	RIDGEFIELD POLICE DEPARTMENT POLICY AND PROCEDURE GENERAL ORDER	Distribution: ALL PERSONNEL	General Order Number:
		Original Issue Date: 02/28/25	Reissue/Effective Date: 10/04/26
Order Title: **AUTOMATED LICENSE PLATE READERS**		Accreditation Standard:	Section: 5
		Section Title: DEPARTMENT ROLE AND AUTHORITY	
Rescinds:		**Jeff Kreitz, 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

A. Purpose:

The purpose of this general order is to establish minimum standards and practices, pursuant to General Statutes § 7-294ee and PA 26-14(a) for Automated License Plate Reader (ALPR) systems, including data management, access requirements, training, and equipment management.

B. Overview:

ALPR technology is used by police departments to automate the process of analyzing license plates and vehicle descriptions/details for official law enforcement purposes, including, but not limited to, identifying stolen or wanted vehicles, stolen license plates, and missing, exploited, or endangered persons. It may also facilitate service of active warrants, suspect interdiction, recovery of stolen property, and active criminal investigations. ALPR technology uses high-resolution cameras and analysis software to identify a vehicle's license plate in real-time, converting images into electronically readable data that is then compared with the Criminal Justice Information Systems (CJIS), National Crime Information Center (NCIC), or Hotlist databases and queried for authorized law enforcement purposes. Some ALPR systems may also be equipped with technology capable of identifying a vehicle's make, model, color, and other characteristics and unique identifiers, which can be compared against the CJIS-NCIC or Hotlist databases.

C. Definitions:

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

ALPR: Automated License Plate Recognition, also referred to as Automated License Plate Reader.

ALPR Operator: Trained police department personnel authorized to operate the ALPR system and equipment.

ALPR Administrator: The Chief of Police or their authorized designee is responsible for ensuring compliance with all applicable laws and regulations related to ALPR systems, as well as providing access and training to department personnel in operating ALPR systems.

ALPR Data: Any data captured, recorded, held or stored, processed or derived from an automated license plate reader system, including, but not limited to, license plate characters, vehicle still or video images, vehicle attributes, location data, time stamps and metadata.

ALPR Data Query Logs: A record of any search or query of ALPR data.

ALPR System: The 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. Automated license plate reader system **does not** include an image recording device that provides evidence used in enforcement of an offense specified in the general statutes or by municipal ordinance, including, but not limited to, such devices as an automated traffic enforcement safety device, as defined in section 14-307b of the general statutes, or those used as part of a work zone speed control system, as defined in section 13a-261 of the general statutes, or a municipal school bus violation enforcement system, as defined in section 14-279c of the general statutes.

Gender-Affirming Health Care Services: Gender-affirming health care services that are permitted under the laws of this state, as defined in Conn. Gen. Stat. § 52-571m.

Hit: ALPR data that corresponds to license plate numbers, or other vehicle descriptors previously entered in the CJIS-NCIC Database, or a Hotlist alert that a license plate, or vehicle, matches a record in an ALPR database related to a law enforcement purpose authorized by this policy.

Hotlist: A list of registration numbers displayed on license plates maintained for comparison against a registration number collected by an automated license plate reader system.

Internal Hotlist Addendum: A hotlist that (A) is maintained for use only at a specific state facility or facilities for which the list was made and by the public agency that made such list, and (B) may contain registration numbers displayed on a license plate of a motor vehicle registered to a person who is identified in the making of such list as a potential threat to a person in the state facility, to the state facility or against the public agency operating the state facility, for reasons that include a previous conviction of such person for a misdemeanor or felony offense involving threats of physical violence or harassment against a person in the state facility, to the state facility or against the public agency operating the state facility or conduct by a person that is documented and involves threats of or attempted violence, harassment or incitement of physical violence against a person in the state facility, to the state facility or against the public

agency operating the state facility, provided no such inclusion on an internal Hotlist addendum is based on an arrest for or conduct that is solely speech, conduct or association protected by article first of the Constitution of the state or the first amendment to the United States Constitution.

Law Enforcement Agency: A department or agency for which a law enforcement officer is an employee of, otherwise paid by, or acting as an agent of, including, but not limited to, a municipal police department or the Division of State Police within the Department of Emergency Services and Public Protection.
Public Agency: Has the same meaning as provided in Conn. Gen. Stat. § 1-200.

Reproductive Health Care Services: Has the same meaning as provided in Conn. Gen. Stat. § 52-571m.

