

	DARIEN POLICE DEPARTMENT POLICY AND PROCEDURE GENERAL ORDER	Distribution:	General Order Number:
		ALL PERSONNEL	5.34
		Original Issue Date:	Reissue/Effective Date:
		10/15/2024	09/15/2026
Order Title: AUTOMATED LICENSE PLATE READERS		Accreditation Standard:	Section:
			5
		Section Title: DEPARTMENT ROLE AND AUTHORITY	
Rescinds: 04/17/2026	Jeremiah P. Marron Jr., Chief of Police		

This General Order is for departmental use only and does not apply in any criminal or civil proceeding. This General Order should not be construed as creation of a higher legal standard of safety or care in an evidentiary sense with respect to third party claims. Violations of this General Order will only form the basis for departmental administrative sanctions. Violations of law will form the basis for civil and criminal sanctions in a recognized judicial setting

I. PURPOSE

The purpose of this General Order is to provide Department personnel with guidance on the application and use of automated license plate readers (ALPRs), management of ALPR data, and maintenance of ALPR equipment in compliance with Connecticut law.

II. POLICY

It is the policy of the Darien Police Department ("Department") to utilize Automated License Plate Recognition (ALPR) technology to capture and store digital license plate data and images only for purposes authorized by Connecticut state law and this General Order.

The Department recognizes the privacy rights of the public and the potential sensitivity of ALPR data. All data and images gathered by an ALPR system are for official Department use only. Automated license plate reader data is confidential and is not a public record for purposes of the Connecticut Freedom of Information Act, except to the extent that state law provides for disclosure of camera locations and redacted audit, usage, and access-log data.

The placement of ALPR equipment shall be determined by crime analysis, operational need, and applicable legal restrictions, in consultation with the Chief of Police or designee and the vendor providing the ALPR service and shall be law enforcement sensitive. The Chief of Police shall have the authority for placement of the ALPR equipment.

The ALPR technology allows for the automated detection of license plates along with vehicle descriptors such as make, model, color, and other unique identifying characteristics through the Department's ALPR system and the vendor's vehicle identification technology.

The Department may use ALPR technology to compare license plate and vehicle descriptor data against approved hot lists and criminal justice databases, and to support active criminal investigations supported by reasonable suspicion, apprehension of persons with outstanding warrants, location of missing or endangered persons, and recovery of stolen motor vehicles.

The Department shall not use ALPR technology for personal purposes, for reasons unrelated to an authorized law-enforcement or public-safety purpose, or in any manner prohibited by Connecticut state law or this General Order.

Consistent with this philosophy, it is the policy of the Darien Police Department to authorize the use of Department-owned, maintained, or issued ALPR systems only by trained and authorized personnel.

III. DEFINITIONS

Alert: A visual and/or auditory notification that activates when an ALPR system detects a hit.

Automated License Plate Reader (ALPR): License plate recognition (“LPR”) technology. A mobile or fixed electronic image recording device that is capable, in combination with computer programs or algorithms, of converting images of license plates or vehicle descriptors into computer-readable data. The term does not include an image recording device used as part of an automated traffic enforcement safety device, a work zone speed control system, or a municipal school bus violation enforcement system.

ALPR Administrator: The Chief of Police or designee(s) who serves as the ALPR Administrator(s) for the Department.

ALPR Data: Any data captured, recorded, held, stored, processed, or derived from an automated license plate reader system, including scan files, alert data, license plate characters, vehicle still or video images, vehicle attributes, location data, timestamps, metadata, and any related documents or data generated by, or obtained through use of an ALPR system.

ALPR Data Query Logs: A record of a search or query of ALPR data from the server or other system of record.

ALPR Operator: A trained Department authorized user who is authorized to use ALPR system equipment or data. ALPR operators may be assigned to any position within the Department, and the ALPR Administrator may order the deployment of ALPR systems for authorized purposes.

Authorized User: Department personnel designated by the Chief of Police, who after receiving proper training, have access to ALPR data, query logs and other ALPR information as determined by the Chief of Police.

Axon Fleet 3 Camera: A vehicle mounted camera that functions as a dashboard camera and has AI capabilities including ALPR capabilities, when enabled.

