GRAFTON POLICE DEPARTMENT	Policy 7.10

Automated License Plate Readers (ALPR)

MASSACHUSETTS POLICE ACCREDITATION STANDARDS REFERENCED:

	Issuing Authority **Neil A. Minardi** ***Chief of Police***	Effective Date: 07/01/2025 Revision: 08/01/2026 Review Date:

GENERAL CONSIDERATIONS AND GUIDELINES

ALPR systems shall be utilized exclusively for authorized law enforcement activities and legitimate public safety purposes. The Department is committed to ensuring that this technology is employed in a manner that respects constitutional rights, maintains public trust, and adheres to applicable laws and regulations.

Compliance Requirement

All Department personnel authorized to operate or access ALPR systems must comply with the procedures and restrictions outlined in this policy. Violations of these guidelines may result in disciplinary action and potential legal consequences.

Accountability

The Department maintains a commitment to transparency and accountability in the use of surveillance technologies, ensuring that ALPR systems enhance public safety while protecting individual privacy rights and civil liberties.

POLICY

It is the policy of the Grafton Police Department to:

The purpose of this Policy is to establish guidelines and procedures for the proper use and application of automatic license plate recognition (ALPR) systems, the management of the data, and the maintenance of the equipment.

ACRONYMS & DEFINITIONS

Alert: A visual and/or auditory notice that is triggered when the ALPR system receives a potential hit on a license plate.

Alert data: Information captured by an ALPR relating to a license plate that matches the license plate on a hot list.

ALPR: Automatic License Plate Recognition. Automatic license plate recognition technology uses high-speed cameras combined with sophisticated computer algorithms capable of converting the images of license plates to electronically readable data. The ALPR system captures an image of a license plate and converts it to a text file using Optical Character Recognition (OCR) technology. The technology also compares the digital images of license plates to the CJIS-NCIC Hot file database.

ALPR data: Scan files, alert data, and any other documents or data generated by, or obtained thorough, utilization of the ALPR system.

ALPR Data Query Logs: A record of a search or query of ALPR data.

ALPR system: The ALPR camera and all associated equipment and databases.

Department: Town/City Police Department.

Fixed ALPR system: ALPR cameras that are permanently affixed to a structure, such as a pole, a traffic barrier, or a bridge.

GPS: Global positioning system.

Hit: An alert that a license plate matches a record maintained in the ALPR database related to stolen vehicles, wanted vehicles, or other alert type files that support investigation or which have been manually registered by a user for further investigation.

Hot list: License plate numbers of vehicles of interest, such as stolen vehicles, unregistered vehicles, vehicles owned by persons of interest, and vehicles associated with AMBER Alerts, Missing Child Alerts, Missing College Student Bulletins, Be On Look Out (BOLO), Attempt To Locate (ATL), and Wanted or Missing Person broadcasts or bulletins in which a license plate number is included, or other license plate numbers of interest entered by the Department or an authorized officer.

Hot list download: The method by which the hot list data is transferred to a computer within a law enforcement vehicle.

OCR: Optical Character Recognition. The technology that supports the automated reading and digitizing images of license plates that are captured by the ALPR system.

PROCEDURES

A. General

ALPR systems and associated equipment and databases are the property of this Department and authorized for official use only. Misuse of this equipment and associated databases or data is subject to sanctions and/or disciplinary actions, as determined by the policies, rules and regulations of the Department.

B. Administration

1. The Department shall designate an employee(s) in a command position with administrative oversight as the ALPR Administrator for the ALPR system deployment, operations, and maintenance. The ALPR Administrator or a designee shall be responsible for the following:

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

   (b) 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.

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

   (d) Ensuring the proper selection of the personnel approved to operate the ALPR system and maintaining an adequate number of trained and authorized users.

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

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

   (g) Managing and securing the data, including requests for searches of the ALPR data, hot lists, and backing up the ALPR data; and

(h) Ensuring that designated, trained personnel check equipment on a regular basis to ensure functionality and camera alignment and removing from service any equipment that falls outside expected functionality until deficiencies have been corrected.

2. ALPR systems repairs (hardware or software) shall be made by Department-authorized sources.

C. Automatic License Plate Recognition System Usage

1. ALPR systems and information shall be accessed and used only for official and legitimate law enforcement operations and public safety related purposes and may only be used based on specific and articulable facts of a concern for safety, wrongdoing, criminal investigations, Department-related civil investigations, or pursuant to a court order.

2. Searches of historical ALPR data shall be done in accordance with established departmental policies and procedures.

3. Only users who have been designated by the ALPR Administrator and properly trained in the use and operational protocols of the ALPR system shall be permitted to use the system. Only those users with an approved login and password will be allowed access to the ALPR system.

