MEDWAY POLICE DEPARTMENT	1.35
AUTOMATED LICENSE PLATE READERS	
MASSACHUSETTS POLICE ACCREDITATION STANDARDS REFERENCED: **None**	

	Issuing Authority **William H. Kingsbury** ***Chief of Police***	Effective Date: **11/13/26** Revision: Review Date: **11/13/2027**

I. GENERAL CONSIDERATIONS

This General Order establishes uniform procedures for acquiring, deploying, accessing, using, sharing, retaining, preserving, auditing, and disclosing information obtained through the Medway Police Department's Flock Automated License Plate Reader ("ALPR") system.

The Medway Police Department recognizes that ALPR technology can provide significant public-safety benefits, including assisting in crime investigations, locating stolen vehicles, identifying vehicles associated with criminal investigations, locating missing or endangered persons, and developing investigative leads.

The Department further recognizes that ALPR technology collects location-associated information concerning vehicles traveling on public roadways and therefore shall be operated in a manner that protects constitutional rights, privacy, civil liberties, and public confidence.

This General Order establishes safeguards to ensure that ALPR technology is used for legitimate law-enforcement purposes and not for personal, discriminatory, retaliatory, harassing, or otherwise improper purposes.

II. POLICY

It is the policy of the Medway Police Department that:

1. ALPR technology shall be used only for legitimate, documented law-enforcement purposes.

2. Access to ALPR information shall be limited to authorized and trained Department personnel.
3. An ALPR alert is an investigative lead and, standing alone, does not establish reasonable suspicion or probable cause.
4. Before taking enforcement action based upon an ALPR alert, officers shall independently verify the license plate and other relevant information.
5. ALPR information shall not be used to monitor, track, or identify persons solely because they are exercising constitutionally protected rights or because of a protected characteristic.
6. ALPR information shall be retained only for as long as authorized by this policy, applicable law, litigation requirements, or a legitimate investigative need.
7. Access and searches shall be auditable.
8. ALPR information shall not be used for personal purposes or for matters unrelated to legitimate law-enforcement duties.
9. The Department shall maintain appropriate supervisory and administrative oversight of the ALPR program.
10. The Department shall periodically review its ALPR program to ensure that its use remains lawful, necessary, proportionate, and consistent with community expectations.

III. DEFINITIONS

A. Automated License Plate Recognition (ALPR) System

A system consisting of one or more fixed or mobile cameras and associated software that automatically captures and processes images of vehicles and license plates and converts license plate numbers, vehicle characteristics, and related information into computer-readable, searchable data.

B. ALPR Data

Information collected, stored, generated, or maintained through the ALPR system, including, as applicable:

- vehicle images;
- license plate images;
- license plate numbers;
- state or jurisdiction of issuance;
- date and time of capture;
- camera or capture location;
- direction of travel;
- vehicle characteristics, including type of vehicle, make, and color;

- confidence scores and other associated metadata;
- alert and hotlist information;
- search queries and search results; and
- audit records associated with access to or use of the system.

C. ALPR Alert

A notification generated when an ALPR system determines that a license plate or vehicle characteristic matches information in an authorized database, hot list, or alert list.

D. ALPR Search

A deliberate query of historical or current ALPR data conducted by an authorized user using a license plate number, vehicle characteristic, date, time, location, or other available search criterion.

E. Hot List

A list of license plates entered into or made available through an ALPR system to generate an alert when potentially matching information is detected.

F. Search Reason

A brief description of the legitimate law-enforcement purpose for which an ALPR search is conducted.

G. Case Number

A Department or outside-agency incident number associated with a legitimate law-enforcement purpose for which an ALPR search is conducted.

H. Exigent Circumstances

Circumstances in which immediate access to ALPR information is reasonably necessary to address an imminent threat of death, serious bodily injury, abduction, or another situation in which delay would materially compromise a legitimate law-enforcement objective.

I. ALPR Manager

The employee the Chief of Police designates to administer the Department's ALPR program.

J. External ALPR Data

ALPR data collected by another agency or entity and made available to the Department through an authorized sharing network or other lawful means.

K. Data Preservation

The retention of ALPR data beyond its routine deletion for an investigative, evidentiary, or other lawful purpose.

