



UNIVERSITY OF KENTUCKY POLICE DEPARTMENT SPECIAL ORDER NO. 14

Automated License Plate Reader Cameras

EFFECTIVE DATE
11/08/2022

KACP STANDARDS

I. POLICY:

It is the policy of the University of Kentucky Police Department (UKPD) to utilize Automated License Plate Reader (ALPR) technology on its campus to capture and store digital license plate data and images to assist in investigations for law enforcement purposes, including but not limited to conducting criminal investigations or ensuring compliance with local, state, or federal law, while recognizing the established privacy rights of the public, and for promoting public safety, deterring crime, and addressing auto theft only. ALPR technology shall not be used to monitor, track, identify, or compile information regarding individuals or groups based solely on the exercise of constitutional rights, including freedom of speech, association, religion, assembly, petition, or other protected activities. ALPR shall not target individuals based on protected characteristics legally safeguarded from discrimination, harassment, and unfair treatment, including those listed in the University of Kentucky's "Governing Regulation I – Declaration of Principles," Paragraph D, "Equal Dignity." All data and images gathered by ALPR are for the official use of this agency. ALPR data shall be maintained, accessed, released, or withheld only in accordance with applicable law, public record requirements, law enforcement exemptions, records retention schedules, and this policy.

This policy is related to ALPR technology administered by UKPD officials. ALPR administered by other university departments is described in section V. D. below.

II. PURPOSE:

Automated License Plate Readers utilize technology to scan, detect, and identify license plate numbers that appear on selected Hot Lists. ALPR devices and information contained within ALPR databases shall be utilized for law enforcement and public safety purposes only. All ALPRs shall be used and maintained in accordance with manufacturer recommendations and this policy.

III. DEFINITIONS

HOT LISTS: A list of license plates associated with vehicles of interest compiled from one or more databases as set out in the Data Collection and Retention section of this policy.

ALERT: A notification generated by an ALPR indicating that a vehicle passed an ALPR with a license plate that matches data held by the National Crime Information Center (NCIC) or another comparable database.

AUTOMATED LICENSE PLATE READER (ALPR): A system of one or more automated high-speed cameras used in combination with data processing to convert images of vehicles and license plates into computer-related data.

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.

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 Network of Kentucky (LINK)/National Crime Information Center (NCIC).

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.

CAPTURED LICENSE PLATE DATA: The vehicle characteristics captured by an ALPR including, but not limited to:

1. Global Positioning System (GPS) device coordinates
2. Date and time
3. Photographs of the license plate and vehicle
4. License plate number
5. Vehicle make, model, and color.

IV. PROCEDURES

The Chief of Police has ultimate authority over the use of ALPR cameras. The Police Administration Major or their designee is responsible for ensuring UKPD officials adhere to this policy. The Police Administration Major shall ensure the Security Operation Center (SOC) Major and the Director of the Central Kentucky Information Sharing and Threat Analysis Center (CITAC) perform audits for authorized units under their command to meet strict compliance standards.

- A. Only officials who have a bona fide requirement to access the ALPR management system shall be provided credentials. Credentials shall be approved by the Administration Major or their designee and entered at their direction. Sharing credentials is strictly prohibited and violations will result in revocation of access and corrective action.
- B. Officials provided access to the ALPR management system shall utilize the system for law enforcement purposes, including but not limited to conducting criminal investigations or ensuring compliance with local, state, or federal law. Access may be suspended, restricted, or revoked for operational, administrative, compliance, security, or policy reasons.
- C. No official shall adjust settings within the ALPR system without the approval of the Office of the Chief, the Deputy Chief of Operations or the Deputy Chief of Administration.
- D. The Administration Major, or their designee, shall be responsible for overseeing the development and administration of the training process for assuring proficiency of ALPR usage. This shall include but not limited to:
 1. Understanding of Hot Lists, Hot List Notifications, the difference between internal and external notifications, and probable cause considerations for these lists.
 2. Developing criteria or thresholds for entering license plates into the system, the duration for those plates' entries and the expected response if those plates are detected.
 3. No personnel are permitted to access ALPR data without first completing the approved training.
- E. The Administration Major shall notify the UKPD Security Systems Manager of any repairs and replacement of damaged or non-functional ALPRs, who will be responsible for coordinating repair. All users are responsible for reporting hardware and software issues.
- F. All requests to add or change ALPR locations shall be forwarded to the Administration Major or his designee.

