CHARLOTTESVILLE POLICE DEPARTMENT

Type of Directive: General Order	Policy#: **427**
Chapter 4: Patrol Operations	Effective Date: **08/27/2024**
Subject: **AUTOMATED LICENSE PLATE READERS (ALPR'S)**	
■ New Directive ☐ Replaces: ☐ Revises:	Reviewed: **08/27/2024**
By authority of the Chief of Police: Colonel Michael Kochis	

427.1 PURPOSE AND SCOPE

The purpose of this policy is to provide sworn members of the Charlottesville Police Department with guidance for the capture, storage and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology.

427.2 POLICY

It is the policy of the Charlottesville Police Department to utilize ALPR technology to capture and store digital license plate data and images only for legitimate law enforcement purposes while ensuring that the privacy, civil rights, and civil liberties of individuals are not violated.

This policy applies to ALPR information collected or received, accessed, used, disseminated, retained, and purged by Charlottesville Police Department. It is not intended to apply, nor does it apply, to any other types of information accessed, retained, or used by the Department.

All data and images gathered by the ALPRs are for the official use of the Charlottesville Police Department. Because such data may contain private and/or confidential information, it is not open to public review unless required by law.

427.3 DEFINITIONS

Definitions related to this policy include:

Alert - aka "Hit" - a positive indication, by visual and/or audible signal, of a potential match between data on the "hot list" and a license plate scanned by the ALPR system. A alert/hit is not conclusive evidence that a plate, vehicle, or occupants therein are wanted, and additional investigation is always required when an alert/hit is indicated.

ALPR Coordinator – The designated Supervisor responsible for the oversight and administration of the Departments ALPR program.

ALPR Data - Data captured by the ALPR cameras of an image (such as a license plate and description of vehicle on which it was 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.

Automated License Plate Reader (ALPR) - A device that uses cameras and computer technology to compare digital images to database lists of known information of interest.

Hot List - Lists created from databases generated from NCIC/VCIN that include, but are not limited to, license plate numbers of stolen vehicles and license plates, wanted persons, AMBER alerts, SILVER alerts, NCMEC missing persons, and terrorist watch list alerts with a license plate associated with the record.

Read - Digital images of license plates and vehicles and associated metadata (e.g., date, time, and geographic coordinates associated with the vehicle image capture) that are captured by the ALPR system.

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 law enforcement agencies.

427.4 GENERAL

a. Information gathered or collected, and records retained by the Departments ALPR Program or system will not be accessed or used for any purpose other than legitimate law enforcement or public safety purposes.

b. The Departments ALPR Program or system will only be accessible by law enforcement agencies within the Commonwealth of Virginia.

c. The Department and other law enforcement agencies authorized to collect ALPR information must use the least intrusive collection and investigative techniques possible while still obtaining the necessary ALPR data.

d. The Department protects all ALPR information as personally identifiable information (PII) because ALPR information may be combined with other information to specify a unique individual (i.e., the identity of an individual could be directly or indirectly inferred by using information that is linked or linkable to that individual).

e. All deployments of the ALPR system are for official use only (FOUO). All information captured, stored, generated, or otherwise produced by an ALPR system is the property of the Charlottesville Police Department regardless of where the information is housed or stored.

f. Any data extracted from the ALPR server to be retained as evidence shall be thoroughly documented in an appropriate report (i.e., Flock Evidence Extraction Report) within the Department's records management system (RMS).

[VLEPSC – OPR.03.03(a)(c)] [CALEA – 41.3.9(a)]

427.5 PROCEDURES

427.5.1 MANAGEMENT AND ADMINISTRATION

a. The Criminal Investigations Division is responsible for the management and administration of the Department's ALPR program.

b. The Criminal Investigations Division Commander will designate an ALPR Coordinator who will be directly responsible for the oversight and administration of the Department's ALPR program.

c. Operators encountering problems with ALPR equipment or programs are responsible for notifying the ALPR Coordinator via email.

427.5.2 ALPR COORDINATOR

a. The ALPR Coordinator, or their authorized designee, will administer the day-to-day operation of the Department's ALPR equipment and its associated data and ensure that the Department's policies and procedures related to the devices conform to current laws, regulations, and best practices. The ALPR Coordinator will also have the following additional duties and responsibilities:

1. Liaising with and being the Department's primary point-of-contact with the ALPR provider.

2. Establishing protocols for access, collection, storage, and retention of ALPR data and associated ALPR media files.

3. Establishing protocols to ensure the security and integrity of data captured, stored, and/or retained by the ALPR system.

4. Identifying locations across the city for the placement of ALPR cameras so as to ensure that their deployment does not disproportionately target any group or segment of our community.

5. Coordinating the proper and efficient installation, maintenance, and deployment of the Department's ALPRs.

6. Ensuring that stored ALPR information is automatically purged from the ALPR database within established timeframes, unless determined to be of evidentiary value.