State Facility: Any building, or part thereof, owned, leased, occupied, or controlled by or used for business by an office or agency of the Executive Department, Legislative Branch, or Judicial Branch, either directly or indirectly, including entities providing direct services on behalf of such offices or agencies, but not including state-owned property leased to a federal entity. "State facility" includes the grounds of such facility and any garages or parking lots utilized in the operation of such facility, irrespective of whether such garages or parking lots are contiguous to the facility.

D. ALPR Administrator

The Chief of Police shall appoint an ALPR Administrator to oversee the ALPR system. Their duties shall include:

1. Ensuring that the ALPR system is used solely for proper department business and in compliance with this policy, as well as local, state, and federal laws.
2. Ensuring that only properly trained sworn officers, crime analysts, and communication operators are allowed access to the ALPR system, and/or to collect ALPR information.
3. Issuing login credentials to authorized users.
4. Ensuring that training requirements are completed for authorized users.
5. Monitoring ALPR systems to ensure the security of the information and compliance with applicable privacy laws.
6. Monitoring the ALPR system to ensure it operates according to specifications and reporting any software or hardware failures to the vendor for repair.
7. Reporting any violations of this policy, or law to the Chief of Police.
8. Reviewing any request for data sharing from an external law enforcement agency.
9. Performing a monthly audit of the department's ALPR system to verify compliance with this policy and other applicable policies. Audits shall include reviewing audit logs to confirm that queries are made for authorized and legitimate purposes and that each user has entered all required information.
10. Providing recommendations to the Chief of Police regarding any necessary updates.

E. <u>Permitted Use of the ALPR System:</u>

a. Queries:

ALPR data may be queried by authorized department employees upon a law enforcement officer's determination that data in the system may:

1. Be relevant and material to a specific active investigation of a criminal offense in which there is reasonable suspicion that the offense has been or is being committed.
2. Note: Any access to ALPR data for the purpose described in paragraph 1, above, shall result in a written record of the reason for the access and any associated case number for the complaint or incident that is being investigated and that is the basis for the access.
3. Assist in the apprehension of an individual with an outstanding warrant.
4. Assist in locating a missing or endangered individual.
5. Assist in the recovery of a stolen motor vehicle.
6. Be automatically compared with records of the Connecticut Online Law Enforcement Communications Teleprocessing System (COLLECT).
7. Be automatically compared with data contained in the Federal Bureau of Investigation's Kidnapping and Missing Persons list.
8. Be automatically compared with data contained in the Connecticut Criminal Justice Information System (CJIS).
9. Be automatically compared with data contained in the Federal Terrorist Screening Database.
10. Be automatically compared with data contained in the National Crime Information Center (NCIC) database.
11. Be automatically compared with data contained in the National Center for Missing and Exploited Children (NCMEC) database.
12. Be automatically compared with data contained in the Hotlist.
13. Be automatically compared with data contained in the Internal Hotlist Addendum.

b. Hotlist Entries:

Hotlist information can come from a variety of sources, including the NCIC as well as state, or national Amber Alerts. In addition to agency-supported Hotlists, authorized users may also manually add license plate numbers to Hotlists for a legitimate law enforcement purpose consistent with this policy and an internal hot list addendum for purposes consistent with the applicable definition. A known license plate number may be entered into the ALPR system to alert, otherwise known as a manual entry to the Hotlist, if that license plate number is related to any of the above-listed criteria. Adding a vehicle or license plate to a Hotlist in connection with a crime requires reasonable suspicion. License plate numbers of stolen cars, vehicles of interest, such as vehicles owned or operated by persons suspected of criminal activity and vehicles linked to AMBER or SILVER Alerts are regularly added to Hotlists circulated among law enforcement agencies. **F. <u>Procedures:</u>**

Only users designated by the ALPR Administrator and properly trained in the use and operational protocols of the ALPR system are authorized to operate the system. Access is limited to users with an approved login and password.

c. Queries

Queries can be made to the ALPR System for a permitted purpose. The user must log in with their personal credentials, which are specific to that user only.

