



OAK PARK POLICE DEPARTMENT
GENERAL ORDER



police@oak-park.us

www.oak-park.us/police

708-386-3800

DATE OF ISSUE 01 AUGUST 22	EFFECTIVE DATE 03 AUGUST 22	DISTRIBUTION C	NUMBER 4.68
SUBJECT AUTOMATED LICENSE PLATE READER (ALPR)			
RELATED DIRECTIVES	RE-EVALUATION DATE	ADDENDUM 1	
AMENDS	RESCINDS	NO. PAGES 6	

I. **PURPOSE:**

Automated License Plate Reader (ALPR) technology, also known as License Plate Recognition, provides automated detection of license plates. ALPRs are used by the Oak Park Police Department (OPPD) to convert data associated with vehicle license plates for official law enforcement purposes as defined for purposes of this General Order, including identifying stolen or wanted vehicles, stolen license plates and missing persons.

II. **POLICY:**

The purpose of this policy is to provide Oak Park Police Department personnel with guidelines and principles for the use, collection, access, dissemination, retention and purging of ALPR data to ensure that the information is used for legitimate law enforcement purposes only and to ensure that the privacy, civil rights and civil liberties of individuals are not violated in connection with such ALPR data usage.

III. **DEFINITIONS:**

Automated License Plate Reader (ALPR): Any device that automatically scans the license plates of vehicles and using machine learning, interprets the alphanumeric values on the plate.

Automated License Plate Reader (ALPR) system: A system that includes ALPR hardware and software that processes license plates and other pertinent vehicle identifiers into a data system for searching and retrieval.

Law Enforcement Purposes: The investigation and detection of a crime or violation of law, excluding minor traffic enforcement. Examples include the searches for missing persons or vehicles involved in criminal activity.

Reasonable Suspicion: The standard of proof necessary for a police officer to engage in a temporary investigatory detention of an individual. Must be supported by specific and articulable facts for suspecting a person of criminal conduct.

IV. ADMINISTRATION OF ALPR DATA:

All installation and maintenance of ALPR equipment, as well as ALPR data retention and access shall be managed by the Deputy Chief of Support Services. The Deputy Chief of Support Services will assign personnel under his/her command to administer the day-to-day operation of the ALPR equipment and data.

V. ALPR OPERATION:

Use of an ALPR is restricted to the purposes outlined below. ALPR devices and information contained within the ALPR database will be utilized for official and legitimate law enforcement purposes only. Department personnel shall not use, or allow others to use, the equipment or database records for any unauthorized purpose.

- A. No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.
- B. ALPR data shall only be used as an investigative tool for violent crimes, stolen vehicles and missing or endangered persons. The ALPR may be utilized for other significant felony offenses with a written request approved by the Chief of Police.
- C. An ALPR shall not be used to seek data on any individual or organization based solely on their religious, political, or social views or activities; their participation in a particular non-criminal organization or lawful event; or their race, ethnicity, citizenship, age, disability, gender, gender identity, sexual orientation or other classification protected by law.
- D. An ALPR shall not be used to target any group or individual in a discriminatory manner or infringe on constitutionally protected activities. This shall not preclude the Chief of Police or the system administrator from releasing general information as to the effectiveness of the ALPR equipment and other such communications.

- E. Use of the ALPR system for traffic enforcement and immigration enforcement is prohibited.
- F. All users of the ALPR system will abide by the Oak Park Village Code Reproductive Health Rights Article (13-8-1 through 13-8-6) and Illinois Reproductive Health Act (775 ILCS 55/1-35).
- G. Reasonable suspicion or probable cause is not required before using an ALPR. However, an officer may not detain an individual based on the alert from the ALPR system unless the officer has reasonable suspicion that such person is involved in criminal activity.
- H. Officers shall verify all ALPR activations prior to taking enforcement action. Verification should include the visual inspection of the scanned license plate image regarding the plate letters, numbers and issuing state. The officer should also verify the plate match of the vehicle in question by also comparing the vehicle's make and any other descriptors provided in the ALPR alert. Verification may also be assisted through the use of a query on the vehicle registration via the Illinois Law Enforcement Agencies Data System (LEADS).

Ground-based ALPR installation locations will be determined by the Crime Analysis Unit through multipoint crime analysis of current criminal incidents, historical criminal incidents and high-density violent crime areas. The recommendation of ALPR installation locations must be approved by the Chief of Police. Existing ALPR installations may only be relocated after receiving approval by the Chief of Police after following a similar analysis of criminal incidents near the proposed installation location.

VI. ALPR DATA COLLECTION AND RETENTION:

All data and images gathered by an ALPR are for the official use of the Oak Park Police Department and because such data may contain confidential LEADS information, it is not open to public review. ALPR information gathered and retained by this department may be used and shared with prosecutors or others only as permitted by law.

