ASHEVILLE POLICE DEPARTMENT POLICY MANUAL

Chapter: 5 - Law Enforcement Operations
Original Issue: 3/1/2024
Policy: 505 - Automated License Plate Recognition
Last Revision: N/A
Previously: N/A

CONTENTS

INTRODUCTION
POLICY STATEMENT
DEFINITIONS
RULES AND PROCEDURES
505.1 SYSTEM USE [41.3.9 a]
505.2 HOT LISTS
505.3 DATA SECURITY AND ACCESS [41.3.9 b]
505.4 DATA STORAGE AND RETENTION [41.3.9 d]
505.5 ADMINISTRATIVE RESPONSIBILITIES

ASSOCIATED DIRECTIVES

Policy 206 - Technology Use & Security
Policy 1701 - Criminal Intelligence

INTRODUCTION

This policy establishes department guidelines for providing employees with an automated method of identifying license plates related to law enforcement purposes.

POLICY STATEMENT

It is the policy of the Asheville Police Department (APD) to ensure that Automated License Plate Recognition systems are used by department members responsibly and professionally, following all applicable laws and directives.

DEFINITIONS

Automated License Plate Recognition (ALPR) System: a system that uses cameras and computer technology to compare digital images of license plates to lists of known plates of interest. ALPR may be deployed in different configurations, including fixed and mobile.

Hot List: license plates associated with vehicles of interest from an associated database, including, but not limited to, NCIC, DMV, and local BOLOs (be on the lookout).

Hit: notification that data matched to a plate previously registered on a hotlist of vehicle plates related to stolen vehicles, wanted vehicles, or other factors supporting the investigation or which has been manually registered by a coworker for further investigation.

RULES AND PROCEDURES

505.1 SYSTEM USE [41.3.9 a]

A. Automated license plate recognition-equipped vehicles and associated databases will be used for legitimate law enforcement purposes following state and federal law.

B. **ALPR systems are an investigative tool only. All users must verify "hits" before taking enforcement action to ensure the information is not expired or outdated.**

C. Department employees are prohibited from using or authorizing the use of ALPR equipment or database records for non-law enforcement purposes.

D. Unless there is a criminal nexus, ALPR operators will attempt to avoid public gatherings such as political rallies, public demonstrations, and religious gatherings; if the sole purpose is to obtain plain read intelligence, see Policy 1701 - Criminal Intelligence. This does not preclude members from responding to a call for service where there may be incidental plate reads or from searching for stolen vehicles and vehicles of interest in these areas.

E. Only authorized personnel trained in using ALPR are to operate the system. [41.3.9 c]

F. Employees who become aware of damage or malfunctions related to an ALPR system must immediately report it to their immediate supervisor and the Law Enforcement Technology Unit.

G. All successful uses of the ALPR system will be documented and forwarded to the Data Accountability Supervisor for review.

505.2 HOT LISTS

A. To use the most up-to-date information, the hot list will be acquired, developed, and/or compiled at least every 24 hours in the following manner.

1. Available NCIC extract downloads will occur every six (6) hours, and hot list data will be transferred to the ALPR server.

2. Officers and users of the ALPR system may only have the Data Accountability Supervisor enter additional vehicles of interest into the hot list for official and legitimate law enforcement purposes.

3. User entries should be entered to expire within ninety (90) days or less.

4. Other local hot lists may be developed for manual entry.

B. Information will be submitted to the ALPR system for inclusion on the hot list in the following ways:

1. NCIC records, including stolen vehicle files, stolen plates, stolen Canadian plates, wanted persons, missing or endangered persons, and nationwide domestic violence protection orders.

2. Official BOLOs or alerts or official law enforcement bulletins; vehicles associated with crime incidents; suicidal, homicidal, missing or wanted persons; AMBER alerts; stolen vehicles; or vehicles of interest.

3. Departmental watch lists may be developed for local warrants associated with a vehicle.

C. The Data Accountability Supervisor may approve additional potential sources of vehicles of interest as they become available.

505.3 DATA SECURITY AND ACCESS [41.3.9 b]

A. Department employees are responsible for the security of ALPR data. Employees will only access, use, release, or disseminate hot list and scan file data for official and legitimate law enforcement purposes.

