

Arlington Police Department

POLICY 708 — AUTOMATED LICENSE PLATE READER

Policy Number 708

Effective Date 03/30/2026

Policy Subject Automated License Plate Reader

Responsible Division: Operations Division

Authority: RCW Chapter 10.130; RCW 42.56.240; RCW 42.56.904; applicable Washington State Archives records-retention schedules; applicable criminal justice information-security requirements; and other applicable law to include ESB6002

TABLE OF CONTENTS

- 708.1 Purpose and Scope
- 708.2 Definitions
- 708.3 Policy
- 708.4 Administration
- 708.5 Operations
- 708.6 Prohibited Use of the ALPR System
- 708.7 Data Collection and Retention
- 708.8 Accountability
- 708.9 Releasing ALPR Data
- 708.10 Training
- 708.11 Transparency, Public Awareness, and AGO Reporting
- 708.12 Violations
- 708.13 Records and References

708.1 PURPOSE AND SCOPE

Automated License Plate Reader (ALPR) technology provides automated detection of license plates and related vehicle information. The Arlington Police Department (APD) may use ALPR systems only for lawful, authorized public-safety purposes. This policy establishes requirements for the acquisition, deployment, use, access, retention, audit, disclosure, oversight, and reporting of ALPR systems and ALPR data. This policy applies to every APD-operated, APD-controlled, or APD-accessed ALPR system, including fixed-camera systems, mobile or vehicle-mounted systems, Flock Safety systems, Axon FLEET 3 or successor in-car ALPR functions, software platforms, vendor-hosted data, hot lists, alerts, searches, stored data, and related audit trails.

708.2 DEFINITIONS

ALPR data means information or data collected, retained, accessed, or generated by an ALPR system, including license plate characters, plate images, vehicle images, Global Positioning System coordinates, location, date, time, speed, query results, alert data, vehicle characteristics, and other identifying information or associated metadata. ALPR data does not include video recordings captured by body-worn cameras or in-car video systems unless the recording is converted to computer-readable plate data or the recording or associated metadata is

searchable, analyzed, compiled, or indexed for the purpose of identifying a vehicle, person, biometric information, or reconstructing a vehicle or person location.

ALPR system means one or more mobile or fixed high-speed cameras combined with computer algorithms to convert images of license plates into computer-readable data.

Audit trail means a record of access to or activity within an ALPR system or ALPR data, including searches, views, exports, downloads, sharing, entries, updates, and other system actions.

Audit trail data means data collected or generated by an ALPR system for purposes of producing an audit trail, including information about who accessed or used the system and how and when the system was accessed or used. Audit trail data does not include ALPR data.

Authorized user means an APD employee or other person specifically approved by the ALPR Program Administrator to access an ALPR system for an authorized purpose.

Hot list means a list used by an ALPR system to identify a plate or vehicle associated with a statutorily authorized database or a qualifying, documented investigation.

Privately held ALPR data means ALPR data collected, possessed, or controlled by a private person or entity and not by a government agency.

Protected facility means a facility or location identified in RCW 10.130.030, including a protected health-care facility, a facility conducting immigration matters, an elementary or secondary school, a place of worship, a court, or a food bank.

Search means a query, review, filter, alert follow-up, historical lookup, vehicle-location query, or other retrieval of ALPR data.

708.3 POLICY

It is the policy of the Arlington Police Department to use ALPR technology only for lawful and authorized public-safety purposes while recognizing and protecting the constitutional and privacy rights of the public. All ALPR data and images collected or maintained by APD are for official Department use only and shall be handled, retained, accessed, shared, and released only as authorized by law and this policy. No member may access, search, use, retain, share, export, download, disclose, or otherwise handle ALPR data except as specifically authorized by this policy and applicable law.

708.4 ADMINISTRATION

The Chief of Police shall designate an ALPR Program Administrator and may designate one or more backup administrators. The ALPR Program Administrator shall have primary responsibility for program oversight and compliance. APD is the legal owner of ALPR data collected by an ALPR system operated by APD.

The ALPR Program Administrator shall:

- Maintain an inventory of each APD ALPR system, camera, deployment location, vehicle assignment, software module, vendor platform, approved user account, hot-list source, and applicable retention and sharing configuration.
- Coordinate required registration, certification, policy submission, and other communications with the Washington State Attorney General's Office (AGO).
The Chief of Police or authorized head of agency shall make required AGO

certifications only after verifying statutory compliance, an operative policy, and a documented training process.

- Maintain written documentation of APD's ALPR training process and training-completion records.
- Approve or deny user access, conduct periodic access reviews, and ensure prompt deactivation of access when a user no longer requires it.
- Coordinate with Information Technology, Fleet, Records, Procurement, City Attorney, and vendors to verify that system configurations and contracts comply with this policy and law.
- Conduct or coordinate periodic compliance checks and the annual internal audit required
- Coordinate public-awareness measures, website publication, and required annual reporting required
- Promptly notify command staff and City Attorney of suspected material noncompliance, unauthorized access, security incidents, prohibited sharing, or a vendor configuration that may conflict with this policy or law.