Connecticut Online Law Enforcement Telecommunications System (COLLECT): The State of Connecticut's version of NCIC.

Fixed Camera: A camera that is permanently affixed to a structure, such as a pole, bridge, overhead fixture, or other fixed location.

Global Positioning System (GPS): Satellite-based navigation system providing precise location and time data worldwide.

Hit: An alert from the ALPR system that a scanned license plate number or vehicle descriptor matches a record in an approved hotlist or criminal justice database, including but not limited to NCIC, CJIS, and other approved sources.

Hot List: A list of license plate numbers and other vehicle description manually entered into a local ALPR system database that are relevant and material to a criminal investigation or a missing or endangered person.

Internal Hotlist Addendum: A hotlist maintained for use only at a specific state facility or facilities for documented threats to persons, facilities, or agency operations, and not based solely on constitutionally protected speech, conduct, or association.

License (Registration) Plate: A metal or plastic plate attached to a vehicle for official identification purposes, that displays a registration number or alphanumeric code to identify the vehicle. The code can be unique to the entire country, a state or province.

Mobile ALPR: An automated license plate reader affixed to a police vehicle. See Axon Fleet 3 definition above.

Mobile Camera: A camera affixed to a vehicle either permanently or by magnet mount.

MOU: Memorandum of understanding

National Crime Information Center (NCIC): A computer system controlled and operated by the Federal Bureau of Investigation in Washington, DC, that gives law enforcement agencies access to information on warrants, criminal histories, stolen property, and missing persons statewide and nationwide.

Optical Character Recognition (OCR): Technology that converts text from images into a machine-readable format.

Portable Camera: A camera that is stationary when deployed, but is capable of being moved as needed, such as equipment mounted to a temporary structure, traffic barrel or similar device.

Standard Operating Procedure (SOP): A written document that outlines a series of instructions and protocols for performing tasks. SOPs can help to reduce miscommunication and ensure compliance with industry regulations.

Vehicle of Interest: Including, but not limited to, a vehicle that is reported as stolen; displays stolen license plates; is linked to missing and/or wanted persons, or otherwise lawfully associated with an approved alert, hotlist, warrant, or criminal investigation.

IV. PROCEDURE

A. ALPR Administration

1. The Department has designated sworn supervisors and the Public Safety IT Professional to have administrative oversight of the ALPR system, acting as system administrators, and they shall be responsible for compliance with the following:
 - a. Ensuring the ALPR system is used solely for proper Department business and in compliance with this General Order, local regulations, town ordinances, and state and federal laws.
 - b. Ensuring that ALPR systems and ALPR data are used solely for purposes authorized by this policy and Connecticut law.
 - c. Ensuring that only properly trained Department personnel and approved staff are allowed access to the ALPR system or to collect ALPR information.
 - d. Issuing login credentials for authorized users.
 - e. Ensuring that training requirements are completed for authorized users.
 - f. Monitoring the ALPR system to ensure the security of the information and compliance with applicable privacy laws.
 - g. Monitoring the ALPR system to ensure it operates according to specifications and reporting software or hardware failures to the vendor for repair.
 - h. Maintaining the title and name of the current designee overseeing the ALPR operation.
 - i. Ensuring compliance with statutory retention limits, including the default twenty-one (21) day retention cap, and documenting and supervising all approved retention beyond that period.
 - j. Ensuring this General Order, related policies and procedures, and required transparency information are conspicuously posted on the Department's website.
 - k. Reviewing any request for data sharing from an external law enforcement agency for compliance with Connecticut law, including written declaration requirements, warrant requirements where applicable, and restrictions on real-time, bulk, or automatic access.

- l. Performing a quarterly audit of the Department's ALPR system to verify compliance with this General Order and other applicable policies. Audits shall include review of system use, query logs, hotlist entries, access logs, retention decisions, and data-sharing activity.
- m. Reporting any violations of this General Order through the chain of command to the Chief of Police.
- n. Providing recommendations to the Chief of Police regarding any necessary updates.
- o. Ensuring annual ALPR usage reporting and website publication in the form and manner required by Connecticut law and implementing guidance.

