OVERLAND PARK POLICE DEPARTMENT
STANDARD OPERATING PROCEDURE

NUMBER: 2370
TOPIC: AUTOMATED LICENSE PLATE READER (ALPR)
EFFECTIVE DATE: 10/08/2026
SUPERCEDES: 02/16/2026

/s/ Doreen Jokerst	/s/ Eric Houston	/s/ Eric Blevins
Chief of Police	**Deputy Chief**	**Public Safety Attorney**

I. PURPOSE
II. DEFINITIONS
III. PROCEDURE
A. ADMINISTRATION
B. AUTOMATED LICENSE PLATE READER USAGE
C. MAINTENANCE
D. RETENTION
E. TRANSPARENCY

CALEA References: 41.3.9 (A)(B)(C)(D)

I. PURPOSE

A. The purpose of this written directive is to provide members with guidelines regarding access to and proper use of the Automated License Plate Reader (ALPR) systems and data to ensure the privacy, civil rights, and civil liberties of individuals are not violated.

II. DEFINITIONS

A. *Alarm*: Is a visual and/or auditory notice triggered when the ALPR system receives a potential "hit" on a license plate.

B. *Automated License Plate Reader (ALPR)*: An electronic device using cameras and optical character recognition technology. ALPRs can be mounted on a law enforcement vehicle or placed in a stationary location to photograph, record, and compare license plate numbers to lists of known license plates of interest in law enforcement databases for investigative purposes.

C. *Hit*: Is a read matched to a license plate previously registered on a local or national "hot list" of vehicle license plates related to stolen vehicles, wanted vehicles, or other factors supporting an investigation, or manually registered by a user for further investigation.

D. *Hotlist*: Is a list of license plate numbers of stolen vehicles, stolen license plates, AMBER/SILVER alerts, missing persons, or vehicles associated with persons of interest, such as wanted individuals, that is regularly updated and circulated among law enforcement agencies. The hotlist is essential to ALPR systems, as it is required to notify law enforcement that a vehicle on the list is near an ALPR camera.

E. *Read*: Is a digital image of license plates and vehicles and associated metadata (e.g., date, time, and geographic coordinates associated with the vehicle image capture) that are captured by the ALPR system.

III. PROCEDURE 41.3.9 (A)(B)

A. ALPR technology helps police departments fulfill their mission of keeping communities safe. The ethical and responsible use of this technology is vital for maintaining a strong relationship with the community. Therefore, the use of this technology by the Overland Park Police Department is limited to the scope of community safety, investigations, and crime prevention.

1. ADMINISTRATION
   - a) The Police Technology Unit is designated and responsible for all aspects of the ALPR systems, including administration, training, technical troubleshooting, repairs, and auditing.
   - b) ALPR data mining, sharing, and dissemination will be for law enforcement purposes only and must be:
     - i) Based on at least reasonable suspicion of unlawful behavior or endangerment,
     - ii) Based upon an official investigation,
     - iii) For intelligence gathering, or
     - iv) Conducted by an authorized user and recorded for audit purposes.
   - c) Inquiries of the system for testing, maintenance, and training are authorized and will be recorded for audit purposes.
   - d) In the event a questionable use of the ALPR system is identified, the Technology Unit Captain or designee shall refer the matter to the Office of Professional Standards, and if misconduct is identified, the District Attorney's Office for review.
   - e) To ensure the ALPR system is being used appropriately, the Police Technology Unit, in coordination with the Office of Professional Standards, shall conduct monthly audits of system queries by OPPD users. These audits shall include, at a minimum, a random sample of one percent of all searches for the previous calendar month. Routine audits will include:
     - i) Accuracy, completeness, and security of ALPR data,
     - ii) System access history to monitor who accessed ALPR data, when, and for what purpose, and
     - iii) Continued compliance with policy.

B. AUTOMATED LICENSE PLATE READER SYSTEM USAGE 41.3.9 (A)(B)(C)

1. All ALPR operators must be trained in CJIS to access the ALPR systems. ALPR data will be stored securely and accessed through software requiring a unique username and password for each Member.

2. ALPR equipment will only be accessed and operated by personnel trained in its operation. Annual ALPR training will be provided to all authorized users.

3. ALPR software will contain access log and audit capabilities to track inquiries. Members must enter an associated case number or event number and a valid reason for each search, detailing sufficient facts to demonstrate its legitimacy. Vague entries, such as "investigation" or "routine patrol" are prohibited.

