Black Mountain Police Department

Policy Manual

Policy Creation Date	Revision	Date of Revision	Approved by Chief of Police
03/28/2023	02		*Steven R Parker*

422 - Automated License Plate Readers (ALPRs)

422.4 PURPOSE AND SCOPE

The purpose of this policy is to provide ethical guidance for the capture, storage and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology (N.C.G.S. § 20-183.31). All ALPR data is for official law enforcement purposes only while protecting the constitutional rights of all people.

422.5 POLICY

The policy of the Black Mountain Police Department is to utilize ALPR technology for legitimate purposes only. ALPRs are used to capture and store digital evidence used in law enforcement investigations, find missing persons, identify suspects, and to further crime reduction strategies. license plate data and images while recognizing the established privacy rights of the public.

The use of LPRS is restricted to the personnel and law enforcement purposes outlined in this policy. All use of this technology inconsistent with this policy is strictly prohibited.

All data and images gathered by the ALPR are for the official use of this department, and other recognized law enforcement agencies. The information garnered may contain confidential information, it is not open to public review.

422.3 **Definitions**

Agency Administrator – the person assigned the responsibility of managing, auditing, and reporting.

Automated License Plate Readers (ALPRs) - equipment consisting of fixed and mobile cameras and computer hardware/software used to automatically recognize, interpret, and compare characters on a vehicle license plate against data contained in authorized law enforcement systems.

Hot List – known license plate numbers of stolen cars, persons of interest, and vehicles associated with Amber Alerts circulated among law enforcement agencies.

Hit - a match to a plate associated with a stolen vehicle, wanted person, Amber Alert, or other legitimate law enforcement purpose.

422.4 ADMINISTRATION

1. The ALPR technology, also known as License Plate Recognition (LPR), allows for the automated detection of license plates. It is used by the Black Mountain 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. It may also be used to gather information related to active warrants, homeland security, electronic surveillance, suspect interdiction and stolen property recovery.
2. All installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Deputy Chief. The Deputy Chief will assign members under the Deputy Chief's command to administer the day-to-day operation of the ALPR equipment and data.

3. The Chief of Police is ultimately responsible for:

    a. Establishing protocols for access, collection, storage, and retention of LPRS data and associated data files.
    b. Establishing protocols to preserve and document LPRS data that are acted on in the field or associated with investigations or prosecutions.
    c. Establishing protocols that protect the security and integrity of data captured by the LPRS.
    d. Ensuring the proper selection of the personnel approved to operate the LPRS and maintain training.
    e. Ensuring compliance with the terms of use associated with LPRS.
    f. Ensuring the LPRS follows NCSBI rules relevant to the technology.
    g. Maintaining records identifying approved LPRS locations and significant incidents and arrests that are related to LPRS usage.

4. Upon the conclusion of any law enforcement action, authorized personnel shall report the incident outcome in the LPRS and in any official police report required by the incident. In the Electronic Management System.
5. The designated Agency Administrator shall regularly inspect LPRS equipment for proper function and alignment.

    a. Equipment that falls outside expected functionality shall be removed from service until deficiencies have been corrected or repaired.
    b. Equipment that falls outside expected functionality shall not be used and shall be removed from service until the LPRS is tested and repaired as necessary.
    c. LPRS diagnostics and repairs, hardware or software upgrades and/or updates shall be made by agency authorized personnel or contractors.

422.5 OPERATIONS

Use of an ALPR is restricted to the purposes outlined below. Department members shall not use, or allow others to use, the equipment or database records for any unauthorized purpose.