V. ALPR OPERATIONS

ALPR Operations are limited to ALPR devices installed on or about the University of Kentucky jurisdiction. UKPD Hotlist Notifications outside of UKPD jurisdiction shall be for investigative and/or information only. UKPD shall rely on LINK/NCIC hot-list notifications and department-approved UKPD manual hot-list entries. Manual entries may be created only for a documented public safety and law enforcement purpose and must include a UKPD case number or incident number, the reason for the entry, the entering or requesting official, the notification recipient, and the authorized duration of the entry. UKPD prohibits entering External agency lists, notifications, or searches.

- A. The ALPR Devices passively read license plates of moving or parked motor vehicles using ALPR optical character recognition technology and compares that against Hot Lists automatically downloaded from available LINK/NCIC wanted information.
- B. Manual additions, which further UKPD's legitimate investigative needs, may be entered into the UKPD Hot List by the SOC Major, CITAC Director, the Office of the Chief, or specifically designated authorized personnel. All entries must be accompanied by a UKPD, or appropriate task force, case number, reason for the entry and the email address for the person(s) who should be notified by the UKPD Hot List Notification. Examples of possible scenarios where manual entry of a license plate number include, but are not limited to:
 - 1. Be On Look Out (BOLO);
 - 2. Attempt to locate;
 - 3. Missing person/student;
 - 4. AMBER alert;
 - 5. Child abduction;
 - 6. Wanted Person.

C. Hot List Notifications

During operations, ALPR alerts are indicated by a notification. An ALPR alert shall not be used as the sole reason for a traffic stop or enforcement contact until the officer receiving the notification has verified that the Hot List entry matches the digital image displayed by the ALPR. If, for any reason the information does not match, the alert shall be rejected. If, however, the information does match, the alert shall be accepted and the officer shall independently verify the alert through LINK/NCIC.

- 1. Alert response procedures:
 - a. Police Communications Officers shall monitor notifications generated by the ALPR System and communication information to Patrol Supervisors for an appropriate response. Prior to performing a traffic stop based on an ALPR alert, the Police Officer or Police Communications Officer shall visually confirm that the scanned plate in the captured license plate data matches the alert and that the stop meets UKPD policy and applicable law. Officers shall independently validate the license plate and vehicle description visually from the ALPR system information provided by Police Communications, then run the vehicle tag via LINK/NCIC to confirm the entry is still valid. Officers responding to investigate the hit should advise the Police Communications Officer of the call type they are responding to and the location.
 - b. Supervisors shall manage and coordinate the appropriate number of resources responding the alert. If contact is made with individuals due to an ALPR system alert, the officer(s) shall follow established policy/procedures related to the type of incident they are handling.
 - c. When responding to Sex Offender, Wanted Persons, Gang/Terrorist, Violent Person, Missing Person Alerts; officers shall keep in mind the person linked to the alert/vehicle may not be the occupants of the vehicle at the time of the encounter. These encounters must be handled respectfully and professionally. These alerts are information only for officers. Officers must have independent reasonable articulable suspicion or probable cause to make contact or detain.
 - d. When responding to UKPD Hot List notifications, officers should recognize this information will often be intelligence developed by CITAC, Flex Team or an investigating officer and intended to be information only. Independent reasonable suspicion or probable cause is needed to make contact.
 - e. Emergency vehicle response to Hot List notifications shall strictly adhere to the guidelines outlined in UKPD General Order 07: Emergency and Pursuit Driving. Officers shall be aware that stolen vehicles, stolen plates, stolen registration and wanted persons alerts inherently increase the potential for fleeing. Well-planned tactics, including simply observing as the vehicle travels through UKPD jurisdiction, should be considered, following all UKPD policy/procedures.