4. ALPR systems and associated equipment, and databases are the property of OPPD. The use and access of ALPR systems are limited to official law enforcement and public safety purposes. The use of ALPR technology can include, but is not limited to, the following:
    a) Identifying and locating suspects suspected of, or vehicles involved in, criminal offenses, ordinance violations, or traffic violations.
    b) Locating vehicles involved in abducted or missing person cases, including Amber or Silver Alerts,
    c) Identifying vehicles and/or license plates associated with potential witnesses or victims of crime,
    d) Apprehension of suspect(s),
    e) Identifying an unknown suspect involved in a crime, or
    f) Recovering stolen vehicles and license plates.

5. The following uses of ALPR systems are specifically prohibited:
    a) Accessing ALPR systems or data for any personal purpose.
    b) Gathering information solely regarding free speech, political, or religious activity.
    c) Use of ALPR systems or data for enforcement of laws not subject to OPPD jurisdiction, such as tax law or immigration law.
    d) ALPR use based on a person's or group's race, ethnicity, national origin, religion, sexual orientation, gender identity, disability, income level, political viewpoint, lawful association, or exercise of First Amendment rights, or based on location at or near places of worship or religious facilities, or any constitutionally protected activity, except where such information is part of a specific suspect description or otherwise directly relevant to a criminal investigation or public safety matter.
    e) Use of ALPR systems by members not trained in their appropriate use.
    f) Use of another member's login credentials to access the ALPR system.
    g) Integration of artificial intelligence facial recognition technology.

6. When an officer receives an ALPR alarm, they will visually verify that the vehicle license plate number matches the license plate number and state run by the ALPR system. The officer will also verify the current status of the license plate through dispatch or MDT query before initiating the vehicle stop. Officers will be mindful that the driver or passenger(s) may not be the registered owner.

7. Police Dispatch may monitor alarms from ALPR systems and provide information to OPPD personnel.

8. Manual additions can be added to the hotlist with supervisory approval. Members may enter license plate numbers of vehicles for which they have at least a reasonable suspicion of being involved in unlawful activity, or are associated with an endangered person.
    a) When requesting a license plate be entered for a hotlist alert, Members will provide the license plate number, license plate state, vehicle make, vehicle model, vehicle color (if known), the reason or criminal offense for the alert, and the OPPD-related case number.
    b) If the hotlist alert is being entered for an offense that will create a license plate entry into NCIC, the alert duration will be set to one day. If the hotlist alert is being entered for a license plate that will not be entered into NCIC, the alert duration can be set for up to 90 days. If there is a need to continue beyond 90 days, the member will resubmit another manual entry with additional justification. If a hotlist alert is no longer needed, the requesting Member will contact the Police Technology Unit to have the expired alert removed. BOLO alerts require a

supplement report to be created on an OPPD-associated case number to document the alert entry

c) Examples of possible reasons for manual entry of a license plate number include, but are not limited to:
   i) Be On Look Out (BOLO),
   ii) Investigative interest in a vehicle,
   iii) Motorist overdue to a destination,
   iv) AMBER/SILVER Alerts,
   v) Child Abductions, or
   vi) Wanted and/or missing persons.

d) Log files document all current and expired alerts. These hotlists will follow the same auditing and retention procedures as standard reads.

9. The ALPR data may be shared only with other local, state, and federal law enforcement or prosecutorial agencies for official law enforcement purposes in accordance with existing agreements, or as otherwise permitted by law using the following procedures:
   a) The agency makes a written request for the ALPR data that includes:
      i) The name of the agency,
      ii) Agency case number,
      iii) The name of the requestor, and
      iv) The intended purpose of obtaining the information.

10. No ALPR vendor shall be permitted to maintain access to Overland Park ALPR data.

11. Fixed ALPR cameras will not be placed within 100 feet of any place of worship, polling place, or medical facility without the agreement of the owner or operator of the aforesaid location.

C. MAINTENANCE

1. Members of the Technology Unit are assigned to manage and maintain all ALPR equipment. Devices are checked regularly to ensure proper functionality. If department members discover ALPR equipment is not functioning as intended, they should notify a member of the Technology Unit as soon as possible.

D. RETENTION 41.3.9 (D)

1. Automated License Plate Reader data is generally retained for 30 days and may be queried for use in ongoing law enforcement investigations. Data associated with a criminal investigation or civil action may be retained indefinitely within the official case file. Audit trails will be purged no later than two years from the date of its capture, unless a preservation request is made.

E. TRANSPARENCY

1. The Overland Park Police Department will maintain a public-facing Transparency Page that provides information about mobile and fixed-site cameras operated by the Department. The Transparency Page is accessible through the Department's official website.

Origin Date:	04/23/2014	
Revision Date:	01/18/2017	
Revision Date:	01/31/2025	Reviewed by: Captain Richard Breshears
Revision Date:	02/16/2026	Reviewed by: Captain Joshua Taylor
Revision Date:	10/08/2026	Reviewed by: Captain Joshua Taylor