7. Acting as the authorizing official for individual access to and data retention of the ALPR information.

8. In collaboration with the Training Coordinator, ensuring that all members with authorized access to ALPR information receive the appropriate initial and any required refresher/recurrent training.

9. Updating authorized users of any technological, legal, or other changes that affect the use of ALPR system.

10. Ensuring that inspections and maintenance of the Department's ALPRs are completed

to ensure their continued operational readiness.

11. Ensuring that any of the Department's ALPRs or its associated equipment that is damaged or not functioning properly is taken out of service, and promptly repaired and/or replaced.

427.5.3 GUIDELINES FOR USE OF THE ALPR SYSTEM

a. An ALPR alert, including an alert sent by the ECC, does not create reasonable suspicion to justify a traffic stop or the detention of an individual. The officer must develop independent reasonable suspicion for the stop.

b. Before initiating any enforcement action, the officer shall:

   1. Make a visual confirmation that the license plate actually matches the information captured by the ALPR and reported in the corresponding alert.

   2. Confirm the license plate information with the National Crime Information Center (NCIC) and the Virginia Criminal Information Network (VCIN).

   3. Ensure the hit conforms to the parameters set forth in this directive.

c. Officers conducting a traffic stop based on a confirmed ALPR alert shall consider the level of risk associated with the nature of the offense and ensure that their response complies with all applicable laws and Department policies/procedures.

427.5.4 PROHIBITED USES

a. When using the ALPR system, officers shall not target any person based on their actual or perceived race, color, religion, creed, sex, gender, gender identity, sexual orientation, age, national origin, ethnicity, disability, veteran status, marital status, partnership status, pregnancy status, political affiliation or beliefs, and, to the extent permitted by law, alienage or citizenship status.

b. Users shall not employ the ALPR system to intimidate or harass any individual or group.

c. Members shall not obtain, attempt to obtain, or convert any data obtained with ALPR for their personal use or the unauthorized use of another person. Department personnel shall only access and use the ALPR system for official and legitimate law enforcement purposes consistent with this directive. Members found in violation of the aforementioned shall be subject to internal discipline and may also be subject to criminal prosecution, for a violation of Va Code § 18.2-152.4 (Criminal Trespass).

d. Unless there is a criminal nexus, officers shall not use the ALPR system or use, retain, or transmit license plate reader data to investigate persons who are, or were, exercising their First Amendment rights, including freedom of speech, assembly, association, and exercise of religion, such as attending political rallies, organizational meetings, public demonstrations, and religious gatherings.

e. The Department shall not use or operate the ALPR system or its data for operations

focused on collecting past due traffic fines, or any other similar purpose of generating revenue or collecting money owed by the public.

f. The Department shall not use the ALPR system or its data to conduct criminal investigations on a person's immigration status.

g. Any alleged misuse or inappropriate application of ALPR operations, information, data, or software by a member will be thoroughly investigated in accordance with applicable laws and Department policy. Allegations that are substantiated shall result in disciplinary action and may also result in criminal prosecution.

[VLEPSC – OPR.03.03(a)(c)] [CALEA – 41.3.9(a)]

427.5.5 SECURITY AND ACCOUNTABILITY SAFEGUARDS

a. All ALPR data will be closely safeguarded and protected by both procedural and technological means against network intrusions. The Charlottesville Police Department will observe the following security and accountability safeguards regarding access to and use of stored data:

    1. All ALPR data downloaded to the mobile workstation and in storage shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date, and time.

    2. Each authorized User will have a unique log-in identification and password to access the ALPR database and its associated data. Usernames and passwords to ALPR information are not transferrable, must not be shared, and must be kept confidential**.**

    3. Members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relates to a specific criminal investigation or department-related civil or administrative action. All user access and queries are subject to review and audit.

    4. ALPR data may only be released to other authorized and verified law enforcement officials and agencies <u>within</u> the Commonwealth of Virginia for legitimate law enforcement purposes.

    5. Access to ALPR information will be granted only to members whose positions and job duties require such access and who have successfully completed the required training.

    6. ALPR system audits shall be conducted on a monthly basis.

b. If any member reasonably believes that another law enforcement agency has used or is using the Departments ALPR systems or data in a manner that violates Section #427.5.4 (Prohibited Uses) of this policy, the member shall promptly report that information to the ALPR Coordinator, or Internal Affairs, who shall then investigate the allegation and determine if sharing ALPR data with the outside agency will continue.

c. When an officer takes any action due to an ALPR alert/hit, but it is later discovered that they acted on the wrong vehicle due to an error in data entry, fictitious or swapped license plates, or a misinterpretation of the license plate, the officer shall email the incident details

to their Supervisor and the ALPR Coordinator before the end of their shift. The ALPR Coordinator shall include this data and the circumstances surrounding it in the next monthly audit.