L. Legally Protected Health-Care Activity

Health-care activity protected under Massachusetts law, including reproductive and gender-affirming health care, as defined by applicable law.

IV. PROCEDURE

A. AUTHORITY AND LEGAL FRAMEWORK

The Department shall operate its ALPR program consistent with:

1. The Fourth Amendment to the United States Constitution;
2. Article 14 of the Massachusetts Declaration of Rights;
3. Applicable Massachusetts General Laws;
4. Applicable Massachusetts appellate decisions;
5. Applicable Massachusetts POST Commission requirements;
6. Applicable CJIS/DCJIS requirements;
7. Applicable public records and records-retention requirements;
8. Applicable court orders, warrants, subpoenas, and production orders;
9. Applicable Department policies; and
10. Applicable contractual, licensing, and security requirements governed by the Department's ALPR system.
11. The Department shall continually monitor changes in Massachusetts law concerning ALPR technology.

B. Commonwealth v. McCarthy

In *Commonwealth v. McCarthy*, 484 Mass. 493 (2020), the Massachusetts Supreme Judicial Court concluded that the limited ALPR deployment involved in that case did not constitute a search under Article 14 or the Fourth Amendment.

The Court nevertheless recognized that individuals possess a constitutionally protected privacy interest in the whole of their public movements and that sufficiently widespread ALPR deployment could produce a detailed "mosaic" of an individual's movements that implicates constitutional protections.

Accordingly, Department personnel shall not interpret *McCarthy* as establishing that all ALPR searches or uses are categorically free from constitutional restrictions.

When determining whether additional legal process or supervisory authorization is appropriate, consider the scope, duration, geographic coverage, sensitivity of locations, and purpose of an ALPR inquiry.

C. ALPR PROGRAM ADMINISTRATION

The Chief of Police shall have ultimate responsibility for the Department's ALPR program.

The Chief may designate an ALPR Manager to manage the system's day-to-day operations.

The ALPR Manager shall:

1. Maintain a current list of authorized users.
2. Coordinate user access, including the prompt modification or deactivation of accounts when appropriate.
3. Ensure users receive required training.
4. Coordinate system configuration with the ALPR vendor.
5. Establish appropriate user roles and permissions.
6. Monitor system use.
7. Conduct periodic audits.
8. Review unusual or potentially improper system activity.
9. Coordinate investigations of suspected misuse.
10. Maintain documentation concerning system configuration and camera deployment.
11. Coordinate data-retention, deletion, and preservation practices.
12. Periodically review external sharing permissions and participating agencies.
13. Oversee Department-created hot lists and alert lists.
14. Coordinate the response to system malfunctions, security incidents, or suspected unauthorized access.
15. Recommend modifications to the ALPR program when necessary.
16. Report significant compliance issues to the Chief of Police.
17. Conduct an annual review of this policy and the Department’s ALPR program.
18. Monitor relevant changes in law, contractual requirements, and ALPR system capabilities.

D. AUTHORIZED USERS

Access to the Department's ALPR system shall be limited to personnel specifically authorized by the Chief of Police or ALPR Manager.

Authorized users shall:

1. Use only their individually assigned credentials.
2. Protect passwords, multifactor authentication methods, or other authentication credentials.
3. Not permit another person to access or use their account.
4. Use the system only for authorized law-enforcement purposes.
5. Complete required training.
6. Comply with applicable search-documentation requirements.
7. Protect ALPR data from unauthorized access or disclosure.
8. Promptly report suspected unauthorized access, disclosure, or misuse.
9. Comply with all Department policy and applicable law.

Shared user accounts are prohibited with the exception of dispatch and OIC phones.

The Department shall promptly modify, suspend, or disable access when a user separates from the Department, changes assignments, no longer requires access, or the Chief of Police or ALPR Manager determines the user is ineligible for access.

E.TRAINING

No employee shall be authorized to use the Department’s ALPR system until completing Department-approved training.

Training shall include, at a minimum:

1. ALPR system operation, capabilities, and limitations;
2. Authorized and prohibited uses;
3. Constitutional, privacy, and civil-rights considerations;
4. Reasonable suspicion, probable cause, and verification of ALPR alerts;
5. Search reason, case number, and audit requirements;
6. Hotlist, alert list, external data, and sharing procedures;
7. Data retention, evidence preservation, and information security; and
8. Misuse and disciplinary consequences.

