



Lexington Police Department

Lexington, Kentucky

GENERAL ORDER

BY THE AUTHORITY OF THE CHIEF OF POLICE

G.O. 2022-01 License Plate Readers

Rescinds: NA

Effective Date: 03/20/22 Distribution All Department Employees

Originally Issued: 2022

I. PURPOSE

The purpose of this policy is to provide guidance for the capture, storage, and use of digital data obtained through the use of license plate reader (LPR) technology.

II. POLICY

It is the policy of the Lexington Police Department to utilize LPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public.

It is department policy that all installation and maintenance of LPR equipment, as well as LPR data retention and access, shall be managed as determined by the Chief of Police or designee. The Chief of Police will assign a supervisor to administer the day-to-day operation of the LPR equipment and data.

It is department policy to use LPR systems only for legitimate law enforcement and public safety purposes. The LPR administrator shall ensure that LPRs are not deployed or used to enforce the law in any discriminatory manner that is prohibited by the United States Constitution and laws, the Commonwealth of Kentucky Constitution and laws, or the Lexington City Charter and Code of Ordinances.

III. DEFINITIONS

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

Hit: Alert from the LPR system that a scanned license plate number may be in the National Crime Information Center (NCIC) or other law enforcement database for a specific reason including, but not limited to, being related to a stolen car, wanted person, missing person, domestic violation protective order or terrorist-related activity.

Hot List: A list containing vehicles of interest with an articulable criminal nexus or valid public safety concern, including but not limited to, vehicles which are reported as stolen, display stolen license plates, vehicles linked to missing and/or wanted people, and vehicles flagged by law enforcement agencies.

License Plate Reader (LPR): A device that uses cameras and computer technology to compare digital images to database lists of known information of interest.

LPR Data: Data captured by the LPR cameras of an image (such as a license plate and description of vehicle on which it was displayed) within public view that was read by the device, including GPS coordinates and date and time information of the LPR system at the time of the LPR's read.

Vehicles of Interest: Including, but not limited to vehicles which are reported as stolen; display stolen license plates or tags; vehicles linked to missing and/or wanted persons and vehicles flagged by law enforcement agencies.

IV. PROCEDURES

A. General

1. Use of an LPR is restricted to the purposes outlined in policy and training.
 - a. Information gathered or collected, and records retained by department LPR system cameras will not be accessed or used for any purpose other than legitimate law enforcement or public safety purposes.
 - b. Officers shall not use, or allow others to use, the equipment or database records for any unauthorized purpose.
2. The following uses of the LPR system are specifically prohibited:
 - a. **Invasion of Privacy:** Except when done pursuant to a court order such as a search warrant, it is a violation of this policy to utilize the LPR to record license plates except those of vehicles that are exposed to public view (e.g., vehicles on a public road or street, or that are on private property but whose license plate(s) are visible from a public road, street, or a place to which members of the public have access, such as the parking lot of a shop or other business establishment).
 - b. **Harassment or Intimidation:** It is a violation of this policy to use the LPR system to harass and/or intimidate any individual or group.
 - c. **Personal Use:** It is a violation of this policy to use the LPR system or associated scan files or hot lists for any personal purpose.

B. Administration

1. All installation and maintenance of LPR equipment, as well as LPR data retention and access, shall be managed by the LPR administrator.
 - a. All LPR equipment shall be considered department owned property.
2. The Special Investigations Section lieutenant is the designated LPR administrator, with administrative oversight for LPR system operations and is responsible for:
 - a. Establishing protocols for access, collection, storage, and retention of LPR data and associated media files.

- b. Establishing protocols to preserve and document LPR reads and “alerts” or “hits” that are acted on in the field or associated with investigations or prosecutions.
 - c. Establishing protocols for LPR system monitoring to ensure the security and integrity of data captured, stored, and/or retained by the LPR system and compliance with applicable privacy laws.
 - d. Establishing the training requirements for officers to operate the LPR system, and coordinating with the Training Section as needed.
 - e. Maintaining records identifying approved LPR deployments and documenting their results, including appropriate documentation of significant incidents and arrests that are related to LPR usage.
 - f. Analyzing crime patterns and demographic information when an LPR is moved or when additional LPRs are added to the department’s LPR system.
 - g. Authorizing any requests for LPR systems use or data access in consultation with the Chief and according to department policies and guidelines.
- 3. Officers will report any damage to department LPR equipment, via the chain of command, to the LPR administrator who will coordinate any necessary repairs.
 - 4. The LPR administrator will ensure that designated, trained personnel check LPR equipment on a regular basis to ensure functionality and camera alignment.
 - 5. Repairs or modifications to LPR systems hardware or software, shall only be made by authorized sources or employees as determined by the LPR administrator.