B. As with other law enforcement databases, the department will ensure that the storage, use, and transmission of ALPR data is as secure as reasonably possible, see Policy 206 - Technology Use & Security.

C. Only designated department personnel will be able to query license plate recognition data, create reports, and use analytic tools.

D. Hot list and ALPR data are considered confidential information.

1. Security of the hotlist data is the responsibility of the officer using the ALPR or personnel accessing the data

2. Use of the ALPR database will be regulated by requiring employees to log into the system, which can record details of when and who accessed information within the database.

E. Officers may only access data stored in the ALPR database based upon a reasonable belief that the data may be related or valuable as part of a specific official action or investigation.

F. Incidental sharing of information from the department's computerized information systems or remote access by an outside law enforcement agency will conform to the requirements of this policy.

G. All requests for shared data access from other law enforcement agencies and invitations to access data from private ALPR systems will be forwarded to the Law Enforcement Technology Unit for approval.

H. ALPR data will only be shared with another law enforcement agency or prosecutor regarding an official criminal investigation upon a written request to the Law Enforcement Technology Unit, which may be made electronically.

I. The release of ALPR data is not required if the disclosure of requested ALPR data will compromise an ongoing investigation.

J. ALPR data is not a public record and will not be disclosed except as provided in N.C. Gen. Stat. § 20-183.32(e).

K. Officers requesting the retention or release of ALPR data maintained by another agency will obtain supervisor approval before making the request.

1. Officers requesting the data must submit a sworn written statement to the agency pursuant to N.C. Gen. Stat. § 20-183.32. A copy of the request will be retained in the case file.

2. Officers requesting the data will contact the outside agency to cancel any request once the information is no longer needed.

505.4 DATA STORAGE AND RETENTION [41.3.9 d]

A. ALPR data will be collected and securely retained in a cloud-based server. Only the Data Accountability Supervisor or Law Enforcement Technology Unit may download and distribute ALPR data.

B. ALPR data will be purged after ninety (90) days unless one of the following methods of preservation occurs:

1. A federal or state search warrant has been issued for the data, or

2. A preservation request is made under N.C. Gen. Stat. § 20-183.32(c). Upon the documented request from a coworker, the Data Accountability Supervisor will

take all necessary steps to preserve the requested captured plate data immediately. The documented request must specify in a written, sworn statement on the Automated License Plate Recognition Preservation Request Form (form ALPR-1) all of the following:

a. The location of the fixed camera or mobile device identification of the particular camera(s) for which captured plate data will be preserved and the particular license plate for which captured plate data will be preserved.

b. The date(s) and time frames for which captured plate data will be preserved.

c. Specific and articulable facts showing that there are reasonable grounds to believe that the captured plate data is relevant and material to an ongoing criminal or missing persons investigation or is needed to prove a violation of a motor carrier safety regulation.

d. The case and identity of the parties involved in that case.

C. Relevant ALPR data cannot be added to a case file unless the data is preserved by one of the methods outlined in N.C. Gen. Stat. § 20-183.32.

D. Data will be subject to the same logging, handling, and chain of custody requirements as other evidence.

505.5 ADMINISTRATIVE RESPONSIBILITIES

A. The Data Accountability Supervisor is responsible for:

1. Managing the utilization of the ALPR software from the end-user through reporting, storage, monitoring, and data sharing.

2. Administering and preserving ALPR data per N.C. Gen. Stat. § 20-183.32.

3. Review and assist with requests for ALPR use or data access.

4. Managing the gathering of hotlists.

B. The Law Enforcement Technology Unit is responsible for:

1. Overseeing the storage and management of ALPR data systems with the support of the vendor(s) and City of Asheville Information Technology Services (ITS), as necessary.

2. In partnership with the Recruitment & Career Development Section, provide appropriate, documented training for ALPR operators. [41.3.9 c]

3. Providing ongoing training on ALPR systems, as necessary.
4. Ensuring the program complies with record retention requirements.
5. Will be responsible for conducting, reviewing, and retaining audits of the ALPR system at least annually. Audits should consist of at least the following:
    a. Records of ALPR users, system usage, data files being deleted as scheduled, and ensuring that all users are appropriately trained.
    b. Audits will be forwarded to the Office of the Chief through the chain of command.

BY ORDER OF:

Michael Lamb
Chief of Police