

Automated License Plate Readers (ALPRs)

462.1 PURPOSE AND SCOPE

Automated License Plate Reader (ALPR) technology, also known as License Plate Recognition, provides automated detection of license plates. This Morton Grove Police Department (the "Department") ALPR Policy defines a minimum set of binding guidelines to govern the use of ALPR data, in order to enable the collection and use of such data in a manner consistent with respect for individuals' privacy and civil liberties. ALPRs are used by the Department to convert data associated with vehicle license plates for official law enforcement purposes including but not limited to identifying stolen or wanted vehicles, stolen license plates and missing persons. ALPRs may also be used to gather information related to active warrants, homeland security, electronic surveillance for criminal investigations, suspect interdiction and stolen property recovery.

462.1.2 DEFINITIONS

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

ALPR: Automated License Plate Reader/License Plate Reader

Hit: A read matched to a license plate that has previously been registered on the Department's "hot list" of vehicle plates or on the local "hot list" on the LPR's computer that has been added by a user.

Hot List: License plate numbers of stolen vehicles, wanted subjects, missing persons, AMBER alerts, suspended, revoked, or expired registration, parking scofflaws, or any other criteria as determined by the Deputy Chief of Field and Support Services. Hot list information can come from a variety of sources including but not limited to: the National Crime Information Center (NCIC), Law Enforcement Agencies Data System (LEADS), and Illinois Secretary of State. Officers may also manually add license plates to a local "hot list" based on information relayed to them regarding a law enforcement or public safety concern.

Read: The capture of digital images or license plates and vehicles with associated metadata (date, time, GPS coordinates with vehicle image capture).

462.2 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 Field and Support Services. The Deputy Chief of Field and Support Services will assign personnel under his/her command to administer the day-to-day operation of the ALPR equipment and data.

462.3 ALPR OPERATION

Use of an ALPR is restricted to the purposes outlined below. 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 being Law Enforcement Agencies Data System (LEADS) trained and first completing Department-approved training.
 - (b) An ALPR shall only be used for official and legitimate law enforcement business.
 - (c) An ALPR may be used in conjunction with a legitimate police operation, official Department investigation and for training to ensure the proficiency of all ALPR operators. Reasonable suspicion or probable cause is not required before using an ALPR.
 - (d) The Investigations Commander will be responsible for ensuring that the “hot files” are downloaded from the Illinois State Police System.
 - (e) The ability to access the database and conduct inquiries will be provided to all sworn personnel and those civilians with a need for access. Access shall be accessible only through a login/password protected system.
 - (f) An ALPR may be used to canvass license plates during criminal investigations of any crime. Partial license plates and vehicle descriptions reported during crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.
 - (g) An ALPR may be used to support local, state, federal and tribal public safety departments in the identification of vehicles associated with criminal investigations.
 - (h) Any search through the ALPR database should include a case number or detailed description of the reason for the search.
 - (i) Department managed Hot Lists should include a case number if applicable, an explanation as to the reason for being on the hotlist, and specific instructions on the expected enforcement action if applicable.
 - (j) If practicable, the officer should verify an ALPR hit through the Illinois Law Enforcement Agencies Data System (LEADS) before taking enforcement action that is based solely upon an ALPR hit.
 - (k) ALPR will not be used in order to determine someone's immigration status or for immigration enforcement purposes.
 - (l) ALPR will not be used in order to deny or interfere with a person's right to choose or obtain reproductive health care services or any lawful healthcare services as defined by the Lawful Health Care Activity Act.
 - (m) Department members shall not share ALPR information with an out-of-state law enforcement agency without first obtaining a written declaration from the out-of-state law enforcement agency that it expressly affirms that ALPR information obtained shall not be used in a manner that violates subsection (b) of 625 ILCS 5/2-130.
 - (n) ALPR units may not be used for the sole purpose of monitoring individual activities protected by the First Amendment to the United States Constitution.
-

- (o) Patrol Supervisors, Patrol Officers, Investigations Bureau personnel, and Desk personnel should log in to the ALPR system as soon as practicable after the start of their shift. They should remain logged in for the duration of their shift to actively monitor alerts in real time.

462.4 ALPR DATA COLLECTION AND RETENTION

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

The Deputy Chief of Field and Support Services or designee is responsible to ensure proper collection and retention of ALPR data. Data and images will be automatically purged on a rolling 30-day schedule, except for specific data downloaded and retained in connection with a legitimate police operation or official law enforcement investigation.

All ALPR data downloaded should be stored for the minimum period established by the Department's record retention guidelines and thereafter may be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a lawful action to produce records. In such circumstances, the applicable data shall be downloaded onto portable media and inventoried into evidence.

ALPR camera placement shall be approved by the Chief of Police and every effort will be made to ensure such placement captures roadway images and not movement into or out of a sensitive location where privacy would be expected.

462.5 ACCOUNTABILITY AND SAFEGUARDS

All saved data will be closely safeguarded and protected by both procedural and technological means. The 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 Supervisor and processed in accordance with applicable law.
- (b) All ALPR data shall be accessible only through a login/password protected system capable of documenting all access of information by name, date and time.
- (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) ALPR system audits should be conducted on an annual basis.

462.6 AUDIT

Access to, and use of, ALPR data is logged for audit purposes. Audit reports will be structured in a format that is understandable and useful and will contain, at a minimum:

- (a) The name of the law enforcement user;
- (b) The date and time of access;
- (c) The specific data accessed;
- (d) The supplied authorized law enforcement or public safety justification for access; and
- (e) A case number associated with the investigative effort generating the ALPR data query.

Audit reports will be provided monthly and on request to the Department's supervisory personnel.

Every month, the Department will audit a sampling of ALPR system utilization from the prior month to verify proper use in accordance with the above authorized uses. Any discovered intentional misconduct will lead to further investigation and termination of system access. In addition, the auditing data will be used to identify systemic issues, inadvertent misuse, requirements for policy changes, training enhancements, or additional oversight mechanisms.

These ALPR audits shall be conducted by a supervisor other than the person assigned to manage the Department's ALPR function. Audit results shall then be reported to the Chief of Police.
