POSTC Automatic License Plate Readers (ALPR)
Model Policy

A. Purpose:

This Police Officer Standards and Training Council (POSTC) Model Policy establishes minimum standards and practices, pursuant to General Statutes § 7-294ee, for Automated License Plate Recognition (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 Hot List 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 Hot List 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: Scan files, alert data, and any other documents or data generated by, or obtained through utilization of an ALPR system.

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

ALPR System: The ALPR camera and all related hardware and software used by the Police Department, which includes stationary ALPR cameras and ALPR cameras mounted on structures such as poles, traffic barriers, or bridges, as well as mobile ALPR cameras that are affixed to law enforcement vehicles or other equipment for mobile use.

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

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

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 quarterly 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. Permitted Use of the ALPR System:

a. Queries:

ALPR data may be queried by authorized department employees in the following circumstances:

1. Investigations of criminal offenses, where there is reasonable suspicion that a criminal offense was committed. ALPR data may not be queried in connection with civil immigration matters unless the query pursuant to Conn. Gen. Stat. §54-192h*(b)(1)(A)(i), (ii) or (iii)*. ALPR data may not be queried in connection with any investigation, civil or criminal, of any individual in connection with any reproductive health care or gender-affirming health care services that are legal in this state
2. As part of an active investigation related to a missing, exploited, or endangered person, or a person associated with Human Trafficking.
3. To locate a person with an outstanding warrant, a suspect in a crime, a stolen vehicle, or a stolen license plate.
4. Any case involving allegations of flight or evasion from law enforcement.
5. Efforts to locate a fugitive from justice.
6. Cases where physical surveillance of a target of a criminal investigation is determined to be dangerous or compromised.
7. Emergencies involving wrong-way drivers, operators who seem intoxicated, or those experiencing medical emergencies.
8. Motor vehicle accidents resulting in fatalities or serious injuries.
9. Motor vehicle crashes related to evading responsibility.
10. Situations that would meet the "exigent circumstances" exception to the Fourth Amendment.
11. National Security & Counterterrorism: Identifying vehicles associated with individuals on federal or state Terrorist Watch Lists

b. Hot List Entries:

Hot List information can come from a variety of sources, including the NCIC as well as state, or national Amber Alerts. In addition to agency-supported Hot Lists, authorized users may also manually add license plate numbers to Hot Lists for a legitimate law enforcement purpose consistent with this policy. A known license plate number may be entered into the ALPR system to alert, otherwise known as a manual entry to the Hot List, if that license plate number is related to any of the above-listed criteria. Adding a vehicle or license plate to a Hot List 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 Hot Lists 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.

a. 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:
    i. Parameters of the query (e.g. license plate, vehicle characteristics, time, date).
    ii. Reason for the query, offense type; and
    iii. Case number, or other identifying number.
2. ALPR system queries should focus on investigating criminal activity.

b. Hot Lists

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

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

c. Stop Procedures (Traffic/Field)

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

i. 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.

ii. 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 are strictly prohibited:

1. **Invasion of Privacy**: Except when done pursuant to a court order such as a search warrant, it is a violation of this policy to utilize the ALPR to record license plates, or vehicle descriptors except for vehicles visible to the public (e.g., vehicles on a public road or street, or on private property but whose license plates are visible from a public road, street, or a publicly accessible place, such as a parking lot of a shop or business).

2. **Harassment or Intimidation:** Using the ALPR system to harass or intimidate any individual or group is a violation of this Model Policy.

3. **Use Based on a Protected Characteristic**: It is a violation of this Model Policy to use the ALPR system or associated scan files or Hot Lists 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 under applicable U.S. federal or Connecticut law.

4. **Personal Use:** It is a violation of this Model Policy to use the ALPR System or associated data files or Hot Lists for any personal purpose.

5. **First Amendment Rights:** It is a violation of this Model Policy 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.

H. Data Sharing:

1. A Connecticut law enforcement unit shall not share with, sell or transfer to, or allow access by ALPR data with an out-of-state law enforcement agency without first obtaining a written declaration from the out-of-state law enforcement agency which expressly affirms that the ALPR information obtained will not be used in a manner that violates this POSTC Model Policy or the Connecticut General Statutes as delineated in this policy. If a written declaration of affirmation is not executed, the law enforcement unit shall not share the ALPR information with the out-of-state law enforcement agency. By expressly affirming that it will abide by the terms of this Model Policy, the requesting agency agrees not to use its ALPR data in violation of Connecticut State Law, including but not limited to, the Connecticut General Statutes § 54-192h (the Connecticut Trust Act) and Connecticut General Statutes § 54-155b. (FLOCK Safety has a "Policies" page on their agency portal that may be used for this purpose.
2. The Chief of Police or their designee will decide which external state, regional, or national networks can access the department's ALPR data.
3. ALPR data may only be accessed, retrieved, or shared for official law enforcement or public safety purposes.
4. Information sharing between law enforcement agencies shall be guided by departmental policies or memoranda of understanding.
5. 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. Accountability and Safeguards:

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

The following shall be adhered to:

1. All Freedom of Information (FOIA) requests for ALPR data shall be processed in accordance with Connecticut General Statutes §§ 1-210(b)(3) and 1-215.

2. ALPR data cannot be queried in connection with civil immigration issues unless the query is pursuant to § 54-192h *(b)(1)(A)(i), (ii) or (iii)*.
3. 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.
4. 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.
5. A regular 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.
6. 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).
7. People approved to access ALPR data under these guidelines are only allowed to use the data for legitimate law enforcement purposes.
8. 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 by affirming it will abide by the provisions set forth herein. By making such affirmation to abide by the terms of this Model Policy, 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, General Statutes § 54-192h, and General Statutes § 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.
9. Police departments shall publish their ALPR policy and transparency portal (if available) on their website or other public platform.
10. Anyone who intentionally misuses the ALPR system or its data may face administrative penalties, including termination of employment, civil liability, and potential criminal charges.

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. Department ALPR data may be downloaded and retained by department personnel for legitimate and authorized law enforcement purposes, including specific investigations. This data shall be kept in accordance with Connecticut Public Records laws and maintained at least until a final disposition has been reached in the case.
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 mount camera systems.
5. 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.

K. Data Retention

1. ALPR data shall be retained for no more than thirty (30) days, unless otherwise preserved as potential evidence in a criminal, administrative, or civil matter.

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. **Hot List management** – How to download, interpret, and update Hot Lists.
4. **Reporting requirements –** Reporting, including the retention requirements for LPR data.
5. **Data Sharing –** The sharing of ALPR data outside of the State of Connecticut requires that the requesting agency receive a copy of the adopted POSTC Model

Policy, and that the requesting agency has accepted the terms outlined in 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 -** 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 the General Statutes § 54-192h (Trust Act), and the General Statutes § 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).
10. **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.
11. **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.

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; and
2. Any contract or agreement between a law enforcement agency and such ALPR vendor must expressly incorporate the provisions of this section and the Model Policy adopted pursuant to this section and section I, paragraph 8.