



# Seattle Police Department Policy Manual



## 16.170 – Automatic License Plate Readers

Original Effective Date: 02/01/2019

**Revised Effective Date: 10/15/2024**

This policy applies to the use of automatic license plate readers (ALPR) by all department employees.

This policy defines a minimum set of binding guidelines to govern the use of ALPR data, to enable the collection and use of such data in a manner consistent with respect for individuals' privacy and civil liberties.

ALPR uses high speed cameras to photograph vehicle license plates. ALPR technology will only be placed on law enforcement and parking enforcement vehicles for authorized law enforcement and public safety purposes as set forth in this policy.

ALPR data is law enforcement information and will be used solely for law enforcement purposes. Any non-law enforcement usage of ALPR data is strictly prohibited.

Any data obtained from ALPR technology will be used and handled pursuant to this policy and applicable city, state, and federal laws. A search warrant will be obtained when legally required.

### 16.170-POL-1 Definitions

**ALPR Administrator:** a trained department employee who manages the utilization of the ALPR software from the end user through training, reporting, and monitoring.

- The department will have two (2) ALPR Administrators: one for Parking Enforcement personnel who use Gentec Security Center, and one for personnel who use Evidence.com's ALPR module.
- Gentec Patroller data is used during a PEO's shift and is not retained at the completion of their shift. Evidence.com retains ALPR read data for 90 days.

**Automated License Plate Reader (ALPR):** a device that uses cameras and computer technology to compare digital images of license plates to lists of known plates of interest.

**Evidence.com ALPR Module:** ALPR network data storage system accessible only to trained and authorized department employees.

# Seattle Police Department Policy Manual

**Genetec Security Center:** ALPR network data storage system access portal, accessible to authorized department employees. Genetec Security Center resides on desktop computers, but only authorized users can use their login credentials.

**Hit:** alert from the ALPR system that a scanned license plate number may be in the NCIC or other law enforcement database for a specific reason including, but not limited to, being related to a stolen vehicle, wanted person, missing person, domestic violence protective order, other criminal activity, unpaid parking violations, or current parking violations.

**Hot List:** license plate(s) associated with vehicles of interest from an associated database, including, but not limited to: National Crime Information Center (NCIC), Washington Crime Information Center (WACIC), Department of Licensing (DOL) databases, local be on the lookout notices (BOLOs), or Seattle Municipal Court.

**Reads:** data obtained by an ALPR of license plates within public view that were read by the device, including images of the plate and vehicle on which it was displayed, and information regarding the location of the police vehicle at the time of the ALPR read.

**SCOFFLAW:** license plates associated with four or more unpaid parking citations subject to City of Seattle Scofflaw Ordinance ([SMC 11.35](#)).

## 16.170-POL-2 General Policy

### 1. Only Employees Trained in the Use of ALPR Equipment Will Use and Access ALPR Devices and Data

Before employees operate the ALPR system or access ALPR data, they will complete department training on the proper and lawful use of the system.

The parking enforcement users will be trained by parking enforcement FTO's and or the ALPR Administrator. Parking enforcement will keep a documented record of employees that have completed the training.

### 2. The Education and Training Section Will Coordinate with the Two (2) Department ALPR Administrators to Provide Department ALPR Training and Document Approved Users

Training will include:

- Instruction on the appropriate use and collection of ALPR data with emphasis on the requirement to document the reason for any data inquiry in the ALPR System, whether through the ALPR client or the ALPR server.
- Requirements of any Surveillance Impact Report regarding ALPR adopted by the City Council.

# Seattle Police Department Policy Manual

Additionally, all ALPR Operators will maintain ACCESS Level 1 Certification pursuant to ACCESS, WACIC, and NCIC.

The Education and Training Section will coordinate with the ALPR Administrators to maintain a roster of approved ALPR users.

- The Parking Enforcement ALPR Administrator will maintain a list of all employees trained in the use of Parking Enforcement ALPR equipment.
- The Patrol ALPR Administrator will maintain a list of all employees trained in the use of Patrol ALPR equipment and the ALPR client software.

### **3. Authorized and Prohibited Uses**

ALPR systems will only be deployed for official law enforcement purposes. These deployments are limited to:

- Locating stolen vehicles;
- Locating stolen license plates;
- Locating wanted, endangered or missing persons; or those violating protection orders;
- Canvassing the area around a crime scene;
- Locating vehicles that have failed to pay for parking in a paid parking zone;
- Locating vehicles that have not purchased a parking permit for specific Residential Parking Zones;
- Locating vehicles under SCOFFLAW; and
- Electronically chalking vehicles for parking enforcement purposes.

ALPR data maintained on Evidence.com or Gentec Security Center will only be accessed by trained, SPD employees for official law enforcement purposes. This access is limited to:

- Search of specific or partial plate(s) and/or vehicle identifiers as related to:
  - A crime in-progress;
  - A search of a specific area as it relates to a crime in-progress;
  - A criminal investigation; or
  - A search for a wanted person; or

# Seattle Police Department Policy Manual

- Community caretaking functions such as, locating an endangered or missing person.

Officers/detectives conducting searches in the system will complete the Read Query screen documenting the justification for the search and applicable case number.

ALPR will not be used to intentionally capture images in private area or areas where a reasonable expectation of privacy exists, nor will it be used to harass, intimidate, or discriminate against any individual or group.

