			
Issue Date: **09/25/25**	Effective Date: **10/22/26**	Distribution: **All Sworn Personnel**	
Subject Area: **INVESTIGATION**		CALEA Standard: **41.3.9**	
Amends/Rescinds: **Policy Effective: 09/25/25**		Review Date: **As Needed**	Pages: **11**
Per order of the Chief of Police:		**Approved by the Director of Public Safety:**	
Alfredo Ruggiero Jr.			

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. 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 for valid law enforcement purposes 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.

The ALPR technology allows for the automated detection of license plates along with the vehicle make, model, color and unique identifiers through the 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 a valid law enforcement purpose to include investigations relating to a missing or endangered person or a person associated with human trafficking and active criminal investigations. ALPR technology shall not be used for traffic violations, outstanding fines or any civil infractions, immigration enforcement or enforcement of a crime not recognized in the State of Rhode Island. Officers shall receive appropriate training before being authorized to use ALPR cameras for law enforcement purposes.

III. DEFINITIONS

A. **AUTOMATIC LICENSE PLATE READERS (ALPR):** A device that uses cameras and computer technology to convert images or license plates to electronically readable data and compares digital images to lists of known information of interest.

B. **ALPR DATA:** Scan files, alert data, and any other documents or data generated by, or obtained through, utilization of the ALPR system.

C. **ALPR ADMINISTRATOR:** A designee assigned by the Chief of Police who serves as the ALPR Administrator for the Department.

D. **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, for valid law enforcement purposes.

E. **HOTLIST**: A list of license plates associated with vehicles of interest compiled from one or more databases, including but not limited to: National Crime Information Center (NCIC), RI Division of Motor Vehicles (DMV), local BOLO's (Be on the lookout), etc.

F. **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 Division of Motor Vehicle's Administration or law enforcement agencies.

G. **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.

H. **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.

I. **VALID LAW ENFORCEMENT PURPOSE**: A purpose for information/intelligence gathering development, or collection, use, retention, or sharing that furthers the authorized function and activities of a law enforcement agency, which may include the prevention of crime, ensuring the safety of the public, furthering officer safety while adhering to law and agency policy designed to protect the privacy, civil rights, and civil liberties of individuals.

IV. PROCEDURES

A. **ALPR ADMINISTRATOR(S)**

A designee or designees 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. Nothing herein shall preclude the department from restricting access to any of its employees holding these positions;

2. Ensuring that initial and in-service 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(s) overseeing the ALPR operation and all ALPR Operators.

5. Ensuring this policy, related procedures, and the transparency portal are clearly posted on the department's website; and

6. 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 this Policy. For those agencies that do not agree, permission to access data shall be denied.

7. Personnel will report any damage to department ALPR equipment, via the chain of command, to the ALPR Administrator who will coordinate any necessary repairs.

8. Repairs or modifications to the ALPR systems hardware or software, shall only be made by authorized service providers.

B. ALPR USE

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

   a. A valid law enforcement purpose such as being used as part of a criminal investigation into an alleged violation of state or federal criminal law where there is reasonable suspicion that a crime was committed.

   b. As part of an active investigation related to a missing or endangered person or a person associated with human trafficking.

   c. To receive notifications related to a missing or endangered person, a person with an outstanding judicial warrant, a person associated with human trafficking, a stolen vehicle or a stolen plate.

2. ALPR cameras will be positioned to capture only vehicles that are exposed to public view (e.g., vehicles on a public roadway or a place that is publicly accessible, such as public parking lots).

3. 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.

C. ENTRY AND VERIFICATION INTO THE ALPR SYSTEM

1. License plates, including partial plates if applicable, and unique vehicle descriptions reported during an alleged criminal incident should be entered into the ALPR system to identify suspect vehicles.

2. Unless exigent circumstances exist making it impractical, officers 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 shall 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).

3. Designations of hot lists to be utilized by the ALPR system shall be made only after the approval of an ALPR Administrator. Entries into Custom Hotlists may be made by members of the Criminal Investigative Division and authorized Supervisors. The Hotlist groups are defined as “Criminal Investigative Division Hotlist” (restricted access) and “Department Wide Hotlist.”

