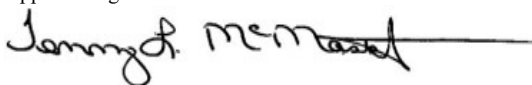


		UNC School of the Arts Police and Public Safety Department General Orders	
Title: Automated License Plate Recognition System (ALPR)		Number: WD2020-800-09	
Distribution: All Personnel		Pages: 6	
Rescinds New	Effective: 06/29/2026	Revised:	
Approved by: Tommy L. McMasters Jr., Assistant Vice Chancellor & Chief of Police		Approval Signature: 	

PURPOSE: The purpose of this directive is to establish guidelines for the use of Automated License Plate Readers (ALPRs) and their technology.

It is the policy of this department to develop and provide the most effective, efficient, and reliable technology for all members of the department. ALPRs are used by the UNCSA Police Department to convert data associated with vehicle license plates for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates, and missing persons. ALPRs may also be used for any other official law enforcement business, including but not limited to suspect identification in crimes under investigation, stolen property recovery, electronic surveillance, and criminal interdiction. It is the intent of the Huntersville Police Department to ensure that the access and use of ALPR data is consistent with respect for individual's privacy, civil liberties, and the law. [CALEA 41.3.9a]

DEFINITION OF TERMS (*The following definitions are for the limited purpose of this directive and may not apply in all other cases:*)

- A. **Automated License Plate Recognition (ALPR):** systems sometimes referred to colloquially as “Automatic License Plate Readers” are equipment consisting of fixed and mobile cameras and computer hardware/software used to automatically recognize and interpret characters on vehicle license plates. This data is then compared against data contained in NCIC, SLED, or DMV files that may bear some significance to law enforcement. This significance may come in the form of stolen cars, stolen tags, Amber Alerts, or wanted persons. LPR cameras record images of vehicles that may be queried against specific information for stated investigative purposes.

- B. **Hot List:** License plate numbers of stolen cars, vehicles owned by persons of interest, and vehicles associated with Amber Alerts that are regularly added to “hot lists” circulated among law enforcement agencies. Hot list information can come from a variety of sources, including stolen vehicle information from the National Insurance Crime Bureau and NCIC, as well as national Amber Alerts and Department of Homeland Security watch lists. These lists serve an officer safety function as well as an investigatory purpose. In addition to agency supported Hot Lists, users may also manually add license plate numbers to Hot Lists to be alerted if and when a vehicle license plate of interest is read by the ALPR system.

- C. **Hit:** A read matched to a plate that has previously been listed as stolen, or matched to a wanted person or Amber Alert, or some other factor supporting further law enforcement investigation.
- D. **Alert:** A visual and/or auditory notice of a hit that triggered when the ALPR system reads a license plate that is a match with information found in any information file such as NCIC.
 - o An alert is not conclusive confirmation that a license plate is wanted.
 - o Additional investigation is always warranted when an alert is indicated
- E. **Read/Scan:** Digital images of license plates and vehicles associated with metadata (i.e. date, time, and geographical coordinates associated with the vehicle capture) that are captured by the ALPR.
- F. **Digital Image:** Image produced of the license plate and the vehicle with each scan.
- G. **Verification:** The user of the digital image system will complete visual verification of each hit.
- H. **Confirmation:** When able or practical, each hit will be confirmed through NCIC, NCDMV, or other relevant databases prior to initiating an investigation and/or traffic stop.

GENERAL

1. The use of the ALPR systems and access to its database records is restricted, and is considered CJIS protected, and shall be used in accordance with the manufacturer's recommendations and this policy.
2. The use of ALPR systems is restricted for public safety related missions of this agency.
3. ALPR systems and associated equipment and databases are authorized for official public safety purposes. Misuse of this equipment and associated databases, or data, may be subject to sanctions and/or disciplinary actions.
4. ALPR systems and ALPR data and associated media are the property of this agency and intended for use in conducting official business with limited exceptions noted elsewhere in this general order.

ADMINISTRATION

The Assistant Vice Chancellor/Chief of Police or his designee shall select an employee(s) with administrative oversight for the ALPR system deployment and operations who is (are) responsible for the following:

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

Establishing protocols to preserve and document ALPR reads and alerts or hits that are acted on in the field or associated with investigations or prosecutions.

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

Ensuring the proper selection of the personnel approved to operate the ALPR system and maintaining an adequate number of trainees.

Ensuring compliance with the terms of any M.O.U. (Memoranda of Understanding) associated with ALPR systems.

Maintaining records identifying approved ALPR deployments and documenting their results, including appropriate documentation of significant incidents and arrests that are related to ALPR usage.

Designated trained personnel must complete a report after ALPR usage results in law enforcement action or significant events. Failure to do so will result in disciplinary action.

Authorizing any requests for ALPR systems use or data access according to the policies and guidelines of this agency.

Designated, trained personnel shall check equipment on a regular basis to ensure functionality and camera alignment. Any equipment that falls outside expected functionality shall be removed from service until deficiencies have been corrected or repaired.

Equipment that falls outside expected functionality shall not be used and shall be removed from service until the ALPR system is tested and repaired as necessary.

ALPR systems diagnostics and repairs, hardware or software upgrades/updates shall be made by agency authorized personnel or contractors.

AUTOMATED LICENSE PLATE READER SYSTEM USAGE

ALPR operation and access to ALPR collected data shall be for official agency purposes only.

All operators of the ALPR system shall keep their individual accounts secure and not allow anyone to access or use their account.

Only agency personnel who have been properly trained in the use and operational protocols of the ALPR system shall be permitted to use it.

ALPR ALERTS/HITS: PRIOR TO INITIATION OF THE STOP:

Visually verify that the vehicle plate number matches the plate number captured by the ALPR system, including both alphanumeric characters of the license plate and the state of issuance.

