



Carmel Police Department

General Order #62



License Plate Reader

CALEA Standard #

Supporting Documents: [SOP Flock](#)

Purpose

The purpose of this policy is to establish clear guidelines for the authorized use, management, and oversight of License Plate Reader (LPR) technology by the Carmel Police Department. LPR systems shall be used only to support legitimate law enforcement and public safety purposes, including crime prevention, investigations, and locating vehicles or persons associated with criminal activity or public safety concerns. LPR systems and data shall be accessed and used only by authorized personnel, solely for official law enforcement purposes, and in a manner that protects privacy and promotes transparency, accountability, and public trust.

This policy governs LPR data collection, access, use, retention, sharing, and auditing to ensure compliance with applicable law and to protect individual privacy, civil rights, and civil liberties.

Policy Statement

It is the policy of the Carmel Police Department to regulate the deployment, access, use, and oversight of License Plate Reader (LPR) systems and LPR data to ensure lawful, ethical, and effective use in support of legitimate law enforcement and public safety purposes. Compliance with this policy is mandatory.

The Chief of Police, or the Chief's designee, shall have overall responsibility for the administration, oversight, and enforcement of this policy, including designation of personnel authorized to manage the LPR program and conduct audits.

Applicability

This policy applies to all Carmel Police Department personnel, as well as any authorized user or vendor, contractor, or other non-law-enforcement or public safety entity granted access to Department-owned or Department-managed LPR systems or LPR data. It governs all LPR technology and related data utilized by the Department, including fixed, mobile, and portable systems, and applies to all LPR data collected, stored, accessed, transmitted, shared, or retained by the Department, regardless of vendor, platform, or method of collection.

Compliance and Limitations

This policy does not supersede or replace applicable federal, state, or local laws, court orders, or other Department policies governing criminal investigations, records



Carmel Police Department

General Order #62



License Plate Reader

CALEA Standard #

Supporting Documents: [SOP Flock](#)

management, public records, or data privacy. In the event of a conflict, applicable law or controlling authority shall govern.

All individuals and entities subject to this policy are responsible for understanding and complying with its requirements. Failure to comply may result in administrative discipline, revocation of access, termination of agreements, or other appropriate action, consistent with Department policy and applicable law.

Definitions

For purposes of this policy, the following terms shall have the meanings set forth below.

Access: The ability to view, query, retrieve, download, export, or otherwise obtain LPR data, or to configure, manage, or administer LPR systems.

Alert: A system-generated notification indicating a potential match between an LPR read and a hot list entry. An alert alone does not establish reasonable suspicion or probable cause and shall be independently verified prior to enforcement action.

Audit: A documented review of LPR system access logs, searches, data use, sharing, and retention conducted to assess compliance with this policy and applicable law.

Authorized Purpose: A legitimate law enforcement or public safety purpose reasonably related to an individual's assigned duties or to an authorized investigation, operation, or response, and permitted by this policy.

Authorized User: A Carmel Police Department employee or other individual who has been formally approved, trained, and granted access to LPR systems or LPR data, with access limited to the minimum level necessary to perform assigned duties.

Hot List: A list of license plates or partial license plates associated with a documented law enforcement or public safety purpose that is used by an LPR system to identify potential matches.

Legal Hold: A requirement to preserve specific LPR data due to an active or reasonably anticipated criminal investigation, prosecution, civil proceeding, court order, or other lawful obligation that suspends routine deletion or purging.

License Plate Reader (LPR) System: A system of cameras, software, and related equipment used to capture images of vehicles and license plates, and to process, store, and manage associated data.



Carmel Police Department

General Order #62



License Plate Reader

CALEA Standard #

Supporting Documents: [SOP Flock](#)

LPR Data: Information captured, processed, generated, or stored by an LPR system, including license plate images, vehicle images, license plate characters, date and time of capture, geographic location, and system or camera identifiers.

Retention Period: The maximum length of time LPR data may be stored before deletion, unless retained pursuant to an authorized investigative need, legal hold, or court order.

Search: Any manual or automated query or review of LPR data using system search, filter, or analytic functions.

Search Justification: The documented law enforcement or public safety reason entered at the time of an LPR search.

Sharing or Dissemination: Disclosure of LPR data, or granting access to LPR data, to another authorized entity.

Verification: The process of confirming the accuracy and current status of an LPR alert prior to enforcement action.

