POLICY AND PROCEDURE NO. 586

License Plate Recognition System

Massachusetts Police Accreditation Standards:
41.3.9

Date Issued: December 8, 2015
Date Effective: October 2, 2026
Review Date: October 2, 2027 7 Pages

1. PURPOSE:

The purpose of this policy is to establish guidelines for the use of the License Plate Recognition (LPR) system by the Worcester Police Department. The LPR system assists officers in locating and investigating vehicles whose license plates have been identified by Department personnel as associated with an investigation. The system is intended to aid in the timely recovery of stolen vehicles, the investigation of missing and abducted persons, and the identification of vehicles of interest in criminal investigations. This policy governs the authorized use of the system, the responsibilities of operators, operator training, the entry of data into the system, the storage and security of collected data, and access to and retention of that data.

2. POLICY:

It is the policy of the Worcester Police Department that the LPR system be used solely for legitimate and permissible law enforcement purposes. Officers and authorized personnel shall operate the system in accordance with this policy, applicable federal and state law, and the Federal Driver's Privacy Protection Act (DPPA). No officer shall initiate a stop or other enforcement action based solely on an LPR alert. Use of the system is subject to the requirements of Policy 211 Bias-Free Policing.

3. SCOPE:

This policy applies to all sworn and civilian personnel who operate or interact with the LPR system and to all authorized personnel who access LPR data for investigative purposes. This policy governs all LPR equipment owned or controlled by the Department, whether vehicle-mounted, fixed, or portable, and all LPR data collected by that equipment.

4. DEFINITIONS:

A. License Plate Recognition (LPR) System

A camera-based system that captures digital images of vehicle license plates, applies optical character recognition to read the plate characters, and compares detected plates against hotlists created by Department personnel. LPR equipment may be vehicle-mounted, fixed, or portable. The data collected by that equipment may be stored on Department or City infrastructure or on infrastructure operated by a vendor under contract.

B. Hotlist

A list of license plates entered into the LPR system by Department personnel, against which detected plates are compared. A hotlist identifies vehicles by license plate only; it does not contain information about persons.

C. Hotlist Entry

A license plate placed on a hotlist under Section 6.D of this policy, together with the entering officer, case number, and law enforcement purpose recorded for it.

D. Alert

An audible or visual notification generated by the LPR system when a detected plate matches a hotlist entry. An alert is directed to the officer who made the entry.

E. LPR Network

A shared platform through which the Department may query LPR data collected by another agency or entity, or through which another agency or entity may query LPR data collected by the Department.

5. SYSTEM DESCRIPTION:

The LPR system captures a digital image of each vehicle and license plate entering its field of view. Each captured image is time-stamped and associated with location data. The system may also record vehicle characteristics derived from the captured image, such as make.

The system compares each detected plate against the hotlists maintained in the system. When a detected plate matches a hotlist entry, the system generates an alert to the officer who made the entry. An alert indicates only that a plate matching the entry was detected. It does not identify the driver of the vehicle and does not establish that the investigative basis for the entry still exists.

6. PROCEDURES:

A. Guidelines for Use

The LPR system shall be used only for legitimate and permissible law enforcement purposes, including the location of stolen vehicles, vehicles associated with missing persons or with AMBER and Silver Alerts, and vehicles of interest in criminal investigations. Personnel shall not use the LPR system to conduct any query unrelated to an authorized law enforcement purpose, including a query concerning the user, a family member, an acquaintance, or any person in whom the user has a personal interest. MPAC 41.3.9 [a]

LPR equipment should be deployed where traffic volume, crime analysis, or a specific investigative need supports its use, including roadways and areas of high traffic volume. Deployment locations shall not be selected on the basis of the demographic composition of an area.

The selection of LPR deployment locations and the entry of a license plate onto a hotlist shall not be based on a characteristic protected under Policy 211 Bias-Free Policing or on the exercise of a constitutional right.

The LPR system shall not be used to monitor or record the identity of persons participating in a lawful assembly, demonstration, religious observance, or other activity protected by the First Amendment to the United States Constitution or by the Massachusetts Declaration of Rights, absent a legitimate law enforcement purpose independent of the protected activity.

B. Prohibited Uses

The Department shall not use the LPR system, and shall not provide LPR data, in connection with an investigation into legally protected health care activity, including reproductive health care services and gender-affirming health care services that are lawful in Massachusetts. Massachusetts law prohibits a law enforcement officer, employee, or agency from providing assistance or information to a federal agency, to another state's law enforcement agency, or to a private party in connection with such an investigation, except where required by federal law. G.L. c. 147, § 63; G.L. c. 12, § 11I½.

The Department shall not release LPR data in response to a request that identifies civil immigration enforcement as its purpose.

No facial recognition or facial surveillance capability shall be enabled on the Department's LPR system.

A violation of this policy or other misuse of the system may result in disciplinary action, up to and including termination, and may subject the violator to civil and criminal liability.

C. Operator Responsibilities

An alert notifies the officer who made the hotlist entry that a plate matching the entry has been detected. An alert does not by itself constitute reasonable suspicion to stop a vehicle, or probable cause to arrest or to seize a vehicle.