Users shall also complete any vendor-provided or product-specific training the Chief of Police or ALPR Manager deems necessary.

The Department shall provide periodic refresher training and update its training when material changes occur in applicable law, Department policy, or ALPR system capabilities.

F. AUTHORIZED USES

ALPR technology may be used for legitimate law-enforcement purposes, including:

1. Investigating criminal offenses and serious motor-vehicle incidents, including hit-and-run incidents;
2. Identifying or recovering stolen vehicles and license plates;
3. Locating missing or endangered persons and investigating suspected abductions;
4. Locating vehicles associated with valid warrants, AMBER Alerts, Silver Alerts, BOLOs, or other authorized emergency notifications;
5. Identifying vehicles associated with active investigations, crime scenes, or threats to public safety and developing or verifying investigative leads, and identifying potentially exculpatory information; and
6. Other legitimate law-enforcement purposes approved by a supervisor or authorized by Department policy.

ALPR information shall be treated as an investigative lead and appropriately verified before taking enforcement action.

G. PROHIBITED USES

ALPR technology shall not be used:

1. For personal, commercial, or political purposes, out of curiosity, for private disputes, or for civil debt collection;
2. To locate or monitor a person or vehicle, including a Department employee, or to conduct a background investigation without a legitimate law-enforcement purpose;
3. To retaliate against, harass, or intimidate any person;
4. Solely because of a person's protected characteristics or to identify or monitor vehicles associated with lawful demonstrations, religious services, political events, labor activities, or other constitutionally protected activity;
5. For civil-immigration enforcement, or to investigate, prosecute, or impose liability for protected health-care activity;
6. For traffic enforcement based solely on an ALPR detection, unless specifically authorized by law and Department policy;

7. To create a personal database or conduct surveillance unrelated to a legitimate law-enforcement purpose, or otherwise act inconsistently with this policy or applicable law.

Nothing in this section prohibits an otherwise lawful investigation based on independent and articulable law-enforcement grounds merely because its subject has an immigration-related status, receives or provides health care or is engaged in constitutionally protected activity.

Requests that reasonably appear to involve a prohibited purpose shall be referred to a supervisor and, when appropriate, legal counsel.

H. SENSITIVE LOCATIONS AND PROTECTED ACTIVITIES

Employees shall exercise heightened caution when ALPR information could reveal a vehicle's association with a sensitive location or constitutionally protected activity.

Sensitive locations and activities may include private residences, places of worship, medical or reproductive-health facilities, legal service providers, political or labor organizations, educational institutions, shelters, and lawful demonstrations.

ALPR searches shall not be conducted to identify vehicles associated with sensitive locations or protected activity unless supported by an independent, articulable, legitimate law-enforcement purpose.

Before conducting a search likely to produce a detailed picture of a person's movements through vehicle-location information over an extended period or across numerous locations, personnel shall consult the Detective Sergeant or Chief of Police. When appropriate, the Department shall consult the District Attorney's Office or legal counsel regarding the need for legal process.

I. ALPR SEARCH REQUIREMENTS

Every ALPR search shall have a legitimate law-enforcement purpose.

For every search, the user shall select the most accurate applicable offense type and enter a brief and accurate search reason. Entry of a case or incident number does not replace the required search reason. When known and readily available, a Department or outside-agency case or incident number should be entered in the designated field. The absence of a case or incident number shall not delay a search when immediate action is reasonably necessary due to exigent circumstances or another time-sensitive public safety need.

When an ALPR search produces information that materially contributes to or reasonably bears upon an investigation, the user shall document the relevant information and any resulting investigative action in the appropriate Department report. Relevant ALPR information, including potentially exculpatory information, shall be preserved in accordance with Department evidence procedures and applicable discovery obligations.

User shall not select an inaccurate offense type or enter a false or misleading search reason to facilitate or conceal a search. Violations may result in disciplinary action, and when applicable, criminal investigation.

J. CASE-NUMBER DOCUMENTATION

A case or incident number is not required to conduct an ALPR search, but should be entered whenever known and reasonably available. When a Department or outside-agency case number or incident number is entered, it shall be accurate and associated with the legitimate law-enforcement purpose for the search.