To query the system, the following steps apply:

1. The user must enter the following information into the search screen:
    a. Parameters of the query (e.g. license plate, vehicle characteristics, time, date).
    b. Reason for the query, offense type; and
    c. Case number, or other identifying number.
2. ALPR system queries should focus on investigating criminal activity.

d. Hotlists

To create a Hotlist for a permitted purpose, the following steps apply:

1. Before creating a Hotlist, the user must obtain approval from a designated supervisor.
2. The manual entry shall list the offense type, vehicle description, and officer's name.
3. The user creating a "Hotlist" must set an expiration date and monitor the status of the entry.
4. At the conclusion of the expiration date, or if the vehicle is located, the entry shall be removed from the system.
5. Verification of the license plate shall be queried via CJIS/NCIC to ensure that the plate entered is accurate.
6. Manual entries should also include specific descriptors for vehicles being sought for legitimate law enforcement purposes, when available.

F. Stop Procedures (Traffic/Field)

1. A traffic stop initiated based on an alert from the ALPR System must be for one of the permitted query purposes. Unless there are exigent circumstances, officers shall follow these steps before conducting a traffic stop.

a. Officers shall (1) verify that the alert was accurate by visually confirming that the vehicle's license plate numbers, letters, issuing state, and any other identifying characteristics match the information in the ALPR System; or (2) develop independent reasonable suspicion.

b. Users shall verify the status of the license plate through the state's Criminal Justice Information System (CJIS), the National Crime Information Center (NCIC), the Department's Records Management System (RMS), or other appropriate data sources before a stop when circumstances permit, or as soon as practicable (e.g., when confirming a vehicle is stolen, etc.).

G. <u>Prohibited Use of the ALPR System:</u>

The following uses of ALPR data systems or ALPR data are strictly prohibited:

1. To monitor or investigate an individual based on such individual's actual or perceived race, ethnicity, sexual orientation, gender identity or expression, sex, pregnancy status, disability, citizenship, nationality or income level, or perceived criminal history, except in a case where an individual is being investigated for a potential criminal offense for which an element of such offense is a prior conviction.
2. For the purpose of identifying an individual engaged in an activity protected under the First Amendment to the United States Constitution.
3. For the purpose of investigating a suspected immigration violation or otherwise assisting in any civil or criminal immigration enforcement.
4. For the purpose of investigating or prosecuting any individual who has sought, received, or provided reproductive health care services or gender-affirming health care services that are permitted under the laws of this state.
5. Unless authorized pursuant to Conn. Gen. Stat. § 29-6d, collect ALPR data from an axed ALPR system located on the premises of, or within a distance 250 feet of, a reproductive or sexual health facility (as defined in Conn. Gen. Stat. § 42-515) that primarily provides gender-affirming health care services permitted under the laws of this state, or a nonprofit or community organization that primarily serves immigrant communities, excluding any property under federal jurisdiction, provided such facility or organization has notified POSTC of its location.
6. Permit real-time, bulk, or automatic access to ALPR data, or participate in a multistate, intrastate, or national ALPR data-sharing system or network, except in compliance with Section H of this policy.

H. <u>Data Sharing:</u>

1. A Connecticut law enforcement unit shall not share or provide access to automated license plate reader data, unless the individual or entity requesting such data or access is;
    a. A public agency of this state,
    b. A law enforcement agency of the state of New York or Rhode Island or the Commonwealth of Massachusetts or a municipality of said states or commonwealth.

c. A multijurisdictional task force of which a public agency of this state is a participating member, provided
    i. Such requesting law enforcement agency or task force provides a written declaration affirming that any data received will be used in compliance with the prohibitions set forth below;
        1. Will not be used for an immigration investigation or enforcement action.
        2. Will not be used to investigate or prosecute any individual who has sought, received or provided reproductive health care services or gender-affirming health care services that are permitted under the laws of this state.
        3. Will not be further disclosed except as permitted under the laws of this state.

    ii. In the case of a multijurisdictional task force, such specific data requested must be approved by the head of such task force or such head's designee and is directly and reasonably relevant to a specific investigation of such task force.

d. Any other law enforcement agency other than those of this state or described above, including any federal law enforcement agency, if such requesting law enforcement agency;
    i. Has a judicially issued probable cause warrant for the specific data requested, or
    ii. Is requesting specific data on an individual identified as a possible match in the Federal Terrorist Screening Database.

e. An individual requesting data regarding a motor vehicle registered in such individual's name, provided if a motor vehicle has more than one owner, lessor or regular user, all such owners, lessors and regular users join in the request and are natural persons.

