

MELROSE POLICE DEPARTMENT		Department Manual: Policy No. 5.18
AUTOMATED LICENSE PLATE RECOGNITION (ALPR) POLICY		
MASSACHUSETTS POLICE CREDITATION STANDARDS REFERENCED: 41.3.9		GENERAL ORDER
Effective Date: January 16, 2026	Issuing Authority <i>Kevin Faller</i> Kevin Faller Chief of Police	

I. PURPOSE & SCOPE

A. The purpose of this policy is to establish guidelines for the use, management, retention, access, and oversight of Automated License Plate Recognition (ALPR) technology. This policy is designed to:

1. Ensure ALPR systems are used **only for legitimate, official law enforcement and public safety purposes.**
2. Protect constitutional rights and civil liberties.
3. Ensure compliance with all applicable Massachusetts law, federal law, CJIS requirements, and public records laws.
4. Provide clear procedures for ALPR operations, data security, retention, auditing, and accountability.

B. This department may deploy fixed or mobile ALPR systems, as approved by the Chief of Police or designee. At present, the Melrose Police Department utilizes only fixed Flock cameras.

II. POLICY

- A. It is the policy of this department that:
1. ALPR systems and associated data may be used only by authorized personnel.
 2. All ALPR activity must be conducted in furtherance of official law enforcement or public safety operations.
 3. Unauthorized use, access, or dissemination of ALPR data is strictly prohibited and may result in disciplinary action, civil liability, or criminal prosecution.
 4. All user accounts must be individually assigned, password-protected, and secured with multi-factor authentication.
 5. All ALPR operations must comply with Massachusetts Public Records Law, CJIS policy, and all relevant federal statutes.

III. DEFINITIONS

Alert Data: Any information generated when an ALPR read matches a hot list entry.

ALPR: A system using high-speed cameras and software to capture, read, and compare vehicle license plates to relevant databases.

ALPR Administrator: Designated officer responsible for ALPR oversight, compliance, auditing, training, access authorization, and policy maintenance.

ALPR Program Technician: Designated officer responsible for system maintenance, training support, equipment checks, and troubleshooting.

ALPR Data: All images, metadata, scans, hot list matches, audit logs, search queries, and associated information.

ALPR Query Log: A record documenting each search, user name, date, time, and purpose.

Bulk Data: All non-hit scans collected by ALPR cameras, including metadata such as plate number, timestamp, GPS coordinates, camera location, and vehicle image.

Canadian Police Information Centre - the Canadian Police Information Centre (CPIC) that allows searchable identifiers in CPIC records to be transmitted to NCIC for storage and access, creating the Canadian Vehicle Index (CVI).

Hit/Alert: A notification that a scanned plate matches an entry in a hot list (e.g., stolen vehicle, wanted suspect, AMBER Alert).

Hot List: A database of plates associated with legitimate law enforcement interests, including NCIC, DCJIS, NCMEC, agency bulletins, and manually entered investigative plates.

Protective Interest Files/Lists: The National Crime Information Center's (NCIC's) Protective Interest File (PIF) was designed to aid law enforcement agencies that have a protective mission by providing timely information on individuals who threaten protected persons.

IV. AUTHORIZED USE OF ALPR

- A.** ALPR may be used only for:
 - 1. Criminal investigations
 - 2. Missing or endangered persons.
 - 3. Attempt to Locate (ATL) or Be on the Lookout (BOLO) alerts
 - 4. Stolen vehicles/plates
 - 5. Court-ordered surveillance or monitoring
 - 6. Department-related civil or internal investigations
 - 7. Public safety operations approved by the Chief of Police or his designee.

V. AUTHORIZED VS. PROHIBITED ALERT CATEGORIES

- A. Authorized Categories**
 - 1. Stolen Vehicle
 - 2. Stolen Plate
 - 3. Wanted Person
 - 4. Missing Person / Missing Child
 - 5. AMBER Alerts / NCMEC Alerts
 - 6. Protective Orders

7. Department Investigative Hot Lists

B. Prohibited Categories

(No user may activate alerts or create hot lists for the following)

1. Sex Offender registry
2. Gang affiliation
3. Immigration records
4. Violent Person or CPIC categories
5. “Suspected terrorist” or other federal watchlists without explicit federal task-force authorization
6. Protective Interest lists
7. Supervised Release lists
8. Any list devised to offend or violate Chapter 127 of the Acts of 2022, An Act Expanding Protections for Reproductive and Gender Affirming Care, the “Shield Law” or Chapter 16 of the Acts of 2025, An Act Strengthening Health Care Protections in the Commonwealth, the “Shield Law 2.0.”