Employees shall not create a fictitious case number or enter an unrelated or generic case number to conceal the purpose of a search or circumvent documentation requirements.

K. EMERGENCY SEARCHES

An employee may conduct a time-sensitive ALPR search when reasonably necessary to address an imminent threat to life or public safety, an abduction, a missing or endangered person, an active violent crime, or a fleeing violent offender. Emergency access shall not be used merely because it is more convenient than following normal search procedures.

The user shall select the appropriate offense type and enter a search reason. The absence of a case or incident number shall not delay an emergency search.

Emergency circumstances, relevant information obtained, and any resulting Department action shall be documented as soon as practicable and remain subject to supervisory review.

L. ALPR ALERTS

An ALPR alert is an investigative lead and, standing alone, does not establish reasonable suspicion or probable cause for enforcement action.

Before acting on an alert, an officer shall, to the extent circumstances permit, visually confirm the license plate, issuing jurisdiction, vehicle description, and

verify through an appropriate law-enforcement database that the underlying record remains active. The officer shall consider the possibility of an inaccurate or outdated alert and determine whether the totality of the circumstances provides a lawful basis for the action.

If the alert cannot be reasonably verified, officers shall not take enforcement action based solely upon it.

Any resulting report shall identify the ALPR alert as the source of the information, the verification conducted, and the legal basis for the enforcement action.

M. HOT LISTS AND ALERT LISTS

A license plate may be added to a Department hot list only when there is a reasonable basis to believe that an alert would assist a legitimate investigation or public safety purpose.

Each entry shall include, when available, the plate and vehicle information, the reason for inclusion, the originating case number, and the expiration or review date.

The user shall select an expiration date reasonably related to the anticipated duration of the law enforcement need. Short-term matters, such as locating a missing person, should have a shorter expiration period, while protective orders, warrants, or continuing investigations may justify a longer period. An entry may be created without an expiration date only when supported by ongoing law-enforcement need and shall remain subject to periodic review.

Department hot lists shall generally apply to Department-controlled ALPR cameras. Hotlist information may be shared with or received from another agency only through an authorized sharing agreement consistent with this policy.

All hotlists created through a Department account, including lists maintained by individual users or not shared Department-wide, are subject to administrative access, audit, review, and removal by the ALPR Manager or other authorized system administrator.

An entry shall be removed when the vehicle is recovered, the warrant is located, the underlying alert is canceled or determined to be inaccurate, the investigation concludes, or the entry otherwise no longer serves a legitimate law-enforcement purpose.

N. DATA ACCURACY

ALPR systems may produce incomplete or inaccurate information due to environmental conditions, plate condition or design, camera positioning, obstructions, or software limitations. ALPR information shall be appropriately verified before enforcement action and shall not be represented as infallible or independently conclusive.

O. HISTORICAL SEARCHES

Historical ALPR searches shall be reasonably tailored to the legitimate investigative purpose and no broader than necessary to identify relevant information, including potentially exculpatory information.

A historical search may identify locations associated with a vehicle, determine where it may regularly travel or be found, and develop information about persons connected to the vehicle.

In determining the appropriate scope, users should consider the nature and urgency of the matter, the relevance of the time period, geographic area, cameras, and vehicle criteria involved, and whether the search may reveal activity at a sensitive location.

Greater scrutiny is required when ALPR searches are repeated, ongoing, or combined across numerous cameras or external networks in a way likely to reveal a detailed travel pattern, infer a person's residence, workplace, or routine, or otherwise function as sustained surveillance. Before conducting such searches, the user shall consult a supervisor and, when appropriate, the District Attorney's Office or legal counsel to determine whether judicial authorization is required.

P.EXTERNAL ALPR DATA AND INTERAGENCY SHARING

The Department recognizes that access to and sharing of external ALPR data can assist legitimate regional and multi-jurisdictional investigations while also creating privacy and accountability concerns. Employees may access external ALPR data for a legitimate law-enforcement purpose consistent with applicable law and this policy.