B. General ALPR Use

1. ALPRs will be used only by personnel who have been properly trained in the use of the ALPR system and software.
2. ALPR data may be accessed by Department authorized users only for purposes expressly authorized by Connecticut law and this General Order.
3. ALPR data may be accessed by authorized staff only for purposes expressly authorized by Connecticut law and this General Order.
4. The Field Services Bureau Captain is responsible for receiving reports of ALPR defects, damage, or other matters requiring maintenance of the Department's ALPR systems. The Field Services Bureau Captain is responsible for the inventory of the Department's ALPRs.
5. The Detective Division Lieutenant and the Public Safety IT Professional are responsible for the maintenance of data, including backing up of ALPR data, requests for searches or ALPR data, and for maintenance of internal hot lists.
6. The Field Services Bureau Captain is responsible for the inventory of ALPRs within the Department.
7. ALPR hot lists and data gathered by Departmental ALPR systems will be maintained securely. Requests for searches may be made by personnel of this Department or by other law enforcement agencies subject to the provisions of this General Order.
8. Prior to the use of the ALPR system equipment, personnel must receive training administered by the aforementioned personnel and/or the Public Safety IT

Professional. Changes in hardware, software, policy, or law shall be addressed through updated training, bulletins, or in-service instruction.

C. Permissible Uses

1. The use of ALPR technology, associated equipment, and databases by law enforcement is authorized only for official public-safety purposes expressly authorized by Connecticut law and this General Order.
2. Dissemination: All requests for ALPR use, data or software access shall be reviewed by the aforementioned personnel and/or Administrative Services Bureau Captain.
3. Roles and Permissions: The following roles are maintained in the ALPR software with permissions that can be adjusted as necessary:
 - a. Administrator
 - b. Supervisor/Detective
 - c. Patrol
4. The Department may operate an ALPR system or use ALPR data only for the following law enforcement purposes:
 - a. Comparing ALPR data with approved hot lists, COLLECT, CJIS, the FBI Kidnapping and Missing Persons list, the Federal Terrorist Screening Database, NCIC, and the National Center for Missing and Exploited Children database.
 - b. Entering or querying a license plate where an officer determines that the data may be relevant and material to a specific active criminal investigation supported by reasonable suspicion.
 - c. Assisting in the apprehension of an individual with an outstanding warrant.
 - d. Assisting in locating a missing or endangered individual.
 - e. Assisting in recovering a stolen motor vehicle.
5. Use of Hot lists:
 - a. Hot list information may come from approved criminal justice databases and lawfully issued alerts, including NCIC, CJIS, AMBER Alerts,

SILVER Alerts, missing-person databases, and other lawfully authorized sources.

- b. Authorized users may manually add license plate numbers to hot lists only for a lawful purpose consistent with this policy and only with supervisory approval.
- c. Adding a vehicle or license plate to a hot list in connection with a crime requires reasonable suspicion.
- d. Manual hot list entries shall include the offense or reason for the entry, vehicle description, requesting officer, case number or incident number, the date entered, and an expiration date.
- e. Manual hot list entries shall be validated, time-limited, and removed upon expiration or once the basis for the entry no longer exists.
- f. Personnel using ALPR shall ensure the most current hot list data available is uploaded.
- g. When the ALPR indicates a hit from a hot list, prior to initiating any stop, personnel shall verify that the captured plate image matches the plate number and issuing state of the vehicle. A hit from the hot list, standing alone, is not probable cause to make an arrest
- h. Hot list categories should be limited to categories that correspond to authorized statutory purposes, such as missing or endangered persons, stolen vehicles, stolen license plates, wanted persons with warrants, threat-related alerts, and vehicles relevant to specific criminal investigations supported by reasonable suspicion.

6. ALPR Queries:

- a. Queries may be made to the ALPR system only for a permitted purpose.
- b. The user must log in with personal credentials specific to that user.
- c. Before submitting a query, the user shall enter: (1) the query parameters; (2) the reason for the query and offense type, if any; and (3) the associated case number, or other identifying incident number.
- d. ALPR system queries shall focus on purposes authorized by law and this General Order.

7. ALPR Hot list Creation:

- a. Before creating a hot list entry, the user must obtain approval from a supervisor.
- b. Verification of the license plate shall be queried via CJIS, NCIC, or other approved sources to ensure that the entry is accurate.
- c. Manual entries should include specific descriptors for vehicles being sought for authorized purposes, when available.

