

	Berea Police Department SOP: 3.17			
	Automated License Plate Reader (ALPR)	EFFECTIVE DATE 05/07/2024	REVIEW DATE	REVISION DATE 06/16/2026
	CALEA STANDARDS	KACP STANDARDS		

- I. **Purpose:** The purpose of this policy is to provide guidance for the capture, storage, and use of digital data obtained using automated license plate reader (ALPR) technology.

- II. **Policy:** The policy of this agency is to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public. All data and images gathered by ALPR are for the official use of this agency. Because such data may contain confidential information, it may not be subject to public review. Berea Police Department SOP 3.17, Automated License Plate Reader, adopts the provisions of KRS 189.632 pertaining to a law enforcement agency's use of ALPR technology.

- III. **DEFINITIONS:**
 - A. **ALPR:** Allows for the automated detection of license plates along with the vehicle make, model, color, and unique identifiers through the agency's ALPR system. The technology is used to convert data associated with vehicle license plates and vehicle descriptions for official law enforcement purposes.
 - B. **ALPR Operator:** Trained agency members who may utilize ALPR systems/equipment. ALPR operators may be assigned to any position within the agency, and the ALPR administrator may order the deployment of the ALPR systems for use in various efforts.
 - C. **ALPR Administrator:** The chief of police or a designee serves as the ALPR administrator for the agency.
 - D. **Hot List:** A list of license plates associated with vehicles of interest compiled from one or more databases, including, but not limited to, the National Crime Information Center (NCIC), local "Be on the Lookout" (BOLO) notices, etc.
 - E. **Vehicles of Interest:** Including, but not limited to, vehicles reported as stolen; displaying stolen license plates or tags; vehicles linked to missing and/or wanted persons, and vehicles flagged by law enforcement agencies.
 - F. **Detection:** Data obtained by an ALPR of an image (such as a license plate) within public view that was read by the device, including potential images (such as the plate and description of the vehicle on which it was displayed), and information regarding the location of the ALPR system at the time of the ALPR's read.
 - G. **Hit:** Alert from the ALPR system that a scanned license plate number may be in the 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 violence protective order, or terrorist-related activity.
 - H. **LPR:** A fixed or mobile device that uses cameras and computer technology to compare digital images to database lists of known information of interest.

- I. **LPR Data:** Data captured by the LPR cameras of an image (such as a license plate and description of the 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.

IV. Procedures:

- A. Only properly trained, authorized personnel are allowed access to the ALPR system or to collect ALPR information. No member of this department shall operate ALPR equipment or access ALPR data without first completing departmentally approved training. Department training should include:
 1. Completion of current Flock Academy Law Enforcement User Training, Alerts training, and search training.
 2. Have read and acknowledged receipt of BPD SOP 3.17 Automated License Plate Reader.
- B. To ensure proper operation and facilitate oversight of the ALPR system, all users will be required to have an individual login for access and use of the systems and/or data, which can be fully audited.
- C. Department members will not use or allow others to use the equipment or database records for unauthorized purposes.
- D. The ALPR administrator will monitor the security of the system's information and compliance with applicable policies and laws.
- E. An ALPR shall only be used for official law enforcement business.
- F. An ALPR may be used in conjunction with any routine patrol operation or criminal investigation.
- G. Partial license plates and unique vehicle descriptions reported during major crimes should be entered into the ALPR system to identify suspected vehicles.
- H. An officer should verify an ALPR before taking enforcement action based solely on an ALPR alert.
 1. Once an alert is received, the operator should confirm that the observed license plate from the system matches the license plate of the observed vehicle before any law enforcement action is taken. An ALPR alert will be verified through an inquiry via MDT or dispatch.
 2. Officers will not take any police action that restricts the freedom of any individual based solely on an ALPR alert unless it has been validated. Because the ALPR 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 an enforcement stop of any vehicle.
- I. Hot lists are obtained or compiled from sources consistent with the purposes of the ALPR system set forth in this policy. Occasionally, there may be errors in the ALPR system's reading of a license plate. Therefore, an alert alone should not be a basis for police action other than following the vehicle of interest. Prior to initiation of a stop of a vehicle or other intervention based on an alert, officers shall undertake the following:

1. An officer must receive confirmation from the communications center or other department computer device that the license plate is still stolen, wanted, or otherwise of interest before proceeding, absent exigent circumstances.
2. Officers shall visually verify that the license plate of interest matches identically with the image of the license plate number captured (read) by the ALPR, including both the alphanumeric characters of the license plate, state of issue, and vehicle descriptors, before proceeding. Officers alerted to the fact that an observed motor vehicle's license plate is entered as a hot plate (hit) in a specific BOLO list are required to make a reasonable effort to confirm that a wanted person is in the vehicle and/or a reasonable basis exists before an officer would have a lawful basis to stop the vehicle.
3. Officers will clear all stops from hot list alerts by indicating the positive ALPR hit, i.e., with an arrest or other enforcement action.
4. General hot lists will be automatically downloaded into the ALPR system a minimum of once daily, with the most current data overwriting the old data.
5. All entries and updates of specific hot lists within the ALPR system will be documented by the requesting department member within the appropriate related case number. As such, specific hot lists will be approved by the ALPR administrators or designee before initial entry within the ALPR system.
6. All plates, vehicles, and other information entered into the ALPR system will contain the following information at a minimum:
 - a. Entering department member's name
 - b. Requesting officer's name
 - c. Related report number
 - d. Short synopsis describing the nature of the originating call