## **4. ALPR Operators Will Respond to Hits/Alerts by Confirming the ALPR Information**

Sworn employees have discretion when responding to calls. The department recognizes there may be times when employees are unable to recover all located stolen vehicles, such as when they are enroute to a dispatched call. At a minimum, sworn employees should verify and confirm hits and note their location through DATA, at their earliest opportunity.

When an operator receives a Hit/alert indicating a positive Hit from the Hotlist database, a digital image of the license plate will be displayed on the Mobile Data Computer (MDC) screen.

- ALPR operators will compare the digital image of the license plate to the Hotlist information to verify the Hit for both the state and characters on the plate.
- ALPR operators will confirm the ALPR information by radio or MDC to immediately confirm the Hit prior to taking enforcement or other type of police action (absent exigent circumstances).
- ALPR operators will enter a disposition for all ALPR Hits by selecting either "Accept" or "Misread" before removing the Hit from the computer screen.

Dispositions include:

- Location noted, not recovered;
- Stolen Recovery – Arrest;
- Stolen Recovery – No Arrest;
- Eluded – Lost;
- Plates only;
- SCOFFLAW; and
- Wanted person or vehicle Misread/Twin plate.

# Seattle Police Department Policy Manual

Positive ALPR hits leading to action requiring an incident report will be documented within the report narrative.

- Notified Radio – PEO;
- Cited/notice – PEO;
- Citizen Contact – PEO.

## **16.170-POL-3 ALPR Equipment**

### **1. Operators Will Notify the ALPR Administrator Upon Discovery of any Damaged or Inoperable ALPR Equipment**

Sworn operators will document the damage/issue on the Vehicle Damage Report (Form 1.35) found in Word Templates. PEOs will report any issues or damage to their supervisor.

### **2. Operators Will Activate the ALPR Software and Receive the Automatic Updated Hot List at the Start of Each Shift**

ALPR units installed on marked patrol and PEO vehicles will be activated and used at all times unless the operator of the vehicle has not been trained.

### **3. Operators Will Alert Seattle ITD and the ALPR Administrator of Any Equipment Defects**

## **16.170-POL-4 ALPR Administrator Roles and Responsibilities**

### **1. The Parking Enforcement Unit Will Assign and Support a Parking Enforcement ALPR Administrator for ALPR Electronic Vehicle Chalking**

PEOs may use ALPR electronic vehicle chalking to assist in enforcing parking restrictions in time-limited, no pay parking zones and electronic parking permit management in restricted parking zones (RPZ).

PEOs will not have access to stored ALPR data in Evidence.com.

Only trained PEO's will have access to the Gentec Security Center.

### **2. The ALPR Administrators Will Assist the Office of Inspector General (OIG) in Conducting Periodic Audits of the Department's ALPR Systems**

## **16.170-POL-5 ALPR Data Storage and Retention**

# Seattle Police Department Policy Manual

ALPR technology collects digital images of license plates and associated license plate numbers. The technology collects the date and time that the license plate passes a digital-image site where an ALPR is located. The department will store ALPR data in secured digital storage with multiple layers of security protection. Firewalls, authentication, and other reasonable security measures will be utilized. Only trained department employees can access stored ALPR data and all data search requests are logged within the system.

## **1. Except for Hits and Data Used for a Parking Enforcement Action, No Data Collected by Parking Enforcement ALPR will be Accessed More Than 24 After it was Collected**

Metadata and images of detections will be deleted from the server within 24 hours of collection unless related to hits and data for parking enforcement action.

## **2. Criminal Intelligence Maintains Operational Control Over Patrol ALPR and ALPR Used for Parking Enforcement and Scofflaw**

## **3. The Department Will Store Read Data from Patrol ALPR for 90 days on Evidence.com**

After the 90-day retention period, the Evidence.com will purge the data unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action, or is subject to a lawful action to produce records. In those circumstances, the applicable data should be downloaded from the Evidence.com server onto portable media and entered into evidence.

## **4. ALPR Data Related to a Criminal Investigation Will be Retained by the Case Detective in the Investigation Case File for a Period of Time in Accordance With State Retention Laws**

## **16.170-POL-6 Stored Read Data from Patrol and PEO ALPR Access and Use**

### **1. Employees Accessing ALPR Data Must Login Through the ALPR Password-Protected System**

This system records when an employee accesses ALPR data by logging the employee's name, the date, and the time of the request.

### **2. Employees Conducting Searches in the Patrol ALPR System Will Provide a Case Number and Justification for the Search**

If a case number does not exist, the employees will provide thorough justification for the legitimacy and lawful purpose of the search.

# Seattle Police Department Policy Manual

## **3. Employees Will Not Share ALPR Passwords and Login Credentials**

## **4. Only the Real Time Crime Center (RTCC) and Criminal Intelligence Units may conduct Searches of ALPR Data**

Sworn Employees should work with personnel in either of these two groups to complete a search of ALPR data. Sworn employees will still be able to see the recent hits/reads that have occurred in their vehicles while logged on into Axon Fleet Dashboard.

## **5. Sworn Employees are Prohibited From Taking Photos or Screen Captures of ALPR Information and/or Sharing ALPR Data Without Authorization**

## **16.170-POL-7 Releasing or Sharing ALPR Data**

ALPR data will only be shared with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law.

Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed by the Legal Unit pursuant to the applicable Rules of Civil or Criminal Discovery or the Washington Public Records Act ([RCW 42.56](#)).

The Legal Unit will maintain requests for ALPR data by non-law enforcement or non-prosecutorial agencies.

The OIG may audit department records at any time to ensure compliance with this policy.