The database retention period for all data collected by ALPR hardware and stored on the ALPR cloud storage system shall not exceed 30 days. The ALPR system permanently deletes every 30 days on a rolling basis by default. The exceptions are if it is of evidential value in a criminal, civil action or is subject to a lawful action to produce records. In such circumstances, the applicable data should be downloaded from the server onto portable media and booked into evidence. Mass downloading of ALPR data via the ALPR cloud storage system is prohibited.

Collected ALPR data is encrypted and held in an AWS CJIS compliant cloud. Because this cloud is vendor owned, data contained in the ALPR cloud is not subject to request or disclosure under the Illinois Freedom of Information Act. Individual ALPR data records downloaded as part of an active investigation become records of the Department. Individual ALPR records that are downloaded for use in an investigation are subject to Illinois FOIA request similar to all other data and records belonging to the Department. Downloaded records are to be treated as evidence and stored according to Departmental procedures and policy by the ALPR end user. Evidence created through use of ALPR query shall also be included in an officer's/analyst's investigative report.

VII. ACCOUNTABILITY AND SAFEGUARDS

All saved data will be closely safeguarded and protected by both procedural and technological means. The Oak Park Police Department will observe the following safeguards regarding access to and use of stored data:

- A. All non-law enforcement requests for access to stored ALPR data shall be referred to the Records Division Supervisor and processed in accordance with applicable law.
- B. All ALPR data downloaded to the mobile workstation and server shall be accessible only through a login/password-protected system in accordance with the Village of Oak Park computer use policy.
- C. 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 relate to a specific criminal investigation or department-related civil or administrative action.
- D. Such ALPR data may be released to other authorized and verified law enforcement officials and agencies at any time for legitimate law enforcement purposes. Electronic online sharing of Departmental historical ALPR data to external law enforcement agencies, who use a compatible ALPR system, is permissible and will be at the discretion of the Chief of Police. If the external agency request produces investigative leads in other jurisdictions, the Oak Park Police Department will not provide records from those external agencies to the requesting agency. The Oak Park Police Department will then refer the requesting agency to the outside agency where the original records reside.

When practical, and in absence of exigent circumstances, external law enforcement requests should be referred to the Investigations unit or the Records Department for processing and record keeping.

- E. Agency user audit reports will be produced and inspected monthly to ensure compliance with this policy. The system administrator will be responsible for conducting the monthly audit and reporting any discrepancies, problems or misuse to the Chief of Police. The monthly user audit will also contain anonymized user data and transactional data suitable for release on the Department's web-based Transparency Portal.
- F. The Chief of Police will provide the department's stops and any approved felony-related searches in a monthly report to Citizen's Police Oversight Committee (CPOC). In addition to the department's usage, CPOC will be supplied with the name and number of searches conducted by outside agencies.
- G. The monthly report will be an audit of activity for investigative value, policy adherence and disparate impact.
- H. Any Department member found to be in noncompliance with this policy in their use of the ALPR system will immediately have their access suspended to the ALPR system and be subject to the appropriate disciplinary actions. Any non-Departmental personnel found to have gained unauthorized access will be referred to the appropriate authorities for criminal prosecution, as necessary.
- I. If an outside agency is found to be using ALPR data for personal use, immigration enforcement and/or non-law enforcement purposes the department will revoke sharing access.

VIII. TRAINING

- A. The Department will establish end-user training for those employees provided direct access to ALPR data. ALPR system users shall be trained prior to being granted access to the ALPR system(s). Training will include:
 - 1. this policy
 - 2. Village of Oak Park Computer Use Policy
 - 3. proper handling/storage of ALPR downloaded records
 - 4. searching of the ALPR system(s)

5. requirements and process of creating and appropriate uses of ALPR technology
 6. possible penalties for ALPR policy violation.
- B. All ALPR users shall review and sign off on this policy every year.
- C. All ALPR users are required to obtain a LEADS certification every 2 years.

IX. ALPR DATA ACCESS PROCEDURES:

Access to the ALPR system for the purpose of queries will be granted to all Oak Park Police Department officers, dispatchers, and criminal analysts. Use of the ALPR system for queries must be related to an official investigation, personnel complaint, administrative investigation, or criminal investigation. All users that are granted access to the ALPR system will be issued a unique username and password specific to each individual user. The login will require multifactor authentication. The use of another employee's username and password is prohibited. The sharing of an employee's username and password is also prohibited. The use of the ALPR system outside of work devices is prohibited. Employees who separate from the Department or no longer need access to the ALPR system will promptly have access rights removed.

1. Police Officer user accounts will enable search capability across the Oak Park Police Department ALPR network and other agency ALPR networks from law enforcement agencies that have agreed to ALPR data sharing.
2. Detectives and criminal analyst user accounts will match those of Police Officers with the addition of creation and use of Oak Park Police Department Internal Hot Lists.

When conducting investigative queries into an ALPR database, the requestor is required to enter either a case number or a CAD run number with a short description as to why they are initiating the search. This entry will be associated with the search and be visible in the system audit logs. Queries regarding administrative or auditing purposes will be excluded from the requirement to provide a case number.


Shatonya Johnson
Interim Chief of Police