J. Patrol Officers - Patrol officers will be responsible for monitoring ALPR cameras on their assigned beats. Upon receipt of an ALPR notification, on-duty personnel will respond to the area of the capture and look for the suspect vehicle. If the vehicle is located, proper traffic stop procedures should be followed based on the type of hit, officer observations, and other factors present. The first officer identifying the wanted vehicle should wait for appropriate backup before initiating a traffic stop or engaging the vehicle.

K. Investigative Personnel

1. Investigative personnel may utilize ALPR data to assist in the identification of suspects involved in criminal activity.
2. Investigative personnel may have access enabling them to search the database for vehicles and/or persons of interest.
3. When investigative personnel utilize ALPR data to assist in the identification of a suspect or vehicle linked to criminal activity, the ALPR data will be downloaded from the system and attached to the investigative report as evidence.

L. ALPR Uses - The ALPR system and all data collected are the property of the agency. Only trained agency personnel may access and use the ALPR system for official and legitimate law enforcement purposes consistent with this policy. The following uses of the ALPR system are specifically prohibited:

1. **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 ALPR 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).
2. **Harassment or Intimidation:** It is a violation of this policy to use the ALPR system to harass and/or intimidate any individual or group.
3. **Use Based on a Protected Characteristic:** It is a violation of this policy to use the ALPR system or associated scan files or hot lists solely because of a person's or group's race, gender, religion, political affiliation, nationality, ethnicity, sexual orientation, disability, or other classification protected by law.
4. **Personal Use:** It is a violation of this policy to use the ALPR system or associated scan files or hot lists for any personal purpose.
5. **First Amendment Rights:** It is a violation of this policy to use the ALPR system or associated scan files or hot lists for the purpose or known effect of infringing upon First Amendment rights.
6. Anyone who engages in an impermissible use of the ALPR system or associated scan files or hot lists may be subject to disciplinary action.

M. Data Collection and Retention:

1. Databases:
 - a. The following databases are utilized for comparison with captured data:
 - i. National Crime Information Center (NCIC)
 - ii. National Center for Missing and Exploited Children (NCMEC)
 - iii. Law Enforcement agency created Hot Lists.
2. All data will be closely safeguarded and protected by both procedural and technological means.
3. The LPR vendor will store and ensure proper maintenance and security of data.
4. 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. If data has evidentiary value, it must be stored according to policy as soon as practicable. Information gathered or collected and records retained by the ALPR system will not be sold, accessed, or used for any purpose other than legitimate law enforcement or public safety purposes.

N. RELEASING ALPR DATA:

1. ALPR 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 submitted to the Chief of Police and legal counsel and processed in accordance with applicable law.
3. Any employee who receives a written request for LPR data will immediately forward the request to the Chief of Police and the custodian of records.

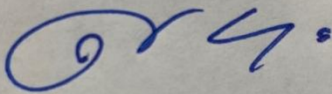
O. Accountability and Safeguards - All data will be closely safeguarded and protected by both procedural and technological means. The agency will observe the following safeguards regarding access to and use of stored data:

1. All ALPR data downloaded to a mobile device, computer, or MDT shall be accessible only through a login/password-protected system capable of documenting all access to information by name, date, and time.
2. Persons approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relates to a specific criminal investigation or department-related civil or administrative action.
3. Every ALPR detection browsing inquiry must be documented by either the associated agency case number or incident number and/or a reason for the inquiry.

P. ALPR Data Detection Browsing Audits

1. Before an officer can access the ALPR database to browse ALPR detections, the inquiring officer must document a reason for the inquiry within the ALPR system.
2. It is the responsibility of the chief of police's designee to ensure that an audit is conducted of ALPR detection-browsing inquiries at least once per quarter. The agency will audit a sampling of the ALPR system utilization from the prior period to verify proper use in accordance with the above authorized uses. The audit shall randomly select at least 50 detection browsing inquiries conducted by agency employees during the preceding period and determine if each inquiry meets the requirements established in this policy.
3. The audit shall be documented in the agency's current form tracking software and approved by the chief of police or their designee. The form should include any data errors found so that such errors can be corrected. After review by the chief of police or designee, the form and any associated documentation shall be retained in agency records in accordance with applicable records retention schedules.

By order of



CHIEF OF POLICE