Smithfield Police Department

GENERAL ORDER 380.30

SECTION	EFFECTIVE DATE	PAGES
300 – Law Enforcement and Operations	July 20, 2023	5
SUBSECTION	**SPECIAL INSTRUCTIONS**	
80 - Equipment	Rescinds 8/15/22 Version	
TITLE	**BY ORDER OF**	
AUTOMATED LICENSE PLATE READER (ALPR)		

I. PURPOSE

To establish guidelines for authorized Department members, regarding the use of Automated License Plate Reader (ALPR) technology.

II. POLICY

ALPR technology allows for the automated detection of license plates, along with vehicle make, model, color, and unique identifiers, that may assist authorized Department members in the identification of or gathering of information related, but not limited to, stolen or wanted vehicles, missing persons, homeland security threats, criminal suspect interdiction, and active criminal investigations.

It is the policy of the Smithfield Police Department to utilize ALPR technology to capture and store digital license plate data/images, while also recognizing the privacy rights of the general public. As such, the data/images obtained through ALPR technology are for official, law enforcement business and shall only be used consistent with the principles and protocols established in this policy.

III. DEFINITIONS

A. **AUTOMATED LICENSE PLATE READER (ALPR) -** A device that uses cameras and computer technology to compare digital images to lists of known information of interest (also known as License Plate Recognition or LPR).

B. **ALPR OPERATOR** – Authorized Department members (users) who may utilize the ALPR system/equipment. ALPR Operators may consist of sworn and non-sworn personnel.

C. **ALPR ADMINISTRATORS** - The Police Chief shall designate sworn personnel to serve as the Department's ALPR Administrators. The ALPR Administrators serve as the Officers-In-Charge of the ALPR system/equipment, and are responsible for system training, deployments, audits, etc.

D. **HOT LIST**- A list of license plates associated with vehicles of interest compiled from one or more data bases including, but not limited to, NCIC, RIDMV, Local BOLO's, etc. Vehicles of interest may include, but are not limited to, vehicles reported stolen, displaying stolen license plates, linked to missing and/or wanted persons, or otherwise flagged by law enforcement agencies.

E. **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.

F. **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 violence protective order violation, or terrorist-related activity.

IV. ALPR ADMINISTRATORS

A. The ALPR Administrators shall be properly trained and well versed in ALPR technology in order to serve in this capacity, and shall ensure that:

1. Authorized Department members complete all training requirements;

2. Authorized Department members are utilizing the system/equipment consistent with policy; and

3. The ALPR system/equipment is appropriately monitored, and that the security of the data and information is maintained in compliance with applicable privacy laws.

V. PROCEDURES

A. The ALPR system/equipment shall only be used for official, law enforcement business.

B. Department members shall not use or allow others to use the ALPR system/equipment or database records for unauthorized purposes.

C. No Department member shall operate the ALPR system/equipment or access ALPR data without first completing Department-approved training.

D. Unless exigent circumstances exist, ALPR Hits (Alerts) "alone" shall not be a basis for taking police action. ALPR Hits (Alerts) shall be responded to in the following manner:

1. ALPR Operators shall make every reasonable effort to verify ALPR Hits through the Rhode Island Law Enforcement Telecommunications System (RILETS) before taking enforcement action that is based solely on an ALPR Hit;

2. Once an ALPR Hit is received, ALPR Operators shall confirm that the license plate (and its state of issue, alphanumeric characters, & type) from the ALPR Hit matches the license plate of the observed vehicle before any law enforcement action is taken; and

3. Because an ALPR Hit may relate to a vehicle and may not relate to the person operating that vehicle, ALPR Operators are reminded that they need to have reasonable suspicion or probable cause to make an enforcement stop of any vehicle. [For example, if a vehicle is entered into the ALPR system because of its association with a wanted individual, officers must reasonably match the observed driver/occupants to the description of the wanted individual prior to making the stop or have another legal basis for making the stop.]

E. The ALPR Administrators may permit ALPR Operators to create Custom Hot Lists, as needed, and restrict the sharing of such lists based on Department needs.

1. The ALPR Administrators shall provide ALPR Operators with specific training in the available features and protocols, (i.e.: information updates, information removal, list expirations, etc.) relative to Custom Hot Lists, before authorizing ALPR Operators to maintain Custom Hot Lists.

2. The ALPR Administrators shall routinely conduct audits of Customized Hot Lists that have been shared with other ALPR Operators to ensure that expired, stale, or otherwise unnecessary information has been removed from the ALPR system by its creator.

VI. AUTHORIZED/UNAUTHORIZED USES

A. The ALPR system/equipment, and all data collected, is the responsibility of the Smithfield Police Department. Authorized users may only access and use the ALPR system/equipment for official, law enforcement business. The following uses of the ALPR system/equipment are specifically *prohibited*:

1. Use of the ALPR system/equipment to record license plates that are **not** exposed to public view, except when done pursuant to a court order/search warrant. Examples of license plates that *are* exposed to public view include:

a. License plates on vehicles traveling on a public roadway;

b. License plates on vehicles that are on private property, but visible from a public roadway; or

c. License plates on vehicles traveling in a public parking area or business establishment to which the public has access.

2. Use of the ALPR system/equipment to harass or intimidate any individual or group;

3. Use of the ALPR system/equipment to target or focus on individuals or groups solely because of their race, gender, religion, political affiliation, nationality, ethnicity, sexual orientation, disability, or any other classification protected by law; and

4. Use of the ALPR system/equipment for any personal purpose.

VII. DATA STORAGE AND RETENTION

A. The ALPR vendor (Flock Safety) stores data (data hosting) and ensures proper maintenance and security of data stored in their data towers. The vendor purges this data after thirty (30) days of storage. However, this shall not preclude the Smithfield Police Department from maintaining any relevant vehicle data obtained from the system on its server or on portable media.

B. ALPR data gathered, stored, or retained by the Smithfield Police Department shall not be sold, accessed, or used for any purpose other than official, law enforcement business.

C. The ALPR Administrators shall ensure that systems and processes are in place for the proper collection, storage, and retention of ALPR data.

D. The ALPR Administrators shall ensure that all ALPR data is purged from the server or portable media when it is no longer required as evidence in a criminal or civil action, or subject to discovery requests or lawful requests to produce records.

VIII. DATA SECURITY AND ACCESS

A. All data shall be closely protected by both procedural and technological means. The Smithfield Police Department shall 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. Authorized ALPR Operators are permitted to access ALPR data for official, law enforcement business only.

4. ALPR data may be released to law enforcement personnel from outside agencies, provided such data is needed for official, law enforcement business.

5. Every ALPR Detection Browsing Inquiry shall include an associated case number, incident number or call number.

IX. TRAINING

A. The ALPR Administrators shall ensure that all ALPR Operators receive initial, Department-approved training, as well as any updated training deemed appropriate by the ALPR Administrators.

X. ALPR SYSTEM AUDITS

A. The ALPR Administrators shall conduct routine, undocumented audits of ALPR Detection Browsing Inquiries conducted by ALPR Operators to ensure compliance with this policy.

B. The ALPR Administrators shall conduct semi-annual, *documented* audits of ALPR Detection Browsing Inquiries conducted by ALPR Operators to ensure compliance with this policy. Semi-annual audits shall consist of at least ten (10) inquiries.

_____

_____