2. Automated license plate reader data is confidential and shall not be deemed a public record for purposes of the Freedom of Information Act, Conn. Gen. Stat. § 1-200 et seq., except as provided in paragraph 3, below.
3. The following are not confidential and are public records for purposes of the Freedom of Information Act: (a) the location of any still or video image recording device used as part of an ALPR system, except that such location remains confidential and is not a public record if the device's purchase was funded in whole or in part by the U.S. Department of Homeland Security and such funding was conditioned on the device's location not being disclosed; and (b) data derived from any audit of the ALPR system, usage logs, and logs

detailing access to ALPR data, provided any ALPR data contained in such otherwise-disclosable records shall be redacted.

4. No public agency shall permit real-time, bulk, or automatic access to ALPR data by another public agency, unless such access is provided in response to a documented, case-specific request and the sharing of the data is not otherwise prohibited by this policy.
5. No Public Agency may participate in a system or network that shares automated license plate reader data, or provide to, or access such data through any multistate, intrastate or national data-sharing system or network unless such system or network requires, as a condition of participation in or access to such system or network, execution of a written declaration by each participant affirming that: (a) Any data shared, accessed or otherwise acquired will be used solely in compliance with this section and other laws of this state; and (b) such participant will not share or use such data, except in compliance with this policy and applicable law.
6. This Model Policy establishes minimum standards governing data-sharing. Each law enforcement agency shall ensure that any sharing of ALPR data complies with applicable federal and Connecticut law.

I. <u>Accountability and Safeguards:</u>

The ALPR data shall be safeguarded by the department's internal data security protocols.

The following shall be adhered to:

1. ALPR data cannot be queried in connection with civil immigration issues.
2. 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 General Statutes § 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 monthly audit of the department's ALPR system shall be conducted to verify compliance with this policy and other applicable policies. Audits will include reviewing audit 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 be from an updated or live NCIC database, and the hit should be verified with NCIC, or the originating agency. An officer must receive confirmation that the hit remains active from the police department communications or other authorized personnel (i.e., that the license plate is still stolen, wanted, or otherwise of interest) before proceeding with additional law enforcement action (unless there are exigent circumstances).

6. People approved to access ALPR data under these guidelines are only allowed to use the data for legitimate law enforcement purposes.
7. Police departments shall publish their ALPR policy and transparency portal (if available) on their website or other public platform.
8. Anyone who intentionally misuses the ALPR system or its data may face administrative penalties, including termination of employment, civil liability, and potential criminal charges.
9. Retention of ALPR data beyond twenty-one (21) days as evidence in an active criminal investigation or prosecution requires the approval of a supervisory law enforcement officer at the time such retention is designated, documented in a record stating the purpose for the retention and any associated case number, in accordance with Section K of this policy.
10. Any law enforcement officer found to have knowingly accessed, used, or disseminated ALPR data with malicious intent for purposes outside this policy shall be subject to disciplinary action, including suspension, cancellation, or revocation of certification by POSTC pursuant to Conn. Gen. Stat. § 7-294d. The ALPR Administrator shall notify POSTC of the suspected malicious use.
11. A public agency may be subject to an action by an aggrieved individual for injunctive or declaratory relief for violations of the permitted-use, prohibited-use, or confidentiality provisions of this policy, and the Attorney General may bring an action against a noncompliant private vendor, in accordance with Conn. Gen. Stat. § 7-294ee.
12. If the department suspects that a law enforcement agency of another state, or a federal law enforcement agency, has used ALPR data shared with it in a manner prohibited by this policy, the ALPR Administrator shall notify POSTC of the suspected prohibited use.

J. ALPR Records

1. The ALPR vendor and/or the police 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, along with the date and time of access, and the reason for the access.
2. The ALPR Administrator may download audit trail data for purposes of generating audit reports.
3. Records shall be maintained on the number and location of all ALPR cameras, including vehicle mount camera systems.
4. Each chief of police or the Commissioner of Emergency Services and Public Protection, as applicable, shall require the submission of reports documenting ALPR usage in accordance with this Model Policy.
5. Not later than January 31 following any calendar year in which the department used an ALPR system, the department shall submit a report detailing such usage, using the standardized reporting form promulgated by POSTC and the Institute for Municipal

and Regional Policy at the University of Connecticut, to said Institute, and shall publish such report on the department's website.

6. Audit logs required under this policy shall document, at a minimum, the number of times ALPR data was retained and the duration of such retention, and audits of the department's ALPR system shall be conducted not less than monthly.

