GENERAL ORDER

SUBJECT: AUTOMATED LICENSE PLATE READER

NUMBER: 3-64

EFFECTIVE DATE: 07/01/25

APPROVED:

CHIEF OF POLICE

AMENDS/ SUPERSEDES: 10/25/24

POLICY:

This policy establishes guidance concerning the installation, operation, maintenance and security of Automated License Plate Readers (ALPR) in support of the Staunton Police Department's mission, goals and objectives.

PURPOSE:

The Staunton Police Department ALPR system provides information for use by Department personnel to assist in the detection and apprehension of certain vehicles traveling through the City of Staunton. The ALPR system can also be utilized to assist in the development of information that could identify suspects who have committed crimes within the City of Staunton, and to help locate missing or endangered persons.

PROCEDURES:

This policy establishes procedures for the lawful and proper use of ALPR technology. It provides the best use of this technology, while protecting the rights of residents and motorists traveling on public roadways in the City of Staunton.

1. General:

The ALPR Program will be managed by the LES Division Commander, in coordination with the Technology Operations Unit, to ensure that the equipment is being effectively utilized and maintained. Locations of fixed ALPR cameras will be determined based upon points of ingress and egress into and out of the City, natural choke points where vehicle traffic must pass, and locations based on criminal activity or ongoing investigations.

2. Operations- Fixed ALPR:

a. Fixed ALPR cameras will monitor traffic within their field of view throughout the City of Staunton, 24 hours a day.

b. The system will passively monitor traffic and retain license plate and related data for a period of 21 days, in accordance with VA Code § 2.2-5517. Information of investigative value entered into the ALPR system from NCIC or a "custom hotlist" will produce alerts for investigative purposes.

c. The LES Division Commander or his designee will serve as the administrator of the Department's ALPR system. He will manage all data entered into the ALPR database and facilitate user profiles.

d. User profiles will be provided to all sworn personnel. Sworn personnel can select the types and method of alert notification (text message, email, or both.) The database automatically updates every 24 hours. The National Center for Missing and Exploited Children (NCMEC) Amber Alert is required to be activated for all personnel and will be evaluated by the on duty supervisor to determine appropriate response.

e. Field users who receive notifications must verify subject/vehicle identification and confirm the NCIC status before taking action. Personnel responding to ALPR alerts in the field will notify the on-duty supervisor, and dispatch, who will record the event as a self-initiated activity for CAD record purposes.

f. Field users may search the ALPR database pursuant to criminal investigative needs (i.e. identification of suspect vehicle.)

1. Hotlist data may contain:

i. Information of investigative interest such as specific license plate information

ii. AMBER/SILVER Alerts

iii. Information relating to Missing/Endangered Individuals or Runaways

iv. Information related to a person associated with human trafficking

g. All personnel will receive training prior to being given access to the ALPR system. Training may be instructor-led, online through the PowerDMS portal, or a combination of both.

h. Retained ALPR data may be accessed by an officer/investigator for criminal justice purposes only. Officers shall not download data unless it meets the permissable criteria in section F.

i. System data will be purged automatically after 21 days by the vendor.

j. Access to the LPR system is controlled by multifactor authentication on all departmental computers, including mobile data terminals. Individual username and passwords are required to login to the program.

3. Operations- Mobile ALPR

a. The Staunton Police Department is a participating agency in the Virginia State Police (VSP) ALPR Program. Access to and use of the VSP ALPR program data is governed by a Memorandum of Understanding between the Staunton Police Department and VSP.

b. The LES Division Captain will designate a Point of Contact for the program, who will be responsible for managing sworn employee accounts and ensuring training is completed prior to using the system. Training shall include but not be limited to the use of and dissemination of information obtained from the VSP ALPR program.

c. VSP ALPR data is considered Criminal Justice Information, and access to such data shall specifically pertain to active investigations and intelligence gathering related to criminal activity. ALPR data may only be downloaded when it specifically

pertains to active investigations and intelligence gathering related to criminal activity. Additionally, the ALPR data may only be shared when the request specifically pertains to active investigations and intelligence gathering related to criminal activity. All users must comply with NCIC/VCIN rules and regulations. Violations may result in disciplinary action and/or criminal prosecution.

d. Users will log in to the program at the beginning of their shift, at which time a new hotlist will automatically download to the unit. The hotlist is updated every four hours, but will only update on the MDT if the user logs out and back in.

e. A supervisor must be notified of any alerts/hits from the system. In the event of verified hits on an unoccupied vehicle, officers will maintain visual observation while supervisory contact is initiated to determine if immediate recovery action will be taken or whether surveillance will be continued.

f. Mobile ALPR cameras are hard mounted to the patrol vehicle. Because of this, no vehicle equipped with an ALPR camera system should be taken through a friction type car wash. Instead, officers operating a vehicle with this equipment should only utilize a touchless car wash.