D. ALPR Database Inquiries

Investigative queries into the ALPR system database shall be limited to law enforcement purposes only. Each inquiry shall be accompanied with a reason for the inquiry, the case or incident number, and the responsible officer requiring the information. When ALPR data is sought primarily to reconstruct an individual's historical movements over time, officers should consult with supervisors, legal counsel, or prosecutors regarding whether judicial process, including a search warrant, is appropriate under applicable law. Where an ALPR device is operated on campus by non-UKPD units for purposes other than law enforcement, requests for data from those systems shall be made in keeping with federal, state, and local law, as well as University regulations and policies.

VI. USE/RELEASE OF ALPR DEVICE DATABASE

Personnel shall not release any information obtained by the ALPR devices to non-law enforcement personnel unless required by law. Using or disseminating information from the ALPR databases for personal reasons, curiosity, personal interest, broad exploratory searches, or efforts lacking documented law enforcement purposes shall be cause for corrective action, up to and including termination and possible criminal charges. ALPR data shall not be sold, shared, accessed or transferred except for purposes authorized by Kentucky law, this policy or a valid legal process. Release to non-law enforcement entities shall occur only after review under applicable law and approval through UKPD procedures.

VII. DATA COLLECTION AND RETENTION:

A. Databases

1. The following sources or systems may be used for ALPR comparison, alerting, storage, or authorized access, subject to this policy and applicable law:
 - a. National Crime Information Center (NCIC)
 - b. Law Information Network of Kentucky (LINK)
 - c. Law Enforcement agency created Hot Lists
 - d. Department-approved ALPR vendor or data-management platform.

B. All data will be closely safeguarded and protected by both procedural and technological means.

C. The department-approved ALPR vendor or data-management platform shall maintain ALPR data using appropriate administrative, technical, and physical safeguards, including role-based access, user authentication, audit logging, secure transmission, retention controls, and restrictions on authorized access, sale, disclosure, or secondary use.

D. ALPR detection data not associated with a documented law enforcement purpose shall be retained for no longer than 30 days. ALPR data retained for a criminal investigation, intelligence purpose, court proceeding, or other law enforcement purpose shall be stored, accessed, retained, and destroyed in accordance with the applicable records-retention schedule and KRS 189.632.

VII. ALPR DATA DETECTION BROWSING AUDITS

A. 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.

B. It is responsibility of the Administration Major to ensure that an audit is conducted of ALPR detection-browsing inquiries to occur every 90 days. The SOC Major and the CITAC Director 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 10 detection browsing inquiries conducted by agency employees during the preceding period and determine if each inquiry meets the requirements established in this policy.

C. The audit shall be documented in the form of an internal memorandum directed to the Office of the Chief. The memorandum shall include any data errors found so that such errors can be corrected. After

review by the Office of the Chief, or designee, the memorandum and any associated documentation shall be filed and retained in agency records with the Administration Major.

- D. The Administration Major or their designee shall audit the system administration and any functions performed by the system designee, the SOC Major, and the CITAC Director. This includes, but is not limited to, users, privileges, system settings and sharing requests. This shall be conducted every 90 days.

VIII. TRANSPARENCY, ACCOUNTABILITY, AND PUBLIC TRUST

- A. UKPD shall use ALPR technology only for lawful law enforcement and public safety purposes. The department shall maintain this policy for internal accountability and public understanding, subject to applicable law and operational security needs. Alleged or actual misuse, unauthorized access, or data-quality concerns shall be reported to the Office of the Chief or their designee for review. The department shall review this policy at least annually and update it as necessary based on changes in law, technology, vendor capabilities, audit findings or operational need.
- B. The department may periodically publish aggregate information regarding ALPR usage, including the number of cameras, alerts generated, audits completed, policy violations identified, stolen vehicles recovered, and missing persons located, when release is consistent with operational security and applicable law.
- C. UKPD shall make this Special Order publicly available.