Before taking any action on an alert, the officer shall confirm that the plate image captured by the LPR system matches the plate characters and issuing state of the hotlist entry, and that the investigative basis recorded for the entry still exists. MPAC 41.3.9 [b]

Any stop, arrest, or seizure arising from an alert shall be supported by reasonable suspicion or probable cause developed in the associated investigation, or by a warrant or court order, independent of the alert itself. If the officer independently observes a violation of law or other articulable facts establishing reasonable suspicion, the officer may conduct a stop on that independent basis.

An officer who takes enforcement action arising from an alert shall document in the incident or arrest report the alert, the confirmation performed, and the basis for the action taken.

D. Hotlist Entries

With the approval of a supervisor, an authorized officer may enter the license plate of a vehicle of interest onto a hotlist for a legitimate law enforcement purpose. Each hotlist entry shall include the plate information, the entering officer, the associated case number, and the law enforcement purpose supporting the entry. Entries shall be made only by personnel trained in LPR data entry procedures. MPAC 41.3.9 [d]

A hotlist entry shall expire ninety (90) days after it is made unless the entering officer's supervisor renews it for a further defined period, with the renewal recorded by a means the

LPR Administrator designates. The LPR Administrator shall remove expired entries and any entry for which the supporting law enforcement purpose no longer exists.

E. Searches of Retained LPR Data

Authorized personnel may search retained LPR data by full or partial plate number, issuing state, vehicle make or another vehicle characteristic recorded by the system, time frame, camera, and geographic area. A search shall be conducted only for a legitimate and permissible law enforcement purpose and shall be associated with a case number.

A search that is defined by geographic area or by vehicle characteristic rather than by a specific plate, or a search by partial plate that returns records for multiple vehicles, shall be approved in advance by a supervisor, and the requesting user shall record the law enforcement purpose supporting the search.

A vehicle identified through a search by vehicle characteristic is an investigative lead and does not by itself establish reasonable suspicion or probable cause.

F. Queries of LPR Data Held by Others

This subsection governs Department access to LPR data held by another agency, by a shared LPR network, or by a private entity, regardless of where that data is stored.

Personnel may query LPR data collected by another agency or held on an LPR network only on the same terms that apply to a search of Department LPR data under this section, and only where the query is supported by specific and articulable facts connecting the vehicle or plate to the associated case. Each such query shall be associated with a case number, shall be supported by a legitimate and permissible law enforcement purpose, and shall be subject to the supervisory approval requirements of this section. A query of a specific plate spanning more than thirty (30) days of data shall also be approved in advance by a supervisor.

Personnel shall not request that another agency or entity conduct an LPR query on the Department's behalf for a purpose that this policy prohibits.

The Department shall not enable reciprocal or network-wide access under which Department LPR data becomes searchable by other agencies as a condition of the Department's own search access, without the prior written approval of the Chief of Police. Where such access is enabled, the LPR Administrator shall record the scope of the access granted and shall include it in the inventory required by this policy.

G. Sharing LPR Data With Other Agencies

LPR data collected by the Department may be shared with another law enforcement agency in response to a specific, case-related request supported by a legitimate law enforcement purpose. Each request shall identify the requesting agency, the requesting individual, the case or investigation, and a purpose permitted under this policy. Sharing shall be approved by a supervisor and recorded in a log maintained by the LPR Administrator.

The Department shall not enter into a bulk, automated, or standing data-sharing arrangement that provides another agency or entity with routine or unrestricted access to Department LPR data without the prior written approval of the Chief of Police. The Department shall not sell, trade, or otherwise transfer LPR data for a commercial purpose.

The LPR Administrator shall maintain a current written inventory of each agency or entity holding standing access to Department LPR data, the basis for that access, and the date access was granted. The inventory shall be reviewed annually and provided to the Chief of Police.

Where an agency or entity holding access to Department LPR data is found to have used that access for a purpose prohibited by this policy, the LPR Administrator shall suspend the access and report the matter to the Chief of Police.

7. TRAINING:

Personnel assigned to operate LPR equipment shall receive training on the system before use. Training shall address system operation, the handling of alerts, the legal standards governing stops, arrests, and seizures arising from LPR alerts, query procedures, bias-free policing requirements, and the provisions of this policy. MPAC 41.3.9 [c]

Personnel authorized to search retained LPR data, to query LPR data held by another agency or network, or to make hotlist entries shall receive training on search procedures, data entry, the prohibited uses established by this policy, privacy requirements, and the provisions of this policy before being granted access.

Training shall be documented and records maintained by the Training Division.

8. DATA STORAGE, SECURITY, ACCESS, AND RETENTION:

A. Storage and Security

LPR data collected by Department equipment remains the property of the Worcester Police Department regardless of where that data is stored. Each plate detection is stored as an image of the vehicle, an image of the plate, and associated location, date, and time data, together with any vehicle characteristics recorded by the system.