8. ALPR Data Sharing and Dissemination:

- a. ALPR data is For Official Use Only and shall be shared only as authorized by Connecticut state law. The Department will abide by the terms of this General Order, the requesting agency agrees not to use its ALPR data in violation of Connecticut state law, including but not limited to, C.G.S. §54-192h (the Connecticut Trust Act) and C.G.S. §54-155b.
- b. The Department may share ALPR data with a Connecticut public agency when the request is documented, case-specific where applicable, and for a purpose authorized by law.
- c. The Department may share ALPR data with a law enforcement agency of New York, Rhode Island, or Massachusetts, a municipality of those states, or a qualifying multijurisdictional task force only after receiving a written declaration affirming that the data will be used in compliance with Connecticut state law, will not be used for immigration enforcement or to investigate or prosecute any person for reproductive health care or gender-affirming care that is lawful in Connecticut, and will not be further disclosed except as permitted by Connecticut state law. See C.G.S. §52-571m.
- d. The Department may share ALPR data with any other out-of-state or federal law enforcement agency only when that agency presents a judicially issued probable-cause warrant for the specific data requested, or requests specific data concerning a possible match in the Federal Terrorist Screening Database.
- e. The Department shall not participate in an ALPR data-sharing network unless each participating agency executes the declaration required by Connecticut state law.
- f. The Department shall not provide real-time, bulk, or automatic access to ALPR data except in response to a documented, case-specific request that is otherwise lawful.

- g. Information sharing between law enforcement agencies shall be guided by this General Order, applicable law, and any departmental policies, procedures, or memoranda of understanding.

D. Operations

1. Prior to a tour of duty, authorized users using an ALPR shall ensure that the daily upload of current hot list data has been performed.
2. Data from field ALPRs, whether mobile or portable, will be uploaded to the Department's approved vendor platform in accordance with Department procedures and retention requirements.
3. When enforcement action, an investigation, or prosecution results from an ALPR hit, the hit will be preserved and documented in an incident report, if applicable.
4. ALPRs may be used in special operations or details such as high-crime area patrols, DWI initiatives, enforcement details, and directed criminal investigations, subject to authorization and only for purposes authorized by this General Order.
5. When violent crimes occur, the Department may solicit assistance from other agencies with ALPR-equipped vehicles to assist in identifying a vehicle or gathering license plate data in a particular area, subject to this General Order and applicable law.

E. ALPR Data

1. Authorized users may request that certain license plate numbers, whether complete or partial, be entered into the Department's hot list only when the request is tied to an authorized purpose and approved in accordance with this General Order.
2. Access to ALPR data shall be limited to authorized users who have been properly trained and authorized.
3. Authorized users making inquiries must make a log entry in the ALPR Query Log.
4. If the ALPR Query Log contains a hit associated with an arrest, the relevant log entry must be retained as part of the case file.
5. ALPR Data Query Logs shall be maintained and secured for future audits.

6. Access to ALPR data must be for a purpose authorized by Connecticut state law and this General Order.
7. Authorized users or staff conducting a query on behalf of an authorized requestor shall make a log entry.
8. Requests to review stored ALPR data and search results shall be recorded and maintained in appropriate case files.
9. ALPR data from all mobile, portable, and fixed ALPRs shall be managed by the designated Lieutenant or other custodian assigned by the Chief of Police.
10. ALPR data shall be stored only in accordance with the retention limits and exceptions set forth in this General Order and Connecticut state law.
11. Backup of the ALPR data system shall be in accordance with municipal data-backup requirements and vendor security standards, provided backups remain subject to all statutory retention and deletion rules.

F. Field Protocols

1. ALPRs are useful in general patrol assignments when the patrol vehicle is in a position to monitor vehicular traffic, but ALPRs may only be used for a purpose authorized by this General Order and law.
2. Authorized users may not use a mobile ALPR unless properly trained in its use and operational protocols. See Section Q of this General Order.
3. ALPR-equipped vehicles should be used as often as operationally appropriate. When not in use, ALPR-equipped vehicles should be secured. See Section Q.
4. Authorized users will ensure that a daily upload of hotlist data has been performed so as to reduce the risk of action based on outdated data.
5. When the ALPR indicates a hit, prior to making a stop, the authorized user must:
 - a. Verify that the captured plate image matches the plate number of the vehicle.
 - b. Confirm the hit through dispatch, CJIS, NCIC, RMS, or another appropriate source when circumstances permit or as soon as practicable.
6. Proactive entry of data or access to ALPR records must be for a purpose authorized by this policy and by authorized personnel.