1. LPRS access, preservation, and disclosures are for law enforcement purposes only.
2. Only personnel who have been properly trained in the use and protocols of the LPRS are permitted to use it.
3. All operators of the LPRS shall secure their individual account and never permit unauthorized access or use.
4. Operators may not share information captured by the LPRS with any person other than when allowable by law
5. Partial license plates and unique vehicle descriptions reported during crimes can be entered into the LPRS to identify suspect vehicles.
6. Every time the LPRS program is accessed, the user conducting the search shall complete the following information on the ALPR Search Request form in the electronic management system:
    a. OCA, event number, or other legitimate reason(s) for the search
    b. Investigative purpose
    c. Offense or incident type
    d. Specific investigative nexus
    e. Search parameters
    f. Date and time ranges
    g. Geographic area (cameras accessed)
    h. User conducting the search
    i. Results/actions taken.
7. LPRS data searches can be conducted at the request of other law enforcement agencies for official law enforcement purposes only, or when otherwise permitted by law.
8. In those cases, the call, report, and case number of the requesting agency shall be entered into the 'Search Reason' box.
9. Any searches conducted in this manner shall first be approved by the on-duty watch commander.
10. For instances where a case number has not been generated, the officer shall create a call for service, notating the reason for the search in the narrative.
11. While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped vehicles to canvass areas around homicides, shootings, and other major incidents. Partial license plates reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.
12. ~~No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.~~

13. No ALPR operator may access confidential department, state or federal data unless authorized to do so.

~~14. If practicable, the officer should verify an ALPR response through the Division of Criminal Investigation Network (DCIN) before taking enforcement action that is based solely on an ALPR alert (N.C.G.S. § 20-183.31).~~

15. ALPR data shall not be used for the enforcement of traffic violations (N.C.G.S. § 20-183.31)

422.6 ALPR ALERTS/HITS

1. The receipt of a "hit" is not sufficient probable cause for law enforcement action without human verification that the LPRS interpreted the image correctly.
2. When practicable and prior to the initiation of any law enforcement action, the officer shall:

    a. Manually verify that the alphanumeric characters and state of the license plate match the image captured by the LPRS.
    b. Verify the status of the information provided by the hit through the Hendersonville Police Emergency Communications Center or MDT query when circumstances allow or are necessitated.

3. When an officer verifies a hit as being accurate, he/she shall take the appropriate law enforcement action in accordance with agency policy and procedures.

422.7 ALPR HOT LIST ENTRIES

Hot lists are databases of license plate numbers and related vehicle information that are of interest to law enforcement. When an ALPR camera captures a vehicle's plate, the system can instantly compare it against a hot list. If there's a match, the system can trigger a real-time alert to investigators. There are two types of hot lists.

A. **Automatic matches and alerts**: ALPR systems compare scanned plates against SBI maintained National Crime Information Center (NCIC) databases of stolen vehicles, stolen plates, vehicles used in felonies and misdemeanors, carjackings, wanted persons, missing persons including juveniles, AMBER alerts, sex offenders, and protection orders. If there is a "hit" to one of these databases, officers receive an alert within seconds to allow them to locate the vehicle. This often leads to apprehension of a suspect, recovery of a stolen vehicle, recovery of a missing or endangered victim, and/or recovery of evidence from a crime (such as a handgun used in a homicide).

B. **Manual hot list**: Officers can set up a manual hot list of license plate numbers of suspects in their investigations so that they receive an alert when one of those vehicles' license plates is scanned by an ALPR. Entries require a finite end date and should automatically be removed upon expiration. A vehicle should not remain on a hot list indefinitely and should be removed as soon as it no longer serves a criminal justice purpose.
    a. Manual hotlist entries shall only be created for legitimate law enforcement purposes.
    b. An officer may enter a Manual Hot List in Essential Personnel with

supervisor approval only.

c. Members of CID have the authority to initiate a Manual Hot List entry without prior authorization. The ALPR Search form shall be completed in Essential Personnel.
d. LPRS used during non-traditional deployments (e.g., special operations or during criminal investigation) must be approved by the Chief of Police and the appropriate form shall be completed in Essential Personnel.

C. Manual Hot List entries will be reviewed by the Professional Standards Lieutenant regularly to determine if data needs to remain active for ongoing investigations.