Department users should limit the geographic scope of a search when reasonably practicable. Because many ALPR systems require the manual selection of individual agencies, camera networks, or geographic areas, users may select all available ALPRs when a more limited selection would be unduly burdensome, time-sensitive circumstances exist, or the vehicle's location or route is unknown. The selection of all available ALPRs shall not, by itself, render a search unnecessarily broad, provided that the search serves a

legitimate law-enforcement purpose and the remaining search parameters are reasonably tailored to that purpose.

The Chief of Police or ALPR Manager may authorize standing sharing with another law-enforcement agency after reasonably considering the agency's operational need, geographic relationship, applicable laws, and safeguards governing access, auditing, and further dissemination. Geography may be considered but shall not, by itself, determine whether sharing is authorized.

The Department may conduct an ALPR search on behalf of a law-enforcement agency that does not have access to the Department's ALPR system. The requesting agency shall provide a legitimate law-enforcement purpose and, when available, a case or incident number. The Department user shall document the requesting agency and purpose in the required search-reason field and may share relevant results through an approved secure method.

When standing sharing has not been authorized, the Department may approve case-specific temporary sharing when reasonably necessary to assist a legitimate investigation or public-safety matter. Temporary sharing shall be limited in scope and duration and removed when no longer necessary.

Requests for assisted searches, Department ALPR data, or temporary sharing shall be documented through an approved form or other Department-approved method and include:

1. The requesting agency and contact person;
2. The investigative purpose
3. The case or incident number, when available;
4. The requested scope and duration; and
5. The approving official.

The Department shall not provide access to or share ALPR data for a purpose prohibited by law or this policy, including civil immigration enforcement or investigations involving legally protected health-care activity. The Department shall use available system controls to restrict prohibited access but shall not rely solely upon automated restrictions. The Chief of Police or ALPR Manager may limit or discontinue standing sharing with agencies in jurisdictions whose laws or practices create a heightened risk of prohibited use. This shall not prevent an assisted search or case-specific sharing for a verified, legitimate law-enforcement purpose.

The Department may deny a request or refer it for additional review when its purpose, scope, source, or surrounding circumstances create a heightened risk of unlawful or improper use. Suspected misrepresentation of an investigative purpose or use of Department ALPR data for a prohibited purpose may result

in the immediate suspension or termination of sharing and further administrative or legal review.

ALPR information retained or shared shall be handled in accordance with applicable evidence-preservation and discovery requirements.

The ALPR Manager shall periodically review external sharing permissions and discontinue access that is no longer necessary or appropriate.

The ALPR Manager shall maintain a current list of agencies with standing access to Department-controlled ALPR data. Requests for these records shall be handled in accordance with Massachusetts public-records law and applicable exemptions.

Q. FIRST AMENDMENT AND CIVIL RIGHTS PROTECTIONS

ALPR technology shall not be used to identify or monitor a vehicle or person solely because of a protected characteristic, political or religious affiliation, occupation as a journalist or attorney, union membership, or participation in lawful speech, assembly, worship, press, association, or other constitutionally protected activity.

ALPR technology shall not be used to discriminate against any person or to monitor protected associations without an independent and articulable law-enforcement purpose.

Nothing in this section prohibits a legitimate investigation based on independent and articulable law-enforcement grounds merely because its subject is also engaged in protected activity.

R. DATA RETENTION

Routine, non-preserved ALPR data shall be automatically deleted thirty (30) days after collection.

The Department has selected a thirty-day retention period because crimes and other public-safety matters may not be reported or connected to a vehicle immediately, and historical ALPR data may provide relevant investigative or exculpatory information. This period also aligns with the Town of Medway's general retention period for other municipal surveillance systems while limiting the unnecessary long-term accumulation of location data.

Data preserved in accordance with the following section may be retained internally beyond the routine thirty-day period.

The ALPR Manager shall periodically verify that automated deletion is functioning as intended and review whether the retention period remains appropriate.

No employee shall manually retain or export routine ALPR information to circumvent the Department's retention period.

S.INVESTIGATIVE PRESERVATION OF ALPR DATA

ALPR data may be preserved beyond the routine retention period when reasonably necessary for:

1. An active criminal investigation or prosecution;
2. Potentially inculpatory or exculpatory evidence or another discovery obligation;
3. A missing-person investigation;
4. Litigation or anticipated litigation;
5. A court order, lawful preservation request, or public records obligation;
6. An internal investigation; or
7. Another lawful purpose approved by a supervisor.