[VLEPSC ADM.25.03(b)(c), OPR.02.04(d)] [CALEA – 41.3.9(b)]

427.5.6 AUDITS

a. The Professional Standards Division Commander, or their authorized designee, is responsible for conducting audits of the Department's ALPR system. The results of such audits will be presented to the Chief of Police, or their authorized designee, which may be public information as allowed by law.

b. The Professional Standards Division Commander, or their authorized designee, shall perform a monthly random audit of the system to ensure compliance with policies and procedures. This audit shall include, but is not limited to:

1. The number of license plates scanned;

2. The number of license plate alerts/hits;

3. The names of the lists against which captured plate data were checked, and the number of confirmed matches and the number of matches that, upon further investigation, did not correlate to an alert;

4. The number of matches that resulted in the arrest, prosecution, or the location of a missing or endangered person;

5. The number of preservation requests received, broken down by the number of requests by a governmental entity versus by a defendant;

6. The number of data sharing requests received, granted, and denied broken down by agency and offense;

7. The number of data sharing requests resulting in arrest, prosecution, or the location of a missing or endangered person;

8. The number of manually-entered license plate numbers broken down by reason justifying the entry and the number of confirmed matches and the number of matches that, upon further investigation, did not correlate to an alert;

9. Any changes in Department policy that affect privacy concerns;

10. Data gathered and the circumstances surrounding incidents during a detention that did not result in an investigation (See Section #427.5.5(c);

11. Information regarding the race and gender of the driver of any vehicle detained as a result of ALPR action;

12. Information regarding the race and gender of the reported victim of the crime as a result of ALPR action; and

13. Information regarding the offense under investigation as a result of ALPR action.

c. As both a mechanism for accountability and as a means of promoting transparency and instilling public trust and confidence in the Departments ALPR program, the Executive Director of the Police Civilian Oversight Board (PCOB) for the City of Charlottesville will have unfettered access to and is authorized to perform audits of the ALPR system.

427.5.7 ALPR INFORMATION RETENTION AND PURGING

a. All ALPR information contained within the Department's ALPR system will be stored for a period not to exceed 7-days. After the 7-day time period, the information will be automatically purged (i.e., permanently removed from the system). This retention policy, however, applies only to the ALPR information contained in the Department's ALPR system itself. Once an ALPR record is downloaded by Department personnel and incorporated into a criminal intelligence record or investigative case file, the ALPR information is then considered intelligence or investigative information and the laws, regulations, and policies applicable to that type of information or intelligence govern its use.

[VLEPSC ADM.25.11] [CALEA – 41.3.9(d)]

427.5.8 RELEASING ALPR DATA

a. ALPR data may only be shared with other in-state law enforcement or prosecutorial agencies for official law enforcement purposes.

b. ALPR data shall not be distributed, sold, or transferred to any non-law enforcement or non-prosecutorial entities, unless otherwise required by law.

c. Requests for external dissemination of information to law enforcement/prosecutorial agencies outside of the Commonwealth of Virginia shall be made to the Chief of Police, or their authorized designee. The determination to disseminate the requested information shall be based upon the validity of the request (which must be supported by a specific law enforcement need) and in strict accordance with Department policy. All other requests for ALPR information, shall be routed to the Professional Standards Division for processing and compliance with the Virginia Freedom of Information Act (VFOIA).

[VLEPSC ADM.25.03(d)]

427.5.9 MAINTENANCE AND REPAIR

a. All ALPR equipment, software, and components will be properly maintained in accordance with the manufacturer's recommendations and/or any published industry standards.

b. Any ALPR equipment needing maintenance, repair, or that is damaged shall be immediately reported to a Supervisor. The Supervisor is responsible for notifying the ALPR Coordinator so that the appropriate repair or replacement can be completed.

427.5.10 TRAINING

a. Any personnel utilizing the ALPR system shall complete annual training on the policies and restrictions regarding ALPR use, data handling, and processing requests for ALPR data. Among other topics, this training shall cover:

    1. The appropriate use and collection of ALPR data and emphasize the requirement to document the reason for the inquiry;

    2. The specific content included under Section #427.5.5 (Security and Accountability Safeguards) of this policy;

    3. Examples of negative consequences resulting from misuse; and

    4. A clear explanation and warning indicating that the person currently operating the vehicle may not be the individual associated with the Hot List alert, despite the license plate's inclusion in the list.

b. Department members shall only access, use, view, or otherwise participate in the ALPR program when the member completes this annual training. Members who have previously completed the training but fail to timely complete subsequent annual training shall have their access to ALPR systems revoked until they complete the required training.

[VLEPSC – TRN.02.03(a), TRN.04.01(d)] [CALEA – 41.3.9(c)]