

**Higginsville Police Department
GENERAL ORDER**

Flock Camera Usage

EFFECTIVE DATE: April 2025

REVIEW DATE: July 1 – each year hereafter

1. Purpose & Scope

The purpose of this policy is to govern the operation, use, data retention, access, and oversight of automated license plate reader (LPR) systems (including those supplied by Flock Safety or similar vendors) used by Higginsville Police Department, to support legitimate law enforcement functions such as identifying stolen vehicles, wanted subjects, or other investigative needs. This policy applies to all employees, contractors, and authorized individuals who operate or access LPR systems and data.

2. Definitions

Automated License Plate Reader (LPR):

An electronic camera system that captures digital images of license plates and converts them into computer-readable data.

Captured Plate Data:

Includes the license plate number, date/time, GPS location, and any supplemental imagery or metadata captured by an LPR device.

Authorized Personnel:

Personnel designated by the Chief or designee who have completed required training and are authorized to access and use LPR data.

3. Authorized Uses

LPR systems may only be used for legitimate law enforcement purposes, including but not limited to:

- Identifying stolen or wanted vehicles.
- Supporting missing/endangered persons investigations.
- Identifying vehicles associated with active criminal investigations.
- Assisting in locating violators with outstanding warrants.

Personnel shall not use LPR systems for unrelated administrative or non-criminal purposes.

4. Deployment & Operation

- LPR cameras shall be deployed at locations approved by the Chief of Police or designee based on crime trends, public safety needs, and community input.
- Cameras shall be positioned so as not to intentionally capture images of pedestrians or private property beyond what is necessary for license plate reading.

5. Data Retention & Purging

Captured plate data shall be retained only as necessary for investigative and legal purposes and will be automatically purged in accordance with this agency's retention schedule:

- **Standard Data:** Retained for no longer than 30 days unless subject to an active investigation or preservation request.
- **Active Investigations:** Data relevant to an open case may be retained until the conclusion of the

- investigation or other legal requirement, subject to supervisory approval.
- Data purge schedules shall be documented and routinely monitored.

6. Data Access & Security

- Only authorized personnel may access LPR data.
- Access must be logged automatically by system audit trails including user identity, date/time, and purpose of access.
- Personnel shall use unique credentials and secure authentication; sharing of credentials is prohibited.
- Data shall be stored securely, and access controlled in compliance with department information security standards.
- LPR data may only be shared with other law enforcement agencies for official criminal justice purposes.

7. Privacy & Civil Liberties

- LPR use must balance public safety needs with individual privacy rights.
- Data shall not be used to track individuals for non-criminal administrative purposes.
- The agency shall avoid collecting more information than necessary for law enforcement objectives.

8. Training

All personnel authorized to operate LPR systems or access data must complete initial and recurring training covering:

- Policy requirements and legal constraints.
- System operation and limitations.
- Privacy, civil rights protections, and data security.
- Audit and accountability procedures.

9. Auditing, Oversight & Reporting

- The agency shall conduct periodic audits of LPR usage, access logs, and retention practices to ensure compliance with this policy and applicable law.
- Audit findings shall be reported to the Chief of Police or designee.
- Misuse of the system or data may result in disciplinary action or referral for prosecution.

10. Vendor / Third-Party Contracts

- Contracts with third-party vendors (e.g., Flock Safety) shall include provisions for:
 - Data ownership and access rights.
 - Compliance with public records laws and privacy protections.
 - Requirements for secure data handling and deletion per this policy.

11. Public Records & Transparency

- Information on LPR deployment and this policy shall be made publicly available (subject to lawful exemptions).
- Requests for LPR data will be handled in accordance with Missouri's public records laws and applicable exemptions, safeguarding sensitive law enforcement information where appropriate.

12. Policy Review

This policy shall be reviewed at least annually and updated to reflect legal changes, technological developments, community expectations, and best practices.