Automated License Plate Readers (ALPRs)

434.1 PURPOSE AND SCOPE

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

434.2 POLICY

The policy of the Darien Police Department is to properly utilize ALPR data and images for law enforcement purposes while recognizing the established privacy rights of the public. ALPR technology is used by the Darien Police Department to convert data associated with vehicle license plates for official law enforcement purposes.

434.3 LAW

The Illinois State Law, 625 ILCS 5/2-130, places restrictions on the use of ALPRs, to include

- LPR data storage limitations
- LPR data may not be shared with any jurisdiction to investigate or enforce a law that interferes with a person's right to reproductive or lawful healthcare.
- LPR data may not be provided to out-of-state agencies that may use it for immigration enforcement.
- LPR information is held confidentially to the fullest extent permitted by law.
- LPR data may not be used to target any individual or group based on race, religion, sex, or any other protected class.
- LPR data may not be used for Immigration Enforcement.

The Illinois State Law, 5 ILCS 140/7(1)(d-7) restricts the release of data and images from disclosure. However, if an image is exported and incorporated as evidence of an investigation, the data and images may be subject to the Freedom of Information Act (FOIA). Data and images gathered by the ALPR system are for the official use of law enforcement. Because such data may contain confidential information, it is not open to public review.

434.4 DEFINITIONS

The ALPR technology, also known as license plate recognition (LPR), allows for the automated detection of license plates. ALPR cameras can be fixed or mobile.

434.5 ADMINISTRATION

The Deputy Chief of Operations has the responsibility to manage the installation and maintenance of ALPR system. The Deputy Chief of Operations has the responsibility for data retention and access. The Deputy Chief of Operations may assign personnel under his/her command to administer the day-to-day operation of the ALPR system and data.

The Deputy Chief of Operations is responsible for ensuring systems and processes are

in place for the proper collection and retention of ALPR data.

434.6 OPERATION

Department members shall only use, or allow other law enforcement agencies to use, ALPR equipment or database records for any authorized patrol operation or criminal investigation.

The ALPR system is further restricted as outlined below. Members shall:

1. Follow statutory law and legal precedent (see order 4.3.4).
2. Not conduct repeated historical ALPR searches or use ALPR data to identify anticipated locations, routes, schedules, or times of travel for the purpose of locating or apprehending a person solely because the person is believed to have a suspended, revoked, cancelled, or otherwise invalid driver's license, vehicle registration, or license plate registration, or any petty traffic offense.
3. Not operate ALPR equipment or access ALPR data whether departmental, other local, state or federal ALPR system without first completing department approved training.
4. When practicable, verify an ALPR response through the appropriate law enforcement agency before taking enforcement action that is based solely upon an ALPR alert.
5. Not use images gathered through ALPR in conjunction with facial recognition software for purposes other than for the investigation of a felony crime.
6. Not honor requests for ALPR data and/or images by nonlaw enforcement or non-prosecutorial agencies.
7. Enter a valid Darien case number or call for service number associated with the incident in every ALPR search, including searches of other agencies' ALPR systems. Members assigned to a task force may use their assigned agency's case number.
8. Not access ALPR systems or data on any personally owned device, including a personal cell phone, tablet, or computer. ALPR systems shall be accessed only on department-issued devices.

434.7 DATA COLLECTION AND RETENTION

ALPR data shall be retained for seven days, unless the data and / or images are downloaded and saved as digital evidence. Thereafter, ALPR data should 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 discovery request or other lawful action to produce records. In those circumstances the applicable data should be downloaded onto portable media and booked into evidence.

Automated License Plate Readers (ALPRs)

434.8 ACCOUNTABILITY

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

1. ALPR data downloaded to and stored in a mobile workstation shall be accessible following established Criminal Justice Information Services (CJIS) policy and procedures.
2. Members 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.
3. ALPR system audits should be conducted monthly by the DC of operations or designee.

434.9 RELEASING ALPR DATA

The ALPR data may only be shared with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law using the following procedures:

1. The agency makes an electronic request for the ALPR data.
2. The request is reviewed by the DC of Operations or the authorized designee and approved before the request is fulfilled.

The software setting permitting out-of-state agencies access to the Darien ALPR data and images is turned off. If an out-of-state law enforcement agency requests assistance with ALPR data the member shall follow the rules established in 434.6.