Verify the current status of the information provided by the hit through UNCSA Police Communications Center dispatchers when circumstances allow or are necessitated.

Receipt of a Hit is not sufficient probable cause to initiate a stop without verification. When able or practical, verification of the information is essential before initiating a stop, furthering the investigation, or taking any enforcement action.

5. *If an operator verifies a hit as being accurate, the operator shall take the appropriate enforcement action in accordance with agency policy and procedure and document the incident by creating a report.
6. Administrators and operators may manually enter information into the ALPR Hot Lists. Whenever information is manually entered into the Hot Lists:

It must be for legitimate law enforcement purposes.

*It is the responsibility of the person entering the information to remove the information once it no longer serves a legitimate law enforcement purpose. Failure to remove said invalid information may result in disciplinary action.

7. Searches of historical ALPR data within the ALPR system database shall be conducted in accordance with established agency policies and procedures.
8. Special Details: ALPR use during nontraditional deployments (e.g., during criminal investigation) must be approved by the Associate Vice Chancellor/Chief of Police or designee.

SUPERVISORS

1. Supervisors will monitor the use of ALPR systems and ensure they are being used properly.
2. Supervisors will ensure ALPR systems are deployed during the shift only by trained ALPR operators.
3. The supervisor shall investigate any damage to ALPRs in accordance with established procedures. Damage and any reports or documentation will be forwarded to the ALPR Administrator.

DATA SECURITY, RETENTION, AND ACCESS

1. All ALPR-generated data will be purged after a 30-day retention period unless a longer retention period has been identified for court or investigative purposes.
 - a) Preserving data in the ALPR system after 30 days will require a preservation request from a law enforcement agency or search warrant as prescribed under N.C.G.S 20-183.32.
 - b) For retention of the report outside the ALPR system beyond the 30-day retention period, officers may scan the ALPR system report into an investigative case file.

- c) The ALPR system automatically erases stored data when the retention period has elapsed.
- 2. Access to ALPR data is restricted to Department personnel.
 - a) ALPR data may be shared by an authorized member of the Department with another criminal justice agency for a legitimate law enforcement purpose pursuant to a written request. Written requests may be in electronic format. Written requests for data should be preserved subject to applicable record retention statutes.
 - b) Any other use of this data is strictly forbidden.
 - c) Users will be able to access the ALPR data by providing the established username and password. This access will allow for the user to query information as it pertains to vehicle tags read by the tag reader cameras.
- 3. The ALPR System Administrator will determine the personnel to have access to the database for investigative queries and reports.
 - a) Any requests for database access will be handled on a case-by-case basis and those granted access will be provided the username and password for access.
 - b) Any database maintained by the UNCSA Police Department is to be kept in a secured environment. Access to this environment is to be controlled and logged. Should any database be based in the cloud, the vendor in control of providing the cloud services shall be responsible for the safekeeping of any information stored within the cloud at the level required by the government state or federal laws.
 - c) The UNCSA Police Department may grant its officers the ability to monitor or receive information from ALPR systems not under the control of its employees or under control of the UNCSA Police Department (i.e. privately owned systems) for as long as the following conditions are met:
 - 1) The ALPR system meets the guidelines set forth in NCGS 20-183.31.
 - 2) The ALPR system does not require burdensome proprietary software installed on computers owned by the UNCSA Police Department.
- 4. Information stored includes a photo of the registration plate showing the rear of the vehicle, a date and time stamp of when the registration plate was read by the ALPR and a GPS coordinate to identify the exact location the registration plate was read by the ALPR. *[CALEA 41.3.9b, d]*
- 5. In accordance with N.C.G.S. 20-183.31, any ALPR system utilized by the department will conform with the following requirements:
 - a) Data obtained from ALPRs shall be obtained, accessed, preserved, or disclosed only for law enforcement purposes.
 - b) Notwithstanding, data obtained under the authority of this Article shall not be used for the enforcement of traffic violations.
 - c) Auditing and reporting of ALPR system use, and effectiveness shall be made annually (or more frequently as ordered by the ALPR system administrator or department administration).

- d) All users of any ALPR system authorized by the department will comply with the information contained within this directive.

MAINTENANCE

1. Officers should not attempt to modify the ALPR system equipment or software operating system without permission of the ALPR System Administrator.
2. ALPR equipment shall be maintained per the requirements of the ALPR manufacturer the systems administrator is responsible for training users on the required day-to-day maintenance requirements if such exist.
3. The Assistant Vice Chancellor/Chief of Police or designee shall be notified of any ALPR equipment needing maintenance or repair.

ALPR SYSTEM ADMINISTRATOR

1. The Assistant Vice Chancellor/Chief of Police or designee will determine how the ALPR system will be integrated into the Department's patrol and investigative functions. They will also determine any restrictions for the use of the ALPR system.
2. The Assistant Vice Chancellor/Chief of Police or designee or ALPR System Administrator will validate training for system users to ensure they are properly trained before accessing ALPR data.
 - a) Training will be adequate to ensure proper operations of the system in accordance this directive.
 - b) All training will be documented.
3. The ALPR System Administrator will keep maintenance schedules and records for the ALPR system on file.
4. The ALPR System Administrator is responsible for conducting annual audits of the use of the ALPR system, additional random audits or audit so specific internal investigations are allowable should the System Administrator, Internal Affairs, Investigator, or the Chief of Police request one.
5. The ALPR System Administrator shall be notified immediately of any ALPR equipment needing maintenance or repair and ensure that all maintenance and repair of ALPR equipment is completed.

INDEX AS: Automated License Plate Recognition System Cameras

[CALEA 41.3.9a]	1
[CALEA 41.3.9b, d]	4
[CALEA 41.3.9c]	2