4. Administration

a. The Department’s ALPR system database and related information are to be used for official law enforcement/criminal justice purposes only. Personnel shall only access the database for investigative purposes and treat all data as confidential. The utilization of the ALPR system for any other reason will require the approval of the Chief of Police.

b. SPD personnel will not enter any license plates into the Staunton Police custom hotlist unless the vehicle is currently wanted/suspected in criminal activity. All custom hotlist vehicles shall include a case number, CAD event number, or other identifier relating to an ongoing investigation, and the reason for the vehicle being added into the system. All custom hotlist entries shall have an expiration date. If an apprehension occurs through the use of Flock, investigators will utilize the Flock Apprehension tool to properly track the outcomes of officer interactions. This includes the documentation of the following data:

1. Race, ethnicity, age, gender of the person stopped

2. Whether the person stopped spoke English

3. The reason for the stop

4. Whether a notification from an ALPR system was received for the motor vehicle prior to the stop, and if so, the specific reason for the notification

5. The location of the stop

6. Whether a warning, written citation or summons was issued, or whether any person was arrested

7. If a warning, written citation or summons was issued, or an arrest was made, the warning provided, violation charged, or crime charged

8. Whether the vehicle or any person was searched

9. Whether the officer used physical force against any person

10. Whether any person used physical force against any officers

c. ALPR capture data will not remain on Staunton Police servers after 21 days unless it is of evidentiary value. ALPR data needed to be held for evidentiary value will be uploaded to evidence.com and categorized per the current retention policy. System data may be stored until the investigation concludes without any criminal charges, or until the final disposition of any criminal or civil matter related to the data, including any direct appeals, in accordance with applicable record retention laws.

d.When personnel become aware of invalid data being contained within the state NCIC database, SPD personnel shall notify the contributing agency and document who was notified by name and title in the CAD incident notes.

e. The Staunton Police Department may enter into data-sharing agreements with other law enforcement agencies or non-law enforcement agencies who collect ALPR data only under the authority of the Chief of Police (or his designee). In response to a court order or Freedom of Information Act request, only that information stored on Staunton Police Department servers would be authorized for release.

f. Any ALPR related data stored on Staunton Police Department servers or any contracted vendor’s servers will remain property of

the Staunton Police Department and will not be shared or released without the approval of the Chief of Police.

5. Privately Owned/Funded ALPR Systems

a. The Staunton Police Department recognizes that residents may want to purchase privately owned ALPR systems and link them to the Staunton Police network of systems. All private systems linked to the Staunton Police system must be approved by the Chief of Police. All data received by the Staunton Police Department shall become Staunton Police Department data and subject to all provisions of this policy. The Staunton Police Department must be provided search capabilities to any linked ALPR system. The Staunton Police will not be responsible for any costs associated with a privately funded ALPR system.

b. Privately owned ALPR systems must meet City of Staunton ordinances and regulatory standards.

c. The Staunton Police will not actively monitor any privately owned ALPR or video system.

6. System Audits

a. On a monthly basis, the Commander, LES Division, or his designee will conduct an internal audit of the ALPR system. On an annual basis, prior to April 1, the Department shall report to the Department of State Police, on its use of the system during the preceeding year, which shall include the following data:

1. Total number of cameras owned or leased by the Department at the concludion of the calendar year, whether fixed or mobile

2. A list of all state and federal databases with which the system data was compared, unless the existence of any such database itself is not public

3. The total number of times the system was queried, including the specific purposes of the queries,and the offense types for any criminal investigation

4. The race, ethnicity, age, and gender of any individual identified as a suspect and charged with a criminal offense as a result of a query of the system as part of a criminal investigation

5. The number of motor vehicles stopped based on notifications from the system, including the specific reasons for the notifications

6. The race, ethnicity, age, and gender of the driver of any motor vehicle stopped based on a notification from the system

7. Whether the agency allows any other law enforcement agencies to access its system data, and of so, which other agencies have been granted such access

8. The number of identified instances of unauthroized use of or access to the system, including the nature and circumstances of such instances, and

9. The number of subpoena duces tecum, search warrants, and any other requests received from a third party for system data or audit trail data, including the identity of the entity that requested the issuance of such subpoena duces tecum, executed search warrant, or requested such data, and whether any data was provided to such entity, unless disclosure of such subpoena duces tecum, search warrant, or request is otherwise prohibited by law

b. Audit trail data shall be purged after two years from the date of its capture.

c. System data and audit trail data shall not be subject to disclosure under the Virginia Freedom of Information Act.

d. System data and audit trail data are prohibited from being sold pursuant to VA Code § 2.2-5517.

e. This policy and the annual audit report will be posted on the Flock Transparency Portal.