708.5 OPERATIONS

708.5.1 Authorized Use

ALPR systems and ALPR data may be accessed, operated, or used only for purposes authorized by RCW 10.130.030 and this policy. Authorized use is limited to the following:

a. Comparing captured ALPR data with data maintained by the Washington State Department of Licensing, the State Criminal Justice Information System, the Federal Bureau of Investigation Kidnappings and Missing Persons List, the National Center for Missing and Exploited Children List, or the Washington Missing Persons List.

b. Comparing captured ALPR data with license plate numbers or vehicle characteristics entered into a state or local ALPR system database, or entered for a specific search, when an officer determines that the plate or vehicle characteristic is relevant and material to an investigation of a vehicle that is:

1. Stolen;
2. Associated with a missing or endangered person;
3. Registered to an individual with an outstanding felony or gross-misdemeanor warrant; or
4. Related to or involved in a felony or gross misdemeanor.

No other access, operation, use, search, or dissemination of ALPR data is authorized unless required in a judicial proceeding or expressly authorized by a subsequent amendment to applicable law.

708.5.2 Search Documentation and Hot Lists

For each historical search or investigative query, the authorized user shall enter or document, in the ALPR system or associated case record:

- A current case number or call-for-service number.

- The specific investigative or public-safety purpose.
- The qualifying offense type when the search supports a criminal investigation.
- The license plate, vehicle characteristic, or other search parameter.
- The reason the plate, vehicle, or characteristic is relevant and material to the authorized purpose.

APD shall ensure available database and hot-list updates are applied at least every 24 hours. Local hot-list entries shall be limited to qualifying categories, include a case or source reference, be reviewed for continued validity, and be removed promptly when no longer authorized.

708.5.3 ALPR Alerts and Enforcement Contacts

A positive match from an ALPR alone does not constitute reasonable suspicion to stop a vehicle. Before conducting a traffic stop or other enforcement contact based on an ALPR alert, an officer shall either develop reasonable suspicion independent from the ALPR match or immediately complete both of the following:

- Visually compare the actual license plate on the vehicle with the plate image displayed by the ALPR system to confirm a match.
- Confirm by other authorized law-enforcement means that the license plate number appears in an authorized database or qualifying hot list and that the listing supports the proposed contact.

The officer shall document the verification method in CAD, a report, or other approved record, as appropriate. A dispatch confirmation, returned record, or alert status that is stale, incomplete, inconsistent, or otherwise unreliable shall not be relied upon without further verification.

708.5.4 Camera Placement, Deployment, and Configuration

Before a fixed ALPR camera is installed, relocated, or materially reconfigured, the ALPR Program Administrator shall prepare or obtain written deployment documentation identifying the camera identifier, proposed location, direction or field of view, deployment purpose, and protected-facility review.

Fixed cameras shall not be sited, aimed, or configured in a manner that collects prohibited data from the premises, immediate surroundings, or access to or from protected facilities. APD shall review camera siting at least annually and when a substantial location, configuration, operational, or community-impact concern is identified.

Before a mobile or in-car ALPR capability, including Axon FLEET 3 functionality, is activated for operational use, APD shall verify that the technology can meet the requirements of this policy, including user authentication, authorized-use documentation, retention, audit, sharing, and deletion requirements. The ALPR Program Administrator shall ensure vendor and system settings limit collection, access, retention, sharing, and analytic functions to what is authorized by this policy and law.

708.6 PROHIBITED USE OF THE ALPR SYSTEM

APD personnel shall not use an ALPR system or ALPR data for any purpose prohibited by law, including:

- Immigration investigation or enforcement, including use of ALPR systems or ALPR data to assist federal civil immigration enforcement.
- Investigation or enforcement related to protected health-care services.
- Tracking or monitoring a person engaged in activity protected by the Washington Constitution or United States Constitution, including speech, assembly, association, worship, or protest.
- Personal, political, commercial, discriminatory, retaliatory, or curiosity-based purposes.
- Generalized surveillance, location tracking, or intelligence gathering that is not connected to an authorized purpose under Section 708.5.
- Collection of ALPR data on the premises, immediate surroundings, or access to or from a protected facility, including adjacent parking lots used primarily or exclusively by a protected facility.
- Sale, lease, rental, purchase, or other commercial transaction involving ALPR data or audit trail data.
- Accessing or obtaining privately held ALPR data without a valid court-issued probable-cause warrant.
- Circumventing statutory restrictions by using vehicle descriptors, camera selection, vendor analytics, another agency account, or any other technique to obtain information that APD could not lawfully collect or use directly.

708.7 DATA COLLECTION AND RETENTION

Unless a specific exception in RCW 10.130.040 applies, APD shall not use or share ALPR data for any purpose other than the purpose for which it was collected and shall not retain ALPR data longer than 21 days from the date of collection. APD shall configure ALPR systems, including vendor-hosted systems, to automatically delete routine ALPR data at or before the end of the 21-day period.