7. Proactive or manual field entry of an ALPR hotlist is permitted for dispatch reports of crimes, BOLOs, alerts, and other authorized law-enforcement purposes when directed or authorized by a supervisor.
8. Proactive or manual entry of an ALPR hotlist in the field is required for AMBER Alert or Missing Child Alert bulletins when a plate number is part of the alert, and authorized users shall query the system to determine whether there is a prior read of the relevant vehicle.
9. Authorized users will make an entry in their incident report whenever the ALPR is used.
10. A traffic stop initiated based on an alert from the ALPR system must be for one of the permitted purposes listed in this policy. Unless exigent circumstances exist, officers shall verify the alert and confirm status through appropriate databases before conducting a stop, or develop independent reasonable suspicion.

G. Investigative Protocols

1. Access to stored ALPR data shall be limited to authorized personnel and supervisors for purposes authorized by this General Order and Connecticut state law.
2. Authorized users conducting ALPR data inquiries must have been granted access by the ALPR Administrator, or a supervisor.
3. Requests to review stored ALPR data shall be recorded and maintained in the same manner as criminal history logs or in another approved auditable format.
4. All inquiries of ALPR data will be recorded by the authorized user making the inquiry in the ALPR Data Query Log.
5. ALPR Data Query logs, audit logs, and access logs shall be retained in accordance with Department records-retention rules and applicable law and shall be sufficient to facilitate quarterly audits and required public disclosure of redacted audit information.

H. Data Retention

1. Except as otherwise provided by law, ALPR data collected, acquired, held, or stored by the Department or its contracted vendor shall not be retained for more than twenty-one (21) days.
2. ALPR data may be retained beyond twenty-one (21) days only when:

- a. Required by a warrant or court order, or by court rules governing preservation of evidence.
 - b. Retained as evidence in an active criminal investigation or prosecution, with supervisory approval and documented purpose and case number.
 - c. Retained in de-identified, aggregated, or summarized form for traffic analytics where permitted by law.
 - d. Otherwise retained pursuant to a specific statutory exception.
- 3. If ALPR data is retained as evidence in an active criminal investigation or prosecution, the data shall be deleted upon conclusion of the investigation if no charges are filed; upon final disposition if charges are filed and no defendant receives a term of imprisonment; or upon release of the last incarcerated defendant if imprisonment is imposed, unless otherwise required by court order or law.
 - 4. Any retention beyond twenty-one (21) days shall be approved by a supervisor and documented with the purpose of retention, approving supervisor, date of approval, and associated incident number.

I. Prohibited Uses

- 1. The use of ALPR technology is restricted to approved law-enforcement purposes as outlined in this policy. Use of ALPR technology for personal or other non-official purposes is a violation of this General Order.
- 2. License plate reader technology shall not be used for investigatory purposes when the request for identification is based solely upon:
 - a. Religious, political, or social views or activities.
 - b. Participation in a non-criminal organization or lawful event.
 - c. Activity protected by the First Amendment.
- 3. ALPR data shall not be used to monitor or investigate any individual based on that individual's actual or perceived race, ethnicity, sexual orientation, gender identity or expression, sex, pregnancy status, disability, citizenship, nationality, income level, or perceived criminal history, except where a prior conviction is an element of a specific criminal offense under investigation.
- 4. ALPR data may not be queried or used in connection with suspected immigration violations or to assist in civil or criminal immigration enforcement

activity, except as otherwise required by Connecticut state law. See C.G.S. §54-192h(b)(1)(A)(i), (ii) or (iii).