K. Data Retention

1. Except as provided below, ALPR data shall not be retained for a period in excess of twenty-one (21) days, or for a shorter period if required by a contract with a private vendor that accesses the ALPR system or holds or stores such data. ALPR data may be retained beyond twenty-one (21) days only as follows: (a) pursuant to a warrant or court order issued by a judge or magistrate, or pursuant to court rules governing the preservation of evidence; (b) as evidence in an active criminal investigation or prosecution, provided (I) at the time the data is designated for retention, such retention is approved by a supervisory law enforcement officer and documented in a record stating the purpose for the retention and any associated case number, and (ii) the data is deleted upon the conclusion of the investigation if no criminal charges are lied, or upon the final disposition of the criminal case (including exhaustion of all direct appeals) if
there is a conviction with no sentence of imprisonment, or upon the release of the last defendant serving a term of imprisonment for a conviction to which the data relates, whichever occurs first, unless otherwise required to be retained under (a), above; or (c) for the purpose of conducting traffic analytics, provided the data is held, stored, and managed as de-identified, aggregated, or summarized data. Notwithstanding the foregoing, ALPR data may be retained beyond twenty-one (21) days if necessary to establish that a future offense, motor vehicle violation, or infraction is a subsequent offense, violation, or infraction for which the prescribed penalty exceeds the penalty for the prior offense, violation, or infraction. ALPR data is admissible as evidence in any court of this state only if it was collected, acquired, held, or retained in accordance with this policy, or was obtained pursuant to a warrant issued by a judge of the Superior Court.

L. <u>Training:</u>

All police department personnel must complete standardized training before gaining access to and using the ALPR system.

Standardized training shall include the following topics:

1. **System access & controls –** Training on secure logins and permissions.
2. **Hardware & software maintenance –** Guidelines on the condition and status of ALPR equipment (if applicable).

3. **Hotlist management –** How to download, interpret, and update Hotlists.
4. **Reporting requirements –** Reporting, including the retention requirements for LPR data.
5. **Data Sharing –** As listed in Section H of this policy.
6. **Manufacture-specific training –** Technical software and hardware navigation specific to a vendor's product.
7. **Visual verification requirement for hits -** To emphasize that an ALPR hit may not be from an updated or live NCIC database, and the hit should be verified with NCIC, or the originating agency.
8. **Privacy & Civil Liberties –** Educating Officers on protecting First Amendment Rights, ensuring that ALPRs are not used to target persons solely based upon protected characteristics, or to knowingly and intentionally infringe on a person's First Amendment Rights.
9. **Prohibited Uses -** As listed in Section G of this policy.
10. **Retention, Siting & Reporting Requirements –** Data retention limits, the distance restriction on axed ALPR collection near reproductive/sexual health facilities and immigrant-serving organizations, and the department's annual usage-reporting obligations under this policy.
11. **Penalties for Misuse**: Any person who knowingly engages in impermissible use of the ALPR system or its data may be subject to administrative sanctions, including termination, civil liability, and possibly criminal prosecution.
12. **The ALPR Administrator's role:** The ALPR Administrator shall ensure that any changes in the ALPR system or changes in applicable laws are included in the standardized updated training.
13. **Annual Refresher Training**

M. Vendor Requirements

1. Any private vendor, contractor, or third-party entity that stores, processes, or provides access to ALPR systems or ALPR data on behalf of a law enforcement agency is prohibited from sharing, transferring, selling, granting access to, or otherwise disseminating any ALPR data except in full compliance with this section and the policy adopted pursuant to this section. In particular, and notwithstanding any contrary terms of service, use agreement, or vendor policy incorporated into the contract, any such vendor shall not: (a) sell ALPR data; (b) share or transfer ALPR data to any third party without the contracting agency's prior express written authorization for a specific purpose; (c) allow any person other than the contracting agency to access ALPR data, except pursuant to a warrant or court order issued by a judge or magistrate (excluding any subpoena or grand jury demand); (d) share, transfer, or allow access to ALPR data if the vendor reasonably believes it may be used for immigration enforcement, for investigating or prosecuting any person for seeking, providing, receiving, or assisting with reproductive

health care services or gender-affirming health care services permitted under the laws of this state, or to identify or impose liability on any person based solely on constitutionally protected activity; or (e) commingle the department's ALPR data with data held or stored for any other public agency or person, or hold or store such data other than in accordance with industry-recognized data security practices, including encryption in transit and at rest.

2. Any contract or agreement with an ALPR vendor must provide for the above terms and that the vendor consents to personal jurisdiction in Connecticut for any related legal proceeding and that Connecticut law governs the contract. The Attorney General may bring an action against a vendor that violates these vendor requirements, and civil penalties and other relief may be available under Conn. Gen. Stat. § 7-294ee.