~~422.7.1 SUPERVISOR RESPONSIBILITIES~~
~~Supervisors should appropriately monitor ALPR operators to ensure that use of the ALPR equipment and data is consistent with this policy (N.C.G.S. § 20-183.31). Any use of the ALPR system that violates the restrictions contained in this policy may result in disciplinary action.~~

422.8 PRESERVATION REQUESTS AND RETENTION

1. Captured plate data obtained by an automatic license plate reader system, operated by or on behalf of a law enforcement agency for law enforcement purposes, shall not be preserved for more than 90 days after the date the data is captured.
2. 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.
3. 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.
    A. The BMPD Automated License Plate Recognition Preservation Request form available in Power DMS shall be completed by the requesting officer, approved by a supervisor, and notarized.
    B. EXCEPTIONS: per NCGS 20-183.32 (b), data obtained by an automatic license plate reader may be preserved for more than 90 days pursuant to any of the following:
        (1) A preservation request
        (2) A search warrant issued pursuant to Article 11 of Chapter 15A of the General Statutes.
        (3) A federal search warrant issued in compliance with the Federal Rules of Criminal Procedure
4. For retention of the report outside the ALPR system beyond the 90-day retention period, officers may scan the ALPR system report into an investigative case file.
5. The ALPR system automatically erases stored data when the retention period has elapsed.

422.9 AUDITS

1. Monthly Audit
The ALPR Administrator is responsible for conducting a monthly audit of the agency's use of LPRS.

A. This audit will include:

1) the name of the operator(s) conducting each search;
2) the date/time for each search;
3) the offense type for each search; and
4) an official department issued case number or reason for each search

B. The Agency Administrator will report any discrepancies of use found during the audit and then forward the results of that audit to the Chief of Police no later than the tenth day of the month following the period subject to the analysis.
C. The auditor's review should look for the following criteria:
1) Excessive searches
2) Searches without case umbers
3) Repeated searches on the same plate
4) Searches outside normal duties, assignments, or work hours
5) Searches involving employees, family members, acquaintances, etc.
6) Unusually broad geographic searches
7) Searches with multiple case numbers, but for the same plate.
8) Exclusive external network searches.
D. This date may be extended with the approval of the Chief of Police.

2. **Annual Audit**
G.S. § 20-183.31 requires annual or more frequent auditing and reporting of ALPR use and effectiveness to the agency head. Audit records should be maintained according to the appropriate document retention schedule.

The audit should include a review of which employees should maintain access to the system based on their role/assignment, including a review of account inactivity.

1. The annual audit should include the following documentation:
A. User Activity
B. Search Justification
C. Data retention
D. Sharing
E. Security
F. Training Compliance
G. Hot list accuracy
H. False-alert rates
I. System effectiveness
J. Vendor compliance
K. Complaints
L. Misuse incidents

422.10 MAINTENANCE

1 LPRS camera lenses may be cleaned with glass cleaner or mild soap and water and soft, nonabrasive cloth.

2 Damage to LPRS equipment shall be immediately reported to the Agency Administrator who will document and investigate the damage.
3 3. The system administrator will notify the LPRS vendor or contractor if any maintenance or repair is needed.
4 Any observed damage or defects to LPRS cameras will be documented, and notification will be made to the LPRS vendor representative. If the device must be replaced or taken out of service, notifications will be made to the agency.

The Chief of Police or designee is responsible for ensuring systems and processes are in place for the proper collection and retention of ALPR data. When applicable, data will be transferred from vehicles to the designated storage in accordance with the programming of the systems and department policy.

All stored ALPR data should be retained in accordance with the established records retention schedule. Thereafter, ALPR data shall be purged after 90 days unless a warrant has been issued for the data or it is subject to a written and sworn retention request submitted pursuant to N.C.G.S. § 20-183.32.

Data being retained pursuant to a retention request should be downloaded onto portable media, booked into evidence and retained for a period of one year after the initial request unless a subsequent request to maintain the data is received(N.C.G.S. § 20-183.32)

4.6 ACCOUNTABILITY AND UPDATES

All data will be closely safeguarded and protected by both procedural and technological means. The Black Mountain Police Department will observe the following 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. 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.
3. Control Access – Member access will be assigned as follows:

ROLE	ACCESS
Patrol officer	Real-time alerts/limited searches
Investigator	Case related historical searches
Supervisor	Search review/approval
ALPR system administrator	System administration
Analyst	Approved searches for analytical reasons
Auditor	Read only audit access
IT/Security	Technical administration without investigative access

4. The ALPR system should be updated every 24 hours or as soon as practicable thereafter with any license plate data obtained from the DCI network or any other databases used in conjunction with the ALPR system (N.C.G.S. § 20-183.32).