5. ALPR data may not be queried or used in connection with any investigation or prosecution of any individual who has sought, received, provided, or assisted another in obtaining reproductive health care services or gender-affirming health care services that are lawful in Connecticut.
6. The following uses are strictly prohibited:
 - a. Invasion of Privacy: Except when done pursuant to a court order such as a search warrant, it is a violation of this policy to use ALPR to record license plates or vehicle descriptors except for vehicles visible to the public from a public road, street, or publicly accessible place.
 - b. Harassment or Intimidation: Using the ALPR system to harass or intimidate any individual or group is prohibited.
 - c. Use Based on a Protected Characteristic: It is a violation of this General Order to use the ALPR system, associated scan files, or hotlists solely because of a person's or group's race, color, religion or religious creed, sex (including pregnancy, childbirth, breastfeeding, and related medical conditions), sexual orientation, gender identity or expression, national origin, ancestry, age, disability (including physical, mental, intellectual, and learning disabilities), genetic information, marital status (including civil union status), veteran or military status, citizenship or immigration status or any other status protected status under applicable federal or Connecticut state law.
 - d. Personal Use: It is a violation of this General Order to use the ALPR system or associated data files or hotlists for any personal purpose.
 - e. It is a violation of this General Order to use the ALPR system, associated scan files, or hot lists for the purpose of identifying, or otherwise knowingly infringing upon, a constitutionally protected First Amendment right.
 - f. Knowingly accessing, using, or disseminating ALPR data with malicious intent for a purpose outside this General Order and Connecticut state law shall subject the authorized user to discipline and may result in referral to POSTC for certification action.

J. ALPR Records

1. The ALPR vendor and/or the Department will keep a record for each transaction on Department ALPR systems, including query information or hit information,

the name of the individual or agency accessing the data, the date and time of access, and the reason for access.

2. Department ALPR data may be downloaded and retained by Department personnel only for legitimate and authorized law-enforcement purposes, including specific investigations, and only in accordance with Connecticut state law and this General Order.
3. The ALPR Administrator may download audit-trail data for purposes of generating audit reports.
4. Records shall be maintained on the number and location of all ALPR cameras, including vehicle-mounted camera systems. See Section Q of this General Order.
5. The Chief of Police shall require the submission of reports documenting ALPR usage in accordance with this General Order and Connecticut state law.
6. ALPR data shall be stored in accordance with Department General Orders and manufacturer recommendations only to the extent consistent with Connecticut retention, deletion, and confidentiality requirements.

K. Accountability Safeguards

1. ALPR data shall be safeguarded by the Department's internal data-security protocols
2. All Freedom of Information (FOIA) requests for ALPR information shall be processed in accordance with C.G.S. §1-210(b)(3) law governing disclosure, confidentiality, and redaction of ALPR data.
 - a. ALPR data cannot be queried in connection with civil immigration issues unless the query is pursuant to C.G.S. §54-192h (b)(1)(A)(i), (ii) or (iii)
 - b. ALPR data may not be queried in connection with any investigation, civil or criminal, of any person concerning reproductive health care, gender-affirming health services, or any health care services that are legal in the State of Connecticut, or any manner that would violate C.G.S. §54-155b.
3. Officers shall clearly state in any written report, affidavit, or court application that ALPR data was used in connection with the incident or investigation being reported, unless otherwise authorized by the State's Attorney, the Office of the Inspector General, or the Chief State's Attorney's Office.

4. A regular audit of the Department's ALPR system shall be conducted to verify compliance with this General Order and other applicable policies and procedures. Audits shall include reviewing logs to confirm that queries are made for authorized purposes and that each user has entered all required information.
5. An ALPR hit may not reflect an updated or live NCIC status and should be verified with NCIC, the originating agency, communications personnel, or other authorized personnel before proceeding with additional enforcement action unless exigent circumstances exist.
 - a. Personnel approved to access ALPR data may use the data only for legitimate law enforcement purposes.
 - b. The sharing of ALPR data outside of the State of Connecticut requires the requesting agency to receive a copy of the approved POSTC Model Policy, and the requesting (state or federal) agency to accept its terms authorized by affirming it will abide by the provisions set forth herein. By making such affirmation to abide by the terms of this General Order, the requesting agency agrees not to use your ALPR data in violation of Connecticut state law, including but not limited to, the Connecticut Trust Act, C.G.S. §54-192h, and C.G.S. §54-155b, sections 1 & 2. If the written declaration or required affirmation described in this subsection is not executed, the law enforcement agency shall not share or provide access to such ALPR data.
6. Anyone who intentionally misuses the ALPR system or its data may face administrative penalties, including termination of employment, civil liability, and potential criminal charges.
7. Police departments shall publish their ALPR policy/General Order and required transparency information on their website or other public platform.