C. License Plate Reader System Usage

- 1. LPR operation, all data and images gathered by the LPR, and access to LPR collected data shall be for the official use of this department.
- 2. Only properly trained employees are allowed access to the LPR system, to operate LPR equipment, to access LPR data, or to collect LPR information.
- 3. To ensure proper operation and facilitate oversight of the LPR system, all trained users are required to have individual credentials for access and use of the LPR system and/or data, which has the ability to be fully audited.
- 4. Officers shall not use personal devices to take or upload images to the LPR system.

D. Operations

- 1. LPR Alerts/Hits:
 - a. E911 will monitor the LPR system for alerts and dispatch officers as appropriate.

- b. If practicable, officers should confirm the license plate from the alert matches the license plate of the observed vehicle prior to initiating a stop.
- c. Absent exigent circumstances, the officer shall verify the suspect and/or vehicle is still wanted if the alert was generated due to the inclusion of the suspect and/or vehicle on a state or national database.
- d. The officer shall verify an LPR response through the appropriate database before taking enforcement action that is based solely on an LPR alert.
- e. Because the LPR alert may relate to a vehicle and may not relate to the person operating the vehicle, officers are reminded that they need to have reasonable suspicion and/or probable cause to make a stop of any vehicle.
- f. Any traffic stop resulting from an LPR alert will have “LPR alert” added to the call’s narrative.

2. Hot Lists

- a. Designation of hot lists to be utilized by the LPR system shall be made by the LPR administrator or designee.
 - 1. Specific hot lists shall be approved and entered by the LPR administrator (or designee) within the LPR system.
 - 2. All plates, vehicles, and suspect information entered into the LPR system will also contain the following information:
 - a. Entering user’s name
 - b. Requesting officer’s name
 - c. Related case number
 - d. Short synopsis describing the nature of the originating call
- b. Internal requests to add information to the LPR system shall be done by using the currently approved department form. The requests will be processed by the LPR administrator (or designee) and added to the system as appropriate.
- c. Exigent requests and requests from outside law enforcement agencies will be sent to the Duty Commander. If the Duty Commander determines the request is for legitimate law enforcement purposes, they will notify the on-call Intelligence Unit detective for entry into the LPR system.
- d. The LPR administrator (or designee) shall audit local hot list entries weekly, by requesting justification from the requesting officer, case detective, or supervisor to keep

the entry on the hot list. If acceptable justification is not received within seven days of the request, the entry shall be removed.

3. Special Details

a. LPR use during nontraditional deployments (e.g., special operations or during a criminal investigation) must be approved by the BOI Assistant Chief.

E. LPR Data Detection Browsing Audits

1. Before an officer can access the LPR database to browse LPR detections, the inquiring officer must document a reason for the inquiry within the LPR system.
2. It is the responsibility of the LPR administrator or the Chief's designee to ensure that an audit is conducted of LPR detection browsing inquiries at least once each quarter. PIU will audit a sampling of the LPR system utilization from the prior period to verify proper use in accordance with the authorized uses.
3. The audit shall be documented in writing and forwarded to the Chief. The audit shall include any data errors found so that such errors can be corrected. After review by the Chief, the audit and any associated documentation shall be filed and retained by the LPR administrator.

F. Data Collection and Retention

1. All data will be closely safeguarded and protected by both procedural and technological means.
2. The LPR vendor will store and ensure proper maintenance and security of data.
3. The department will retain LPR data for a maximum of 30 days, unless a longer retention period is required by KRS or applicable records retention schedules.
 - a. If data has evidentiary value, it must be stored according to policy as soon as practicable.

G. Releasing LPR Data

1. LPR data may be released to other authorized and verified law enforcement officials and agencies for legitimate law enforcement purposes.
2. All non-law enforcement requests for access to stored LPR data shall be processed in accordance with applicable law.
3. Any employee who receives a written request for LPR data will accept the request in accordance with G.O. series 2018-03 Open Records and will immediately forward the request to the Open Records Unit.