4. The agency's ALPR Administrator shall ensure that any changes in hardware, software, policy, or law are the subject of continuing in-service training or bulletins.

5. The use of ALPR technology must be approved by the agency head or designee.

6. When an enforcement action, investigation, or prosecution results from an ALPR hit, the hit will be preserved.

7. ALPR hot lists and data gathered by departmental ALPRs will be maintained securely.

8. Requests for searches of ALPR data to the ALPR Administrator may be made by members of this Department or by other law enforcement agencies subject to the provisions of this Policy.

9. Misuse of ALPR data, to include unauthorized searches, will expose the user to appropriate discipline. All search activity is recorded and available to public viewing in real-time.

D. Operational Procedures

1. At the start of each shift, users shall ensure that the ALPR system has been updated with the most current hot lists available.

2. At the beginning of each tour of duty, users should verify the aim of the ALPR camera(s) to ensure it is focused on the correct lanes of traffic.

3. ALPR equipment should be cleaned and maintained according to the manufacturer's recommendations.

4. Any damage to ALPR systems will be reported immediately according to the Department's established policy and procedures related to the loss of, or damage to, the Department's equipment.

5. The user shall notify the ALPR Administrator of any malfunction of the ALPR.

E. Manual Entry of Data

1. Users may become aware of additional potential license plate numbers of interest and may request those license plate numbers be entered into the Department hot list. License plates may be entered only when directed or authorized by the shift supervisor and only for official and legitimate law enforcement or public safety operations.

2. A second party check must be conducted on all manual entries.

3. Manual entries may include, but should not be limited to, an AMBER Alert, Missing Child Alert, Missing College Student Bulletin, Be on the Look Out (BOLO), Attempt to Locate (ATL), or Wanted or Missing Person broadcast or bulletin in which a license plate number is included. Such manual entries must be manually updated when the information changes or is no longer current.

4. Whenever a plate is manually entered into the ALPR system, the officer shall document the reason.

F. ALPR Alerts/Hits

Prior to initiation of a stop based on a hit or alert:

(a) Users shall visually verify that the vehicle plate number matches the plate number run by the ALPR system, including both alphanumeric characters of the license plate and the state of issuance.

(b) Users shall verify the current status of the plate through the Commonwealth's Criminal Justice Information System (CJIS), National Crime Information Center (NCIC), Department's Records Management System (RMS), or other appropriate source of data prior to a stop when circumstances allow or as soon as practicable.

INFORMATION MANAGEMENT

A. ALPR Data Query Logs

1. An automated log will be maintained for each transaction that will include the name of the individual accessing the data, along with the date and time of access.

2. Requests to review stored ALPR data and search results will be recorded and maintained in appropriate case files as determined by the rules and regulations of the Department.

3. ALPR Data Query Logs shall be maintained and secured.

4. Audits of agency query activity shall be conducted every thirty (30) days by the system administrator or as needed at the discretion of the Department head.

5. Any agency query activity flagged as suspicious or outside established normal parameters will be thoroughly investigated and the results of such an inquiry will be documented and archived.

B. ALPR Data Sharing and Dissemination

1. ALPR data can be accessed, retrieved, or shared for official and legitimate law enforcement operations or public safety purposes only.

2. Dissemination of ALPR data outside the Department shall be documented in a secondary dissemination log and shall be limited to state and local law enforcement agencies and must be subject to the same search criteria required of our own agency employees.

3. Information sharing among law enforcement agencies, other than the DCJIS, is determined by the Chief of Police.

4. The Grafton Police Department does not share data with the Department of Immigration and Customs Enforcement (ICE).

C. Data Retention

1. Data from ALPRs will be stored and maintained by the technology vendor for the prescribed retention period based on a 30-day rolling window.

2. Deletion of collected data is automated, and deletion is enforced by AWS lifecycle policies and does not rely on manual deletion.

3. Data deletion and access controls are independently validated through annual SOC-2 Type II audits, supported by tamper resistant audit logs and additional security certifications.

4. Data may be retained longer only when required by law, subject to a valid court order.

POLICY REVIEW

Annual Review: The ALPR Administrator shall conduct an annual review of this policy and all associated procedures, submitting recommendations for updates or amendments to the Department head as needed.

Ongoing Assessment: Given the evolving nature of ALPR technology, the Department will continuously monitor legal developments, technological advances, and operational outcomes to ensure this policy remains current and effective.

Adaptive Management: As experience with ALPR systems grows, this policy will be updated to address emerging legal considerations, technological capabilities, and best practices in the field.