4. 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. 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 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 with the image of the complete or partial 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 a hit 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. All vehicle and suspect information entered into the ALPR system will contain the following information at a minimum:

i. Related case number; and

ii. Short synopsis describing the nature of the originating call.

d. Officers shall document all Hotlist stops by recording the ALPR hit and resulting enforcement action.

D. AUTHORIZED COLLECTION, PURPOSES AND USE OF ALPR DATA/GUIDELINES FOR USE

1. A Police Department is authorized to query government or commercial ALPR data contingent on a respective sharing agreement, memorandum of understanding, or intergovernmental agreement in place that is consistent with this Policy.

2. ALPR data may be utilized by the Department personnel for valid law enforcement purposes including, but not limited to, the following:

a. Locate missing children, elderly, and at-risk individuals, including responding to Amber, Silver, and Purple Alerts;

b. Locate witnesses and victims of violent crime;

c. Locate stolen, wanted, and subject of investigation vehicles;

d. Locate and apprehend individuals subject to arrest warrants or otherwise lawfully sought by law enforcement;

e. Support local, state, federal, and tribal public safety departments in the identification of vehicles associated with targets of criminal investigations, including investigations of serial crimes;

f. Protect participants at special events; and

g. Protect critical infrastructure sites.

E. PROHIBITED USE

The ALPR system, and all data collected, is the property of the Police Department and not Department personnel. Department personnel may only access and use the ALPR system for a valid law enforcement purpose consistent with this policy. The following uses of the ALPR system are specifically prohibited:

1. **Invasion of Privacy:** The ALPR system shall only be used to capture license plates 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) except as authorized through the issuance of a court order such as a search warrant.

2. **Harassment or Intimidation:** It is an explicit 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 or Class**: 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, color, gender, gender identity, religion, political affiliation, nationality, ethnicity, sexual orientation, age, disability or other classification protected by law.

4. **Personal Use**: It is a violation of this policy to use, or allow others to use, the ALPR system or associated scan files or hot lists for any personal purpose. The ALPR shall only be used for a valid law enforcement 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. **Determination of Immigration Status:** It is a violation of this policy to use the ALPR system or associated scan files or hot lists for the purposes of determining an individual's legal status within the United States or assisting with the enforcement of potential violations of federal civil immigration law.

7. **Abortion Ban Enforcement/Obstructing of Reproductive Rights**: It is a violation of this policy to use the ALPR system or associated scan files or hot lists for the purposes of enforcing abortion ban or restricting a person's ability to exercise their reproductive rights.

8. Any matter where the criminal investigation concerns a crime that is not recognized under Rhode Island law.

F. AUTHORIZATION TO SHARE ALPR INFORMATION

1. Department employees are prohibited from sharing, disseminating, forwarding, or otherwise providing access to any data, images or alerts to U.S. Immigration and Customs Enforcement or any external agency when the purpose of that agency or request is the enforcement of potential violations of federal civil immigration law.

2. Department employees are prohibited from sharing, disseminating, forwarding, or otherwise providing access to any data, images, or alerts to any third party that is not a law enforcement agency. Notwithstanding, the Department may receive ALPR data from a third party, non-law enforcement agency.

3. Department employees are prohibited from sharing, disseminating, forwarding, or otherwise providing access to any data, images, or alerts to any private citizen or entity without the express authorization of the Chief of Police.

G. ACCOUNTABLILITY AND SAFEGUARDS

All data will be closely safeguarded and protected by both procedural and technological means. The ALPR Administrator(s) shall be responsible for ensuring the Department observes 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. ALPR data downloaded to a 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. ALPR data shall never be downloaded, screenshot or in any way saved to a mobile device. A mobile device can only be used to scan and view ALPR data.

3. Persons approved to access ALPR data under these guidelines are permitted to access the data for valid law enforcement purposes only.

4. ALPR data may be released to other authorized and verified law enforcement officials and agencies for valid law enforcement purposes with the approval of the ALPR administrator or designee, contingent on an appropriate MOU being entered between the agencies.

5. Every ALPR Detection Browsing Inquiry must be documented by both the associated law enforcement agency case number, or incident number, and a reason for the inquiry.

6. The APLR Administrator or their designee will ensure that information entered into any custom hot list is removed from the system at the conclusion of the investigation, or whenever evidence suggests that it is no longer relevant to the investigation.