~~4.6.1 SYSTEM INTEGRITY~~
~~The Chief of Police or his designee shall maintain a schedule to regularly perform audits, maintenance checks and any needed corrections or adjustments to the ALPR system. The audits shall be conducted at least annually and include a report of the use and effectiveness of the system (N.C.G.S. § 20-183.31).~~

4.7 DATA AND SHARING DISSEMINATION

ALPR data shall only be shared with another law enforcement agency or prosecutor upon a written request, which may be made electronically. The request must indicate the purpose for the request. The release of ALPR data is not required if the disclosure of requested ALPR data will compromise an on-going investigation (N.C.G.S. § 20-183.32).

Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Records Maintenance and Release Policy.

1. Both active and historical data should be considered for official law enforcement purposes only.

2. Information sharing between law enforcement agencies shall be for official law enforcement purposes only and be done in accordance with applicable policy and law.

3. All information sharing will be expressly documented according to applicable policy.

4. LPRS data is confidential and not public record. Data shall only be disclosed pursuant to a written or electronic request from a requesting agency. The request must indicate the purpose of the information requested.
5. Operators may not share information without a written or electronic (DCI) request from another law enforcement agency.

4.8 REQUESTS TO OUTSIDE AGENCIES

Members requesting the retention or release of ALPR data maintained by another agency should obtain supervisory approval using the appropriate form prior to making the request. Members may request the disclosure of data from another agency by submitting a request in writing. Members requesting that data be retained by another agency must submit a sworn written statement as required by N.C.G.S. § 20-183.32. A copy of any requests shall be retained in a case file.

Efforts should be made as soon as practicable to obtain a search warrant to access requested data. The member requesting the data should contact the outside agency to cancel any request should the information no longer be needed (N.C.G.S. § 20-183.31).

4.9 TRAINING

1. Users must be trained prior to being granted access to ALPR databases. Intial training should include:
    A. ALPR Purpose
    B. Agency Policy
    C. Legal Authority

D. Constitutional consideration
E. Investigative uses
F. Authorized/Prohibited uses
G. Alert/hit verifications
H. Historical Searches
I. Search Documentation
J. Hot lists
K. Data retention
L. Data sharing
M. Security
N. Privacy
O. Misuse scenarios
P. Audits and accountability
Q. Disciplinary consequences

2. Refresher training should be conducted before granting access and at least annually thereafter, and whenever there is a substantial policy, legal, or system change.
3. Supervisor training should include additional instruction on:
   A. reviewing searches
   B. Identifying misuse
   C. Reviewing audit reports
   D. Investigative documents
   E. Preservation requests
   F. Data-sharing requirements
4. No member is allowed the use of the ALPR mobile systems until training on the use, operation and retention of the ALPR equipment, collection of ALPR data and the security and release of ALPR data and documentation has been provided to the Major. (N.C.G.S. 20-183.31)

4.10 USE OF ALPR BY OUTSIDE AGENCIES

The use of the ALPR systems and technologies is allowed at the discretion of the Chief of Police or his designee. A written request of dates and times of use shall be submitted at least seventy-two hours prior to date of use, or as soon as practicable thereafter and can be submitted electronically to the Chief of Police.

The Chief of Police or his designee shall keep records of the dates and times used as provided in the Records Maintenance and Release Policy.

Any agency requesting the use of the ALPR systems and technology shall ~~attend training provided by the Town of Black Mountain or training offered by the company that the ALPR systems and technology is manufactured by.~~ have their own ALPR policy and be trained ALPR usage.

Documentation of the training shall be submitted with the initial request and shall be kept on file for posteriority.

(THIS POLICY IS CURRENTLY UNDER REVISION AND HAS NOT BEEN ADOPTED)