L. Training

1. All Department personnel must complete standardized training before gaining access to and using the ALPR system.
2. Standardized training shall include the following topics
 - a. System access and controls, including secure logins and permissions.
 - b. Hardware and software maintenance.
 - c. Hot list management, including download, interpretation, validation, and update procedures.

- d. Reporting requirements, including retention requirements for ALPR data.
- e. Data sharing requirements and restrictions, including written declaration requirements and limits on out-of-state sharing.
- f. Manufacturer-specific training for vendor hardware and software.
- g. Visual verification requirements for hits and confirmation procedures.
- h. Privacy and civil liberties protections, including First Amendment protections and restrictions on use based solely on protected characteristics.
- i. Prohibited Uses: Clearly state that ALPR systems and data are intended solely for official law enforcement purposes. They must not be used for personal reasons, shared with unauthorized individuals or organizations, or employed to violate any local, state, or federal laws, including but not limited to C.G.S. §54-192h (Trust Act), and C.G.S. §54-155b (Prohibition on use of public resources in furtherance of interstate investigation or proceeding concerning the provision, seeking or receipt of or assistance with reproductive health care services or gender-affirming health care services).
- j. Prohibited uses, including prohibitions relating to personal use, unauthorized sharing, immigration enforcement activity, and reproductive or gender-affirming health care investigations prohibited by law.
- k. Penalties for misuse, including administrative sanctions, termination, civil liability, criminal prosecution, and possible POSTC action where applicable.
- l. The role of the ALPR Administrator in updating training when there are changes in the ALPR system or applicable law.

N. Vendor Requirements

- 1. The Department shall not enter into or renew a contract with a private vendor for ALPR services unless the contract provides that the vendor shall not:
 - a. Sell ALPR data.
 - b. Share or transfer ALPR data to a third party without the Department's prior express written authorization for a specific lawful purpose.

- c. Allow access to ALPR data by any person other than the Department except pursuant to a warrant or court order.
 - d. Share, transfer, or allow access to ALPR data where the vendor reasonably believes the data may be used for immigration enforcement, prohibited reproductive or gender-affirming health care investigations, or identification of constitutionally protected activity.
 - e. Store the Department's ALPR data commingled with another customer's ALPR data or without industry-recognized encryption and security protections.
- 2. Any contract or agreement between the Department and an ALPR vendor shall expressly incorporate the requirements of this General Order and applicable Connecticut state law.
 - 3. All ALPR contracts shall contain a Connecticut choice-of-law provision and the vendor's consent to personal jurisdiction in Connecticut.

O. Transparency and Annual Reporting

- 1. The Department shall publish this General Order and any associated transparency information on its website.
- 2. Not later than January 31 following any calendar year during which the Department used an ALPR system, the Department shall complete and submit the standardized annual ALPR usage report required by Connecticut state law and shall publish that report on the Department's website.
- 3. Annual reporting shall include, at minimum, the number of license plates scanned, the number and reasons for searches performed, the number of times data was shared with or accessed by another entity, the identity of those entities, the number of times data was shared or accessed pursuant to judicial warrant, any instances of retention longer than permitted, any sensitive-location collection requests, and any privacy-related policy changes required by law.

P. Axon Fleet 3 Mobile ALPR Capabilities

- 1. The Darien Police Department uses the Axon Fleet 3 ALPR technology to capture objective evidence without compromising individual privacy. The Department utilizes real-time alerting in patrol vehicles to arrest wanted criminals, recover stolen vehicles and locate missing persons that are on various hot lists. Refer to General Order 5.18: *Dashboard Cameras*.

2. Usage of the Axon Fleet 3 ALPR capabilities shall comply with all of the provisions of this General Order.
3. The Axon Fleet 3 ALPR can detect license plate images, vehicle images, plate text, as well as date, time and location information.
4. The Axon Fleet 3 ALPR does not capture facial images or people.
5. The Axon Fleet 3 ALPR is currently programmed to include an internal hot list and CJIS information only.