Where LPR data is stored on infrastructure operated by a vendor or by another entity, the Department shall maintain a written agreement providing that the Department retains ownership and control of the data, that the Department has access to complete user and query audit records, that the data is encrypted in transit and at rest, that the data is deleted at the expiration of the retention period established by this policy, and that the data is not used, disclosed, or transferred for any purpose the Department has not authorized.

Access to the LPR system is by individual user account. A user shall not share account credentials and shall not access the system using another person's credentials. MPAC 41.3.9 [e]

B. Access and Retention

Access to retained LPR data is limited to trained personnel authorized by the LPR Administrator. Each search of retained LPR data shall be recorded, and the record shall include the user, the date and time of the search, the plate or other criteria searched, the associated case number, and the law enforcement purpose supporting the search. Where the LPR system does not capture each of these elements, the LPR Administrator shall maintain a record of the remaining elements by a means the Administrator designates. Search records are available for audit and review. MPAC 41.3.9 [f]

Search records maintained under this section shall be retained for seven (7) years, independent of the retention period established for LPR data.

Connecting a plate detection to an individual requires the use of other systems. Such access is governed by the Federal Driver's Privacy Protection Act (DPPA) and may be made only for a permissible purpose.

Retained LPR data shall be purged automatically no later than thirty (30) days after collection, or within any shorter period required by law. The LPR Administrator shall verify not less than annually that the purge is operating as configured and shall document that verification. LPR data obtained from another agency or from an LPR network is subject to the shorter of the retention period established by this policy and the retention period established by the source.

LPR data that constitutes evidence in a criminal investigation, that is subject to a discovery obligation, or that is subject to a preservation request or litigation hold shall be extracted from the system before the expiration of the retention period and handled in accordance with Policy 410 Handling Evidence and Property. The user extracting the data shall document the case number and the basis for preservation.

9. PROGRAM MANAGEMENT:

The Chief of Police shall designate an LPR Administrator responsible for management of the LPR program. The LPR Administrator shall maintain the list of authorized users, coordinate system maintenance and vendor agreements, maintain the search records, data-sharing log, and access inventory required by this policy, record the scope of any network access enabled, remove expired hotlist entries, and serve as the Department's point of contact for inquiries concerning the LPR program.

The LPR Administrator shall conduct a quarterly audit of system queries and access logs. The audit shall review not fewer than twenty-five (25) queries conducted during the quarter and shall verify that each query reviewed was associated with a case number and supported by a permissible law enforcement purpose. The audit shall reconcile the queries recorded by the LPR system against the search records maintained under this policy, and a query recorded by the system for which no corresponding search record exists shall be treated as a discrepancy. The audit shall include a review for repeated queries of the same license plate by the same user in the absence of an associated case.

Where an audit identifies a query that is not supported by a case number and a permissible law enforcement purpose, the LPR Administrator shall first seek to resolve the discrepancy with the user and the user's supervisor and shall document the resolution in the audit record. Where the discrepancy cannot be resolved, or where the inquiry indicates that the query was made for a purpose prohibited by this policy, the LPR Administrator shall report the matter to the Bureau of Professional Standards for investigation under Policy 500 Bureau of Professional Standards Investigations.

The LPR Administrator shall conduct an annual review of LPR system use, including a review of access logs, audit results, hotlist entries, network access, and data-sharing activity, to determine whether use of the system has conformed to this policy and applicable law. The

results of the annual review shall be documented and provided to the Chief of Police, and shall be available for release consistent with the Massachusetts public records law.

Per:

Paul B. Saucier
Chief of Police

Revisions:

October 2, 2026–

Complete rewrite and reformat to the ADA-compliant policy template. Replaced the sixty (60) day retention period for LPR data with thirty (30) days. Replaced the descriptions of hotlists downloaded from law enforcement databases, the types of queries, and the live query and entering-agency confirmation procedures with a description of hotlists created by Department personnel, alerts directed to the entering officer, and confirmation of the entry's investigative basis before action. Removed the statement that the system cannot determine the issuing state of a plate. Replaced the vehicle description and action-to-be-taken elements of a hotlist entry with the entering officer, case number, and law enforcement purpose. Added deployment guidance, a prohibited uses section, and bias-free policing and First Amendment limits. Added expiration and renewal of hotlist entries, searches of retained data by issuing state and vehicle characteristic, and supervisory approval for broad or extended searches. Replaced the designation of supervisors and detectives as search users with authorization by the LPR Administrator. Expanded the search log to record the criteria searched, the case number, and the law enforcement purpose, and added seven (7) year retention of search records. Added documentation of enforcement action arising from an alert, a prohibition on shared account credentials, and extraction of LPR data needed as evidence before the retention period expires. Added sections on scope, queries of LPR data held by others, and data sharing, and expanded training requirements. Added an LPR Administrator, a quarterly query audit, and an annual review provided to the Chief of Police. Replaced the statement that the database resides on a City server with requirements for a written agreement where LPR data is stored on vendor-operated infrastructure. Removed the statement that collected data contains no personally identifiable information and the For Official Use Only classification.

Original Issue Date: December 8, 2015