Authorized Uses of LPR Systems and Data

LPR systems and LPR data may be accessed and used only for legitimate law enforcement and public safety purposes consistent with this policy and applicable law. Authorized uses include, but are not limited to, the following activities when directly related to an authorized purpose:

- Criminal investigations involving suspects, witnesses, or victims
- Locating missing, endangered, or at-risk persons
- Locating vehicles associated with wanted persons or judicial actions
- Public safety and threat mitigation involving credible threats to life or safety
- Stolen vehicles, stolen plates, and vehicle-related offenses
- Traffic safety, civil, or regulatory matters, including documented driving complaints or non-criminal violations when supported by articulable information
- System administration, maintenance, auditing, training, or quality assurance

Prohibited Uses of LPR Systems and Data

LPR systems and LPR data shall not be accessed, used, retained, or shared except as authorized by this policy or applicable law. Prohibited uses include, but are not limited to:



Carmel Police Department

General Order #62



License Plate Reader

CALEA Standard #

Supporting Documents: [SOP Flock](#)

- Circumventing legal, policy, retention, or approval safeguards
- Discriminatory or biased use based on characteristics protected by law
- Harassment, retaliation, or personal use, including any non-law-enforcement purpose
- Improper sharing or disclosure to unauthorized entities
- Monitoring lawful First Amendment-protected activity without legal basis
- Unauthorized prolonged or targeted surveillance without proper legal authorization

Access Control and Authorization Requirements

Access to LPR systems and LPR data shall be restricted to authorized users based on role and limited to the minimum level necessary to perform assigned duties.

Access shall be modified, suspended, or revoked when assignments change, employment ends, training requirements lapse, misuse is suspected or confirmed, or at the discretion of the Chief of Police or the Chief's designee.

Vendor, contractor, or other non-law-enforcement or public safety access shall be permitted only when necessary for system installation, configuration, maintenance, troubleshooting, auditing, training, or technical support, and only with Department authorization. Such access shall be limited in scope and duration and shall not include independent analysis, use, retention, or dissemination of LPR data. Vendor or contractor access shall be subject to the same access control, credentialing, monitoring, and audit requirements applicable to authorized users.

Each authorized user shall be assigned unique login credentials. Sharing of credentials is prohibited. LPR system access logs shall be maintained and subject to administrative review and audit.

Training Requirements

Prior to access, authorized users shall complete Department-approved training addressing program purpose, authorized and prohibited uses, privacy protections, system limitations, legal considerations, documentation requirements, and consequences of misuse. Refresher training shall be required as determined by the Department. Completion of required training shall be documented.

Data Collection



Carmel Police Department

General Order #62



License Plate Reader

CALEA Standard #

Supporting Documents: [SOP Flock](#)

LPR systems may collect images and related data only when lawfully installed or deployed. Image capture shall be limited to vehicles and license plates lawfully visible from the system's location or vantage point, including public places, locations accessible to the public, or private property where installation or access is lawfully authorized or otherwise lawful. LPR systems shall not be used to intentionally capture images from areas not lawfully observable from the system's vantage point, nor to circumvent reasonable expectations of privacy protected by law.

Data Retention

LPR data shall be retained only for the minimum period necessary to support authorized purposes and consistency with applicable law.

Unless otherwise required by law or legal process, LPR data owned or controlled by the Carmel Police Department shall be automatically retained for a period not to exceed 30 days, after which it shall be deleted or purged in accordance with Department policy and system capabilities. LPR data subject to a legal hold or evidentiary requirement may be retained for the duration required by law and applicable Department policy.

LPR data accessed from or provided by another source remains subject to the retention policies and legal obligations of the originating source.

Sharing and Dissemination of LPR Data

All sharing or access under this section shall serve a legitimate law enforcement or public safety purpose and comply with applicable law.

The Carmel Police Department may authorize other law enforcement or public safety agencies to receive access to Department-managed LPR systems or LPR data on either an ongoing or case-specific basis when operationally appropriate. Such access does not confer ownership, custody, or independent control of LPR data and remains subject to this policy, audit, and revocation by the Department. Recipient agencies shall not further share, disseminate, or grant access to LPR data without the prior authorization of the Carmel Police Department or as otherwise required by law.

All searches conducted by external agencies shall be documented, logged, and subject to administrative review and audit.

LPR data shall not be shared with private individuals, for commercial purposes, or in any manner that violates constitutional protections, applicable law, or Department policy.



Carmel Police Department

General Order #62



License Plate Reader

CALEA Standard #

Supporting Documents: [SOP Flock](#)

Audit and Review

The Department shall conduct periodic audits of LPR access and use, no less than annually, to ensure compliance with this policy and applicable law. Audits may be conducted more frequently at the discretion of the Department. Audit reports shall be retained in accordance with applicable records retention laws and Department policy. Access to LPR data for audit purposes shall not extend the applicable retention period unless subject to a legal hold or evidentiary requirement.

Misuse, Noncompliance, and Corrective Action

Misuse of LPR systems or data will not be tolerated. Violations may result in corrective action, discipline, revocation of access, termination of agreements, or other appropriate action, consistent with Department policy and applicable law.

Transparency and Public Information

The Department is committed to transparency while protecting operational security and privacy. Aggregate or summary information may be released when practicable and appropriate. The Department is not required to publish operational metrics or sensitive deployment details.

Public records requests shall be handled in accordance with applicable law and Department policy. Nothing in this policy creates a right of access beyond what is required by law.

Policy Review and Continuous Improvement

This policy shall be periodically reviewed and updated as necessary to reflect changes in law, technology, and best practices.