Asheville Police Department Policy Manual

Chapter: 5 - Law Enforcement Operations
Original Issue: 3/1/2024
Policy: 505 - Automated License Plate Recognition
Last Revision: 10/1/2026
Previously: N/A

Contents

Introduction
Policy Statement
Definitions
Rules and Procedures
505.1 System Use
505.2 Hot Lists
505.3 Data Security and Access
505.4 Data Storage and Retention
505.5 Administrative Responsibilities

Associated Directives

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

Introduction

This policy establishes departmental guidelines for providing employees with an automated method to identify license plates for law enforcement purposes.

Policy Statement

It is the policy of the Asheville Police Department (APD) to ensure that department members use Automated License Plate Recognition systems responsibly and professionally, in accordance with 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 utilized only for legitimate law enforcement purposes, in accordance with state and federal laws.

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 All users must verify “hits” before taking enforcement action to ensure the information is not expired or outdated.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. Intelligence and information gathering, including by use of ALPRs, will be conducted in a manner that respects the constitutional rights of all individuals, groups, and organizations. Use of intelligence-gathering tools and technology in connection with protests or public demonstrations will be limited to that which is necessary to support law enforcement’s role in facilitating individuals' First Amendment right to express themselves while protecting participants and ensuring public safety.

E. Only authorized personnel trained to use ALPR are permitted 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 Technology Section.

G. All successful uses of the ALPR system will be documented and forwarded to the Intelligence Section Lieutenant for review.

H. Violations of this policy may result in disciplinary action and/or the revocation of access to ALPR systems.

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 as follows:

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 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 thirty (30) 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.

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 are as secure as reasonably possible; see Policy 206 - Technology Use and 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 in to the system, which will record when and by whom information was accessed.

E. Officers may access data stored in the ALPR database only upon a reasonable belief that the data may be related to or valuable in 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 Technology Manager for approval.

H. ALPR data will be shared with another law enforcement agency or prosecutor only for an official criminal investigation, and requested through the LPR system.

I. The release of ALPR data is not required if disclosing the requested data would 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 preserved for discovery purposes only.

B. ALPR data will be purged after twenty-one (21) 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 a coworker's documented request, the RTIC 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 A-71) 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 RTIC supervisor is responsible for:

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

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

3. Managing the gathering of hotlists.

B. The Technology Section is responsible for:

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

2. In partnership with the Organizational Support Division, 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. Maintaining calibration and maintenance schedules and records for the system on file.

C. The Intelligence Section lieutenant will ensure that an audit of the ALPR system use and effectiveness is conducted quarterly. Audits will be forwarded to the chief of police through the chain of command. Audits will consist of at least the following:

1. An organizational audit of records of ALPR users, system usage, and ensuring that all users are appropriately trained.
2. A network audit to ensure adherence to department policy and procedures.

By order of:



Jackie Stepp
Chief of Police