





POLICIES AND PROCEDURES MANUAL

	AUTOMATED LICENSE PLATE RECOGNITION SYSTEM (ALPR)	
	POLICY NUMBER: 41-12	ISSUING AUTHORITY 
	EFFECTIVE DATE: August 7, 2025	Christine A. Elow Police Commissioner

I. GENERAL CONSIDERATIONS AND GUIDELINES

The use of Automated License Plate Recognition (“ALPR”) technology has allowed police departments to increase efficiency in investigations and has advanced public safety. ALPR systems are able to capture images of a vehicle and the vehicle's license plate, convert the plate image into alphanumeric characters using optical character recognition (“OCR”), and then compare the plate number acquired to one or more databases (also known as “hot lists”). This information can then be accessed instantaneously, allowing for an immediate response from law enforcement when needed.

The Cambridge Police Department will install ALPR technology at fixed locations throughout the City. This policy establishes the guidelines and procedures for when and how Cambridge Police Department members may utilize this technology.

II. POLICY

ALPR technology and associated equipment and databases, whether owned or under the control of the Cambridge Police Department, are authorized for official use only. Misuse of this equipment and associated databases or data shall be subject to sanctions and/or disciplinary actions, as determined by the rules, regulations, and policies of the City of Cambridge and of the Cambridge Police Department.

It is the policy of the Cambridge Police Department to:

- A. only utilize ALPR technology in the furtherance of official and legitimate law enforcement operations and public safety;
- B. require ALPR Operators and Administrators to abide by the guidelines set forth herein when using an ALPR system;
- C. abide by the City’s Surveillance Ordinance and all related state and federal laws, including public record laws;
- D. establish passwords for assigned users who will protect and maintain their respective password and strictly prohibit the sharing of passwords; and

- E. authorize access to ALPR systems only by assigned users.

III. DEFINITIONS

- A. *Alert*: A visual and/or auditory notice that is triggered when an ALPR system receives a potential hit on a license plate.
- B. *ALPR*: Automated License Plate Recognition technology. This technology uses high-speed cameras combined with sophisticated computer algorithms capable of converting 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 OCR technology. The technology also compares the digital images of license plates to the “hot list” database.
- C. *ALPR Operator*: Trained Cambridge Police Department personnel authorized to utilize ALPR systems and equipment.
- D. *ALPR Administrator*: Deputy Superintendent of the Procedural Justice Section or their designee responsible for (1) compliance with all applicable laws and regulations pertaining to ALPRs and (2) providing access and training to Department personnel in the operation of ALPR systems.
- E. *Alert Data*: Information captured by an ALPR related to a license plate on a “hot list”.
- F. *ALPR Data*: All information including scan files, alert data, and any other data generated, processed or obtained through utilization of an ALPR system.
- G. *ALPR Data Query Logs*: A record of a search or query of ALPR data.
- H. *ALPR System*: The ALPR camera and all associated equipment, databases and software operated by the Cambridge Police Department. This includes fixed ALPR cameras that are attached to a structure, such as a pole, a traffic barrier, or a bridge.
- I. *“Bulk” data*: The large volume of license plate scans collected over time regardless of whether they result in a “hit” or are connected to any investigation and/or license plate scan records. Bulk data is collected continuously by ALPR systems that do not immediately match any hot list or alert. These records include metadata such as: (1) Plate number (2) Timestamp (3) GPS coordinates (location of scan) (4) Camera ID or location (5) Vehicle image.
- J. *DCJIS*: Department of Criminal Justice Information Services.
- K. *GPS*: Global Positioning System.
- L. *“Hit”*: An alert that a license plate matches a record in an ALPR database of a vehicle of interest. For example, a hit may be related to a stolen vehicle, wanted vehicle, or an alert that has been manually registered by an ALPR Operator or Administrator for further investigation as authorized under the Procedures: Authorized Categories section IV(3)(a).
- M. *“Hot List”*: A comprehensive record of license plate numbers of stolen cars, vehicles owned/operated 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 the Commonwealth of Massachusetts DCJIS, the National Crime Information Center (NCIC), as well as national Amber Alerts and Department of Homeland Security watch lists. 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 in accordance with a legitimate law enforcement purpose.