7. The Department shall post 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 within the ALPR data retention period; and

    f. Number of searches within the ALPR data retention period.

H. SECURITY OF INFORMATION

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

1. The ALPR Administrator will maintain usernames and passwords to access ALPR information. Usernames and passwords are not transferable, shall not be shared by ALPR Operators, and must be kept confidential. Access is limited to law enforcement personnel in good standing.

2. Unless preserved as part of an investigation, ALPR data shall purge no later than 30 days after the data was captured.

3. ALPR Operators will not download ALPR data unless such data is related to a valid law enforcement purpose. Any ALPR data that is obtained and used during an investigation shall be saved and uploaded to the associated report and stored in accordance with applicable evidentiary records law and policy.

4. ALPR Operators shall agree to comply with security controls implemented by the ALPR Administrator. At a minimum, such security controls shall include multi-factor authentication, encrypted communications, and other reasonable physical, technological, administrative, procedural, and personnel security measures to mitigate the risks of unauthorized access to the system.

I. RELEASING ALPR DATA

ALPR data may be shared only in the following circumstances:

1. With other law enforcement for a valid law enforcement purpose contingent on an appropriate MOU being entered between the agencies. The requesting agency must provide a written request for the ALPR data that includes:

   a. The name of the agency requesting the data;

   b. The name of the person requesting the data;

   c. The intended purpose of obtaining the data

2. The request is reviewed by the ALPR Administrator or the authorized designee and approved before the request is fulfilled. The approved request is retained on file.

3. With a prosecutorial agency such as the Rhode Island Office of Attorney General, United States Attorney's Office for the District of Rhode Island or a solicitor prosecuting a criminal matter on behalf of a municipality.

4. With a defendant or their counsel for purposes of complying with discovery or a court order in a criminal proceeding.

5. Pursuant to a court order or a court-issued subpoena in any criminal or civil proceeding.

6. With an ALPR vendor for maintenance or quality assurance purposes.

7. To alert the public to an emergency situation, a missing or endangered person, a person associated with human trafficking, or a person with an outstanding judicial warrant.

J. COMMUNICATIONS RESPONSIBILTIES

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.

K. 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.

3. Patrol officers are prohibited from independently conducting searches within the ALPR System. If a patrol officer requires an ALPR search, the officer shall provide the appropriate report number and the justification for the search to their immediate supervisor. The supervisor may conduct the search, provided the request is consistent with Department policy and applicable legal requirements.

L. 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 valid law enforcement purposes.

    a. Searches conducted within the ALPR system shall be documented in the associated call record and/or incident report.

3. Criminal Investigative Personnel and Supervisors shall have access to add, edit, and/or update custom Hotlists.

M. ALPR DATA DETECTION BROWSING AUDITS

1. The Office of Professional Standards (OPS) shall conduct an audit of the ALPR system at least once each quarter. Each audit shall include a random sampling of ten (10) ALPR browsing inquiries to determine compliance with this policy. The audit shall include, but not be limited to, compliance with the following:

    a. Information security and privacy laws;

    b. Queries are conducted consistent with this policy's Authorized Uses

    c. Queries contain an associated reason and report number;

    d. Only trained, authorized users are conducting searches;

    e. Outdated information is cleared from the system.

2. The audit shall be documented in the form of an internal department memorandum to the Chief of Police. After review by the Chief of Police or their designee, the memorandum and any associated documentation shall be filed and retained by the OPS.

N. TRAINING

1. The designated ALPR Administrator(s) shall ensure that prior to being authorized to use or access the ALPR system, members receive Department-approved training consistent with the manufacturer's recommendations that will include, at a minimum, training on the usage of the ALPR system, data sources, legal responsibilities and ramifications; as well as training on this policy.

2. Training shall be updated as technological, legal, and other changes that affect the ALPR Policy occur and will be provided to personnel.

O. VIOLATIONS

1. 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 in addition to access and/or use of the ALPR system be temporarily or permanently suspended.

2. Intentional violations may warrant discipline up to termination.

3. Any officer that observes a violation of this Policy is required to report the violation in writing to their immediate supervisor in the officer's chain of command.

4. Supervisors who observe or become aware of a violation of this Policy shall ensure appropriate remedial action or referral for disciplinary action, consistent with the Department's policies with respect to internal investigations.