Preserved data shall be associated with the applicable case or record. Investigative personnel shall transfer or export evidentiary ALPR information to the Department's approved records or evidence-management system when appropriate.

When a search yields no matches or information relevant to the investigation, the user shall document in the applicable incident report that the search was conducted and produced no relevant results. No separate export is required in those circumstances. Any result that may be inculpatory, exculpatory, or otherwise relevant to the investigation, including information indicating that a vehicle was elsewhere when an offense occurred, shall be exported and preserved in accordance with this section. All searches remain recorded in the organizational audit log.

Information subject to litigation, a court order, a preservation request, or another legal requirement shall be preserved as required. Because underlying ALPR data is automatically purged from the Flock platform after thirty days, information falling within any of the categories above shall be exported as soon as practicable and transferred to the Department’s approved records or evidence-management system.

The Department shall not retain routine ALPR information indefinitely merely because it might possibly become useful at some future time.

T.EVIDENCE

When ALPR information is used as evidence, is potentially exculpatory, or is reasonably anticipated to be used as evidence, the investigator shall preserve it in accordance with Department evidence procedures.

When appropriate, preserved information should include:

1. The original image and associated metadata;
2. Plate number and issuing jurisdiction;
3. Vehicle characteristics;
4. Date, time, and camera location;
5. Search parameters and associated alert information;
6. Case number and user identification;
7. The originating agency or data source, when applicable; and
8. Documentation describing how the information was obtained.

Employees shall not alter or manipulate original evidentiary information. Cropped, enhanced, or annotated copies may be created for investigative or court purposes, provided the original is preserved, and any material modifications are documented.

U. PUBLIC RECORDS

ALPR information is subject to applicable Massachusetts public-records laws, exemptions, retention schedules, court orders, and Department records policies.

Employees shall not destroy, delete, alter, or withhold ALPR information to avoid a public records obligation.

Requests for ALPR records shall be processed through the Department's established public records procedures. The Department shall consult the Town's public records officer and/or legal counsel as necessary.

V.CJIS/DCJIS INFORMATION

Employees shall comply with all applicable CJIS and DCJIS requirements governing the access, use, storage, and dissemination of ALPR information that contains, is combined with, derived from, or used in conjunction with criminal-justice information obtained from restricted databases.

An ALPR system shall not be used to circumvent CJIS/DCJIS restrictions or to access information the employee is otherwise prohibited from obtaining.

W. INFORMATION SECURITY

Employees shall:

1. Maintain secure credentials;
2. Use only Department-authorized systems and accounts;
3. Protect ALPR information from unauthorized access and disclosure;
4. Not photograph, screenshot, transmit, upload, store, or disseminate ALPR information for personal purposes or through unauthorized applications, accounts, or services; and
5. Follow applicable CJIS and Department information-security requirements.

Any suspected unauthorized access, disclosure, loss, or compromise shall be reported immediately to a supervisor and the ALPR Manager.

X. AUDITING AND OVERSIGHT

The Department shall maintain an active audit program. The ALPR Manager shall conduct a quarterly audit of an appropriate sample of ALPR system activity. The Department shall promptly review automated alerts, suspected misuse, and other significant concerns.

The quarterly audit shall review available audit information, including:

1. The user conducting the search;
2. The date, time, and type of search;
3. The networks and time period searched;
4. The documented mandatory search reason;
5. The license plate queried and relevant case number, when entered;
6. Repeated, unusual, or unexplained search activity.

Audits shall be compared with applicable Departmental records, incident reports, or case files as necessary to confirm a legitimate law-enforcement purpose and compliance with this policy.

The Department shall use available automated audit and anomaly-detection functions to supplement, not replace, supervisory review.

Y.AUDIT RESPONSE

When an audit identifies potentially improper activity, the ALPR Manager shall:

1. Preserve relevant audit records and ALPR information, when available;

2. Notify the Chief or designee and determine whether access should be temporarily suspended;
3. Review the user, purpose, scope, and circumstances of the activity;
4. Determine whether information was improperly accessed or disseminated and whether any investigation, evidence, or discovery obligation was affected;
5. Initiate an administrative investigation and notify other agencies or authorities when appropriate or required; and
6. Document the findings, outcome, and any corrective action taken.

