

DARIEN POLICE DEPARTMENT

Community Information Bulletin

Serving and Protecting the City of Darien, Illinois



Frequently Asked Questions

Automated License Plate Reader (ALPR) Program

Department Message

The Darien Police Department is committed to using technology responsibly, transparently, and in a manner that maintains the trust of every resident we serve. This page exists, along with our Transparency Portal, because the department is committed to transparency, which is essential to community trust and effective law enforcement.

Transparency Portal - (<https://transparency.flocksafety.com/darien-il-pd>),

This page will be updated as new information becomes available. If you have a question not answered here, we encourage you to contact the Police Department directly.

Frequently Asked Questions

Q: What Is an Automated License Plate Reader?

A: An Automated License Plate Reader (ALPR) is a camera system mounted at fixed locations on public roadways. As vehicles pass the camera, the system automatically captures an image of the license plate and records the plate number, along with the vehicle's make, model, color, direction of travel, and the date and time of the observation.

Q: When were ALPR's first installed?

A: The Darien Police Department began using ALPR technology in July 2024. Cameras are mounted at key entry and exit points of the city. Darien contracts with Flock Safety for all of Darien's ALPR cameras.

Q: Are these cameras red-light cameras?

A: No. ALPR cameras are not traffic enforcement cameras. They do not issue tickets, monitor speed, or enforce traffic signals.

Q: Is the Department watching me in real time?

A: No. The system does not have live monitoring. It is queried only when officers have a specific, documented law enforcement purpose, and only provides an image of the description of the vehicle that was searched.

Q: Does the system track where I go?

A: The system records when a vehicle passes a fixed camera location. It does not follow vehicles, track GPS location, or provide continuous monitoring. A vehicle that regularly passes a camera will have a record of those observations within the 7-day retention window.

Q: Can the camera identify me by my face?

A: No. ALPR cameras capture only what is already visible to any person on a public street. They do not record audio, use facial recognition, or identify the driver or passengers in a vehicle.

Q: How long is my data kept?

A: All ALPR records are automatically deleted after 7 days unless a specific record is relevant to an active criminal investigation, in which case it may be retained as evidence consistent with that investigation's requirements.

Q: Does a warrant need to be obtained to search the database?

A: No. Under current Illinois and federal law, a warrant is not required. License plates are required by law to be publicly visible and carry no recognized expectation of privacy on a public road.

Q: Who can search the ALPR database?

A: Access is limited to trained, authorized law enforcement personnel. Unauthorized access is subject to disciplinary action and potential criminal prosecution.

Q: Can immigration enforcement agencies access Darien's data?

A: No. Illinois law under 625 ILCS 5/2-130 prohibits sharing ALPR data with agencies that may use it for immigration enforcement. Darien does not authorize access to its data by federal immigration agencies or any out-of-state law enforcement.

Q: Was Darien involved in the data sharing violations identified in the 2025 Secretary of State audit?

A: No. Darien was not among the agencies identified in the Secretary of State's 2025 audit.

Q: Are the ALPR system and the in-car cameras (Axon Fleet) integrated?

A: No. These systems do not communicate with each other. ALPR data must be manually retrieved by authorized personnel and separately transferred into the department's digital evidence storage software. There is no automated exchange of data between the two systems.

Q: Does Darien review or audit the searches that outside agencies run against its data?

A: Darien does not receive the underlying case details, such as the reporting officer's name, report number, or stated reason, when another agency searches Darien's ALPR data through the network. If a specific search appears improper, the Department can raise it directly with that agency's leadership. Each participating agency, including Darien, is responsible for auditing its own personnel's use of the network consistent with its own policies and applicable law. Darien's own safeguards for its personnel are described below.

Q: Does Darien charge other agencies to search its ALPR data, or is Darien charged to search other agencies' cameras?

A: No. There is no cost-sharing arrangement for network access. Outside agencies are not invoiced when they search Darien's ALPR data, and Darien is not charged when its officers search other participating agencies' cameras while investigating matters such as a missing person, a stolen vehicle, or a vehicle involved in a crime.