- N. *“Hot List” Download*: The method by which the “hot list” data is transferred to a computer within a law enforcement vehicle or at a fixed terminal.
- O. *Optical Character Recognition (OCR)*: The technology that supports the automated reading and digitizing of images of license plates that are captured by an (ALPR) system.

IV. PROCEDURES

A. Guidelines for Use

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. 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 an ALPR system.
3. Authorized User Alert Profile: Personnel who have been designated as an authorized user with an approved login and password for access to the ALPR System must establish an alert profile at the time of initial login. In order to minimize disruption from excessive alerts, and to avoid alerts based on categories that are not actionable without a simple CJIS query, all personnel must comply with the following schedule for alert notifications:
 - a. Authorized categories:
 - (1) Stolen Vehicle
 - (2) Stolen Plate
 - (3) Warrants
 - (4) Missing Person
 - (5) Protective Order
 - (6) NCMEC Amber Alert
 - (7) Missing Child
 - (8) Cambridge Police Department “hot list”
 - b. Prohibited Categories:

- (1) Sex Offender
 - (2) Gang Affiliation or Suspected Terrorist
 - (3) CPIC Data Records
 - (4) Immigration
 - (5) Violent Person
 - (6) Protective Interest
 - (7) Supervised Release
4. Exceptions to the requirements for specific users may be authorized by the ALPR Administrator — the Deputy Superintendent of the Procedural Justice Section. These exceptions shall only be made to further a specific investigation or other public safety purpose.
 5. A search of historical ALPR data shall be done in accordance with established departmental policies and procedures.
 6. Requests to use an ALPR system during nontraditional deployments, such as special operations or criminal investigations, must be approved by the Administrator. In their absence, requests may be forwarded to the Duty Chief.
 7. Manual Entry of Data
 - a. Manual entries may include data related to, but not limited to an AMBER Alert, Missing Child Alert, Be On 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 entry must be updated when the information changes or is no longer current. Manual entries of data shall only be utilized concerning vehicles of interest in investigations or incidents that are connected to a specifically authorized category as determined by the Procedures: Authorized Categories section IV(3)(a).
 - b. Personnel may become aware of license plate numbers or vehicles of interest either through internal investigations or from outside agencies related to a specific incident or investigation. Where authorized, personnel may seek to have the relevant vehicle information manually entered into Cambridge Police Department's ALPR systems. The entry of this information will trigger alerts to be forwarded to Cambridge Police Department personnel and to the extent applicable to the designated agency from which the alert regarding the vehicle of interest originated. Designated agencies may include regional, state, or federal agencies.
 - c. Manual entries may only be entered by an authorized Cambridge Police Department supervisor and only for official and legitimate law enforcement or public safety operations.

- d. For all manual license plate entries, a verification of the license plate shall be queried via CJIS to verify the plate to be entered is accurate.
 - e. Manual entries may also include specific descriptions of vehicles that are being sought for specific crimes or in accordance with investigations.
8. "Hits" and Alerts
- a. Prior to initiation of a stop based on a "hit" or alert:
 - (1) Users shall visually verify that the vehicle plate number matches the plate number queried by an ALPR system, including both alphanumeric characters of the license plate and the state of issuance.
 - (2) Users shall verify the current status of the plate through CJIS, 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.
9. Mobile ALPR Procedures
- a. The Cambridge Police Department currently does not utilize mobile ALPR units. Should this change, the policy will be updated to reflect such.
- B. Administrative and Technical Support
1. Administrative Support
- a. The ALPR Administrator will oversee the department's ALPR operations. The Deputy Superintendent of the Procedural Justice Section shall serve in this capacity. Assigned duties of the Administrator include:
 - (1) establishing protocols for data entries, access, collection, storage & security, and retention of ALPR data and associated media files¹;
 - (2) establishing protocols to preserve and document ALPR data including "alerts" or "hits" that are acted on in the field or associated with investigations or prosecutions;
 - (3) establishing protocols to establish and ensure the security and integrity of data captured, stored, and/or retained by the ALPR system;
 - (4) ensuring that the ALPR system is used only for appropriate Department business and in accordance with this policy;
 - (5) monitoring the use of the ALPR and scheduling periodic audits;
 - (6) recommending updates to the ALPR policy;
 - (7) keeping informed of legal decisions, trends, and case law concerning ALPRs;

¹ In Accordance with 41.3.9 (d), (e), (f), (g)

- (8) coordinating with other Department personnel regarding the maintenance and retention of data;
- (9) maintaining records identifying approved ALPR deployments and documenting their results, including appropriate documentation of significant incidents and arrests that are related to ALPR usage; and
- (10) authorizing any requests for ALPR systems use or data access according to the policies and guidelines of this agency.