Potential misuse shall be handled in accordance with Department internal affairs and disciplinary procedures, applicable collective bargaining requirements, and POST Commission requirements

Z. EMPLOYEE MISUSE

Unauthorized ALPR access or use may constitute:

- violation of Department policy;
- misuse of Department technology;
- unauthorized access to law-enforcement information;
- violation of privacy rights;
- conduct unbecoming an employee;
- violation of applicable law; and/or
- grounds for disciplinary action up to and including termination.

AA. CONSTITUTIONAL REVIEW OF DEPLOYMENT

Because the constitutional analysis identified in *McCarthy* may depend upon the scope and density of ALPR deployment, the Department shall periodically evaluate whether its overall camera network could create a substantially more detailed record of vehicle movements than existed in *McCarthy*.

The review should consider:

1. The number, location, and geographic distribution of cameras;
2. Coverage of major roadways and proximity to sensitive locations;
3. Data-retention periods;
4. Access to external-network data;
5. Historical-search capabilities and frequency; and
6. The system's ability to reconstruct vehicle movements.

The Department shall consult legal counsel when a material expansion or change in system capabilities may raise additional constitutional concerns.

BB. ALPR DATA AND INVESTIGATIVE REPORTS

When ALPR information materially contributes to an investigation, the investigator should state that ALPR technology was used and explain the investigative purpose, the relevant date and time period, the general geographic scope, the information obtained, any verification conducted, and any resulting investigative action. Relevant inculpatory and exculpatory information should be documented. When a search yields no relevant results, this should be documented in the applicable report.

The report should clearly identify the source of material information by distinguishing what an officer personally observed, what was captured or reported by the ALPR system, what was obtained through another database, and what represents an investigative conclusion or inference. ALPR information should not be presented as a personally observed or independently verified fact unless verification occurred.

CC. ALPR AS AN INVESTIGATIVE LEAD

ALPR information shall generally be treated as an investigative lead requiring corroboration.

Investigators shall consider:

1. Reliability of the ALPR read;
2. Age of the information;
3. Accuracy of the underlying database;
4. Vehicle description;
5. License-plate configuration;
6. Possibility of a stolen, transferred, or cloned plate;
7. Possibility of a false read;
8. Whether the vehicle may have changed ownership; and
9. Whether the underlying warrant or alert remains active.

ALPR information identifies a vehicle or license plate, not its driver or occupants. The presence of a vehicle at a location shall not, standing alone, establish that a particular person was present or involved in criminal activity.

DD. ALPR AND WARRANTS / LEGAL PROCESS

Nothing in this policy authorizes an employee to circumvent a warrant requirement.

Where applicable law or constitutional doctrine requires judicial authorization, the Department shall obtain the appropriate warrant, order, subpoena, or other legal process.

Employees shall consult a supervisor and, when appropriate, the District Attorney's Office or municipal counsel when uncertain whether legal process is required.

EE. DATA SHARING WITH PRIVATE ENTITIES

The Department shall not sell, rent, lease, or otherwise commercially exploit ALPR data or authorize a vendor or contractor to use Department ALPR data for an independent commercial purpose.

ALPR data shall not be intentionally disclosed to a private person or entity except as required by law or legal process, necessary for a legitimate law-enforcement, public-safety, technical, or contractual purpose, or otherwise approved by the Chief of Police and permitted by law.

FF. ALPR VENDOR ACCESS

An ALPR vendor’s access to Department ALPR data shall be governed by the Department's applicable contract, terms and conditions, and applicable law.

The Department shall review vendor provisions periodically and upon contract renewal or a material change in vendor practices. The review shall include data ownership and permitted uses, vendor and subcontractor access, retention and deletion, storage and security, breach notification, data sharing, and audit capabilities.

To the extent contractually and technically available, the Department shall maintain control over retention, user access, sharing and deletion settings for Department-controlled ALPR data.

GG. DATA OWNERSHIP AND CONTROL

ALPR information collected through the Department's ALPR system is Department-controlled law-enforcement information. Subject to applicable law and contractual requirements, the Department controls who may access the information, its authorized uses, its sharing, and its retention, preservation, and deletion.