Q: What safeguards has Darien put in place to prevent misuse of the system?

A: In addition to the system's standard security features, Darien requires multi-factor authentication for access, requires that every search be linked to a documented case number, uses automated tools that flag irregular search activity, and has a supervisor who reviews search audit logs. Suspected misuse is investigated and can result in discipline.

Q: What ensures ALPR use doesn't disproportionately affect any racial or demographic group?

A: The ALPR system itself does not record or determine a person's race, ethnicity, or any other demographic information; it identifies vehicles, not people. Separately, Illinois law (625 ILCS 5/11-212, the Traffic and Pedestrian Stop Statistical Study Act) requires every Illinois law enforcement agency, including Darien, to record the perceived race of a driver on every traffic stop, regardless of how the stop originated, and the Illinois Department of Transportation compiles this into an annual, publicly available statewide report. This requirement applies to all traffic stops and is not specific to ALPR.

Q: The Transparency Portal shows 30 days of activity, such as vehicles detected and searches performed, but the FAQ says data is deleted after 7 days. How can both be true?

A: The 30-day figures on the Transparency Portal are aggregate statistics, for example the total number of vehicles captured or searches performed. They are not individual, searchable vehicle records. The underlying record for a specific plate, image, date, time, and camera location is deleted after 7 days unless it becomes evidence in an active investigation, in which case it is retained consistent with that investigation's evidence requirements.

Q: Is the information on the Transparency Portal provided directly by Darien, or by Flock?

A: The Transparency Portal is built and maintained by Flock, populated with Darien's actual account data and configuration. General statements about how the technology works are Flock's representations about its product.

Q: Was Darien's ALPR system searched in connection with a request from the U.S. Department of Homeland Security (DHS)?

A: The Department investigated a specific incident in which a DPD member accessed ALPR data after being contacted by the U.S. Department of Homeland Security (DHS). The review determined that the search was conducted in compliance with Department policy and Illinois law restricting ALPR use (625 ILCS 5/2-130).

The review also confirmed that the search was related to an active investigation being conducted by a DHS agency other than U.S. Immigration and Customs Enforcement (ICE). It is important to note that DHS is a large federal department made up of more than 20 component agencies with a broad range of missions, many of which are unrelated to immigration enforcement.

Q: Does Flock sell or share Darien's ALPR data with third parties?

A: No. Per the agreement, data captured by Darien's cameras is owned by Darien and shared only as Darien directs. The policy states that Flock does not rent, sell, or otherwise distribute this information to third parties.

Q: Does the system store any individual data such as name and address of the registered owner of the vehicle or license plate?

A: Flock's privacy policy states that camera footage is not linked to a verified individual identity, so the company cannot confirm whose license plate appears in an image.

Q: Does the Flock use images captured by Darien's cameras to train its own AI or software systems?

A: Yes, in a limited way. The Flock's policy states that less than 1% of images captured across its systems may be used, after being stripped of metadata and identifying information, to improve how its software recognizes vehicles. The policy states these training images are never sold or shared with third parties and are kept separate from identifiable data.

Q: What security standards does Flock say it follows for law enforcement data?

A: The Flock's policy references compliance with the FBI's CJIS Security Addendum, which governs how criminal justice information must be handled, along with multi-factor authentication and password safeguards on user accounts.

Q: Is data captured by Darien's cameras ever processed or stored outside the United States?

A: According to Flock's policy, the company is U.S.-headquartered and processes data within the U.S. by default; any transfer outside the U.S. requires explicit consent from the account holder, which would not apply to Darien's data absent such a request.

Q: Does Flock's own policy confirm that searches must be justified and logged?

A: Yes. The Flock's policy states that any license plate search by authorized law enforcement requires justification to verify the legitimacy of the search and creates an audit trail, consistent with Darien's own case-number and audit requirements described above.