- C. Exceptions may be granted only by the Chief of Police, or his designee, for a specific, documented public safety, or investigative purpose.

VI. MANUAL ENTRY OF LICENSE PLATES

A. Manual entries must:

1. Fit within authorized categories.
2. Be requested only for legitimate investigative or safety purposes.
3. Be approved by the ALPR Administrator or his designee.
4. Be verified through CJIS/NCIC before entry.
5. Be removed or updated immediately when no longer relevant.

VII. HIT CONFIRMATION & FIELD OPERATIONS

A. Before initiating a stop based on an ALPR alert:

1. Visually verify that the scanned image matches the plate number and issuing state.
2. Confirm through CJIS/NCIC/MDT/dispatch that the alert is current and valid.

3. Only after verification may officers initiate a stop, using appropriate safety and high-risk stop tactics when necessary.
4. An ALPR alert alone is not probable cause for enforcement action.

VIII. ADMINISTRATION & OVERSIGHT

A. ALPR Administrator Responsibilities

1. Approve and manage all user accounts.
2. Oversee all ALPR operations and deployments.
3. Establish data access, retention, and security protocols.
4. Conduct or direct quarterly audits of system use and query logs.
5. Maintain documentation of significant ALPR-related incidents or arrests.
6. Recommend updates to this policy annually.

B. Program Technician Responsibilities

1. Provide system training and technical support.
 - a) At a minimum, approved users will be required to complete the following before conducting any query. The courses are provided by Flock Safety:
 - (1) How to use Flock Academy
 - (2) Law Enforcement - Search Certification
 - (3) Law Enforcement - Alerts Certification
 - (4) Law Enforcement User Training Session
 - (5) Flock Safety Mobile Application
2. Conduct periodic equipment inspections and ensure camera alignment.
3. Identify malfunctioning equipment and notify the appropriate vendor/service provider.
4. Maintain records of trained operators.

IX. DATA SECURITY & ACCESS CONTROL

- A.** Access is limited to trained and authorized users with unique logins.
- B.** Where available, multi-factor authentication must be used.
- C.** Password sharing is prohibited.
- D.** All activity is automatically logged and subject to review.

X. DATA STORAGE & RETENTION

- A.** Bulk data is stored exclusively by ALPR vendors for 30 days, unless extended retention is required for evidence.
- B.** Data relating to investigations must be downloaded and stored as evidence according to department procedures.
- C.** All retained data must comply with Massachusetts Public Records Law.

XI. DATA SHARING & RELEASE

- A. ALPR data may only be shared with:**
 - 1. Law enforcement agencies approved by the ALPR Administrator
 - 2. Prosecutorial agencies
 - 3. Courts pursuant to legal process
 - 4. Non-law-enforcement requests must be processed according to public records law, with appropriate redaction.
- B. All requests must be documented with:**
 - 1. Requesting agency
 - 2. Requestor's name
 - 3. Legal basis and intended purpose
 - 4. Records provided
- C. Outside Access Requests and Approvals**
 - 1. Network access requests will be directed to the ALPR Administrator, or designee.
 - 2. Access Approvals will be made by the ALPR Administrator, or designee.

XII. AUDIT REQUIREMENTS

- A.** Quarterly audits will be conducted by the ALPR Administrator or designee and must include:
 - 1. Random sampling of officer searches
 - 2. Verification of search purpose
 - 3. Review of compliance with security controls
 - 4. Identification of anomalies or unauthorized access

5. Review of all Department Investigative Hot Lists for relevance, removal, and/or revision.
- B.** Audit results must be documented and retained. Documentation of the audit will be forwarded in writing to the Officer in Charge of Professional Standards and the Chief of Police.

XIII. TRAINING REQUIREMENTS

- A. All ALPR operators must complete:**
1. Initial training prior to system access
 2. Refresher training every 2 years
 3. Additional training after major system updates or legal changes
- B. Training must cover:**
1. System operation
 2. Data security & access protocols
 3. Legal requirements and privacy protections
 4. Authorized vs. prohibited uses
 5. Hit confirmation procedures
- C. Training records must be maintained by the ALPR Administrator.**

XIV. POLICY REVIEW

- A.** The ALPR Administrator shall conduct an annual review of this policy and recommend revisions based on:
1. Legal updates
 2. Technology advancements
 3. Audit findings

XV. VIOLATIONS

- A.** Unauthorized access, misuse of ALPR data, or violation of this policy may result in:
 - 1. Revocation of access
 - 2. Internal discipline
 - 3. Civil liability
 - 4. Criminal penalties