The Department does not authorize unrestricted access to its ALPR information.

HH. SYSTEM ACCURACY AND MAINTENANCE

The ALPR Manager shall coordinate with the ALPR vendor regarding:

1. camera functionality;
2. software updates;
3. system performance;
4. camera alignment;
5. equipment failures;
6. cybersecurity concerns;
7. data-deletion functionality;
8. audit functionality; and
9. other material system issues.

Known technical problems that could materially affect investigative reliability or information security shall be documented and promptly communicated to affected users. During a system outage, employees may use other authorized investigative resources but shall not circumvent Department security controls to access ALPR information.

II. COMPLAINTS REGARDING ALPR USE

Members of the public may submit complaints or concerns regarding the Department's use of ALPR technology. Complaints shall be handled consistently with Department complaint and internal-affairs procedures, with allegations of unauthorized surveillance, discriminatory use, improper access, disclosure, or other misuse referred for appropriate review.

The Department shall not retaliate against any person for submitting a good-faith complaint concerning ALPR use.

JJ. TRANSPARENCY

The Department shall endeavor to maintain reasonable public transparency regarding its ALPR program. Subject to applicable law and legitimate security considerations, the Department should make available this Policy and Procedure, general information about the program and camera network, retention and sharing practices, appropriate aggregate usage information, and contact information for questions or complaints.

The Chief, or designee, shall include relevant aggregate ALPR data in the Department’s annual report.

Nothing in this section requires disclosure of information that would compromise an investigation or system security, reveal protected information, or otherwise be exempt from disclosure under applicable law.

KK. ANNUAL PROGRAM AND POLICY REVIEW

At least annually, the ALPR Manager shall prepare a program review for the Chief of Police.

The review shall include, when reasonably available:

1. The number and location of cameras and the number of authorized users;
2. Searches, alerts, or other relevant usage information;
3. Documented investigations and outcomes assisted by ALPR, including stolen vehicle recoveries and missing person investigations;
4. External searches, temporary sharing and sharing-network configuration;
5. Audit findings, suspected misuse, policy violations, and complaints;
6. Compliance with retention, preservation, and information-security requirements;
7. Significant system, legal, or constitutional developments; and
8. Recommendations for program or policy modification.

The annual review may incorporate the constitutional deployment review required by this policy and procedure.

This Policy and Procedure shall be reviewed as part of the annual program review, and sooner when a material change in law, controlling court decision, POST Commission requirement, system functionality, or Department deployment occurs, following a significant privacy or security incident, if the ALPR vendor materially violates its contract or applicable terms, or when directed by the Chief of Police. Revision shall be made as necessary to remain consistent with applicable legal, privacy, security, and operational requirements.

LL. COMPLIANCE WITH LAW

Nothing in this policy and procedure authorizes conduct prohibited by applicable federal or Massachusetts law. If any provision conflicts with statute, regulation, controlling court decision, or binding order, the controlling legal authority shall govern pending formal revision of this General Order.

MM. SUPERVISORY RESPONSIBILITIES

Supervisors shall:

1. Promote employee understanding of and compliance with ALPR requirements;
2. Review significant ALPR-related investigative activity and documentation of emergency searches;
3. Address and report apparent misuse;
4. Oversee appropriate evidence preservation and the use of legal process when necessary.
5. Refer unusual constitutional or privacy issues to command staff;
6. Confirm that enforcement action is not based solely upon an unverified ALPR alert; and
7. Participate in periodic ALPR audits as directed.

NN. EMPLOYEE RESPONSIBILITIES

Every employee authorized to access ALPR information shall:

1. Know and follow this policy and procedure, and complete required training;
2. Maintain secure credentials and protect ALPR information from unauthorized access or disclosure;
3. Conduct searches only for legitimate purposes;
4. Select the most accurate offense type, enter the required search reason, and provide a case or incident number when known and available;
5. Verify ALPR alerts before taking enforcement action;
6. Document significant ALPR use and preserve relevant inculpatory or exculpatory information;
7. Immediately report suspected misuse, unauthorized access, or disclosure; and
8. Seek supervisory guidance when uncertain whether a proposed search or use is lawful or appropriate.