2. Technical Support

- a. An officer within the department will be designated as the Program Technician by the Deputy Superintendent of the Procedural Justice Section. In their absence, the Deputy Superintendent of the Procedural Justice Section may assign another officer(s) to assist as needed. Duties of the Technician include:
 - (1) training designated officers in the proper operation of ALPR systems;
 - (2) documenting those trained as Operators and reporting this information to the Training Unit;
 - (3) providing periodic equipment checks to ensure functionality and camera alignment, any equipment that falls outside expected functionality shall be removed from services until repaired;
 - (4) assisting other department personnel as needed;
 - (5) ensuring that designated and trained personnel examine 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; and
 - (6) ensuring the proper selection of the personnel approved to operate the ALPR system and maintaining an adequate number of trained and authorized user.

C. Data Security and Access

1. Access Control

- a. Access to ALPR systems and data shall be restricted to authorized personnel only. Access shall be granted only after proper authorization and training.

2. Authentication and Monitoring

- a. ALPR system access shall require unique user credentials and multi-factor authentication where feasible. System activity, including searches and data access, shall be logged and subject to periodic audits to ensure compliance.

3. Third-Party and Vendor Compliance

- a. Any third-party entity or vendor involved in ALPR system management, maintenance, or data storage must comply with department and CJIS security protocols.
4. All operators of the ALPR system will be assigned a unique login and password.
5. Employees shall not share usernames and passwords with anyone.
6. Data Query Records
 - a. In accordance with agreements between the Cambridge Police Department and contracted ALPR vendors, Department vendors will maintain a record for each transaction conducted on Department ALPR systems that will include the name of the individual accessing the data, along with the date and time of access, and the reason for the access.
 - b. Quarterly audits shall be conducted at the direction of the Deputy Superintendent of the Procedural Justice Section.
- D. 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. Information sharing among law enforcement agencies, other than DCJIS, should be governed by departmental policies or memoranda of understanding.
 3. Data may be released to the Office of the District Attorney for mandatory discovery in criminal prosecutions and through proper legal process in civil matters, such as court orders and subpoenas.
- E. Operator Training
 1. All personnel authorized to use ALPR technology shall complete initial training before being granted access to the system. Training shall cover the proper operation of ALPR equipment, data security protocols, and compliance with department policies.
 2. Personnel shall receive periodic refresher training, not less than once every two years, to ensure continued compliance with best practices, policy updates, and technological advancements related to ALPR use. Additional training may be required following significant system updates or changes in legal requirements.
 3. The department shall maintain records of all ALPR training, including course materials, attendance logs, and certifications of completion.
- F. Data Storage and Retention
 1. Bulk data from ALPRs will not be stored on the department's server and will only be stored by Cambridge Police Department ALPR vendors. Either by their own protocols or at the direction of the Department, Cambridge Police Department ALPR vendors shall not store bulk Department ALPR data for a period greater than thirty (30) days but not less than fourteen (14) days.

2. Department ALPR data may be downloaded and retained by department personnel in accordance with legitimate law enforcement purposes including specific investigations. This data shall be retained in accordance with Massachusetts Public Records laws and maintained until a final disposition has been reached in the case when applicable.
3. The Commanding Officer of the Records Unit shall be responsible for the maintenance and retention of data stored by Cambridge Police Department ALPR systems in accordance with MA Public Records Laws.

G. Policy Review

1. The ALPR Administrator is responsible for the annual review of this Policy and the policies and procedures contained herein and for making recommendations to the Department head for any necessary amendments. This is a new technology for the Department, and it may raise both legal and technological issues. As use of the technology progresses, the Department will continue to monitor and assess the appropriateness of this policy.