ALPR data may be retained beyond 21 days only:

- a.** Pursuant to a valid, court-issued, probable-cause felony or gross-misdemeanor warrant or subpoena, or as permitted by court order in a criminal or civil case. Data retained under this subsection shall be deleted at the conclusion of the applicable criminal or civil case, pursuant to the applicable records-retention schedule. ALPR data may be shared in discovery as allowed by applicable court rules.
- b.** For parking enforcement, if applicable, provided the data is deleted no later than 12 hours after final disposition of the enforcement case, including exhaustion of applicable appeals.
- c.** For traffic studies, if applicable, provided the data is deleted no later than 30 days after collection.

d. For enforcement of commercial vehicle systems, if applicable, provided the data is deleted no later than six months after collection.

e. For as long as captured ALPR data is needed as evidence of specific unlawful conduct.

708.7.1 Preservation and Deletion Controls

- When ALPR data is needed as evidence, the member shall follow approved preservation procedures, document the case number and reason for preservation, and ensure appropriate chain-of-custody and records-retention controls.
- No member may create an unofficial secondary repository, personal download, screenshot collection, or other copy of ALPR data outside an approved evidence, records, or case-management process.
- The ALPR Program Administrator shall periodically verify vendor and internal deletion settings and document corrective action when a retention-control issue is identified.

708.8 ACCOUNTABILITY

708.8.1 Access and Security

Access to ALPR systems shall be limited to authorized users with a demonstrated operational need. APD shall use unique user accounts, role-based permissions, and available multifactor authentication. Shared credentials are prohibited. Access shall be deactivated promptly upon separation, reassignment, suspension, or loss of operational need.

708.8.2 Audit Trails

APD shall retain ALPR audit trail data for at least two years. Audit trails shall capture, to the extent supported by the system, the identity of the user or organization; date and time of access; data elements or search terms used; stated purpose; qualifying offense type for criminal investigations; case or call-for-service number; location of accessed cameras; results or actions taken; and all data exports, downloads, sharing, entries, updates, and other material system activity. Data retained solely as audit trail data may be used only for auditing and compliance purposes. Audit trail data shall not be searched, analyzed, compiled, or indexed for investigative purposes. When audit trail data is subject to public disclosure, data elements containing unique identifiers shall be partially redacted as required by law.

708.8.3 Compliance Audits

The ALPR Program Administrator shall conduct or coordinate a documented internal audit at least annually. The audit shall evaluate user access, search documentation, authorized uses, retention and deletion, sharing and release, vendor configurations, protected-location compliance, hot-list management, training, security, and corrective action.

- Audit findings and corrective actions shall be reported to the Chief of Police or designee.

- Suspected misuse, unauthorized access, or material policy noncompliance shall be investigated promptly. Additional review by City Attorney, Information Technology, Records, or other responsible personnel may occur as deemed appropriate from investigation.
- APD may conduct additional spot checks, supervisory reviews, or vendor-account reviews at any time.

708.9 RELEASING ALPR DATA

708.9.1 Sharing and Disclosure

APD shall not disclose, share, or permit access to ALPR data except as required in a judicial proceeding. Direct system access shall not be granted to another entity unless that entity is a state or local agency authorized by RCW 10.130.030 to collect ALPR data, and access is specifically approved by the Chief of Police or designee

A third-party vendor may access an APD ALPR system only to the extent necessary to fulfill a specific APD-authorized purpose.

708.9.2 Requests and Public Records

Requests from another agency, prosecutor, court, or other person for ALPR data shall be documented in writing and routed through the ALPR Program Administrator, Records, a supervisor, and/or City Attorney as appropriate.

The request record shall identify the requester, legal authority, case or CFS number, purpose, scope of data sought, approving authority, and data disclosed. Public disclosure requests involving ALPR data shall be referred immediately to the designated handler of Public Disclosure Requests.

ALPR data is exempt from public disclosure except as otherwise provided by law, including qualifying nonidentifiable bona fide research.

708.9.3 Vendor Controls

APD shall maintain vendor agreements and technical configurations that, at a minimum, require or enable:

- APD and City control of data generated by APD-operated or APD-controlled systems.
- No sale, lease, rental, or unauthorized secondary use of ALPR data or audit trail data.
- Sharing disabled by default except where specifically authorized and approved.
- APD knowledge of and consent to material changes in sharing, access, retention, analytics, or data-use settings.
- Technical controls designed to prevent unauthorized access and disclosure, including access by federal civil immigration enforcement personnel.
- Availability of complete audit logs, including vendor-generated audit data, to APD.
- Retention and deletion settings that comply with Section Arlington Police Departments' data and retention policies.

- Prompt security-incident notification, cooperation, and data return/destruction requirements.
- A documented process for review of vendor updates that may affect statutory or policy compliance.

708.10 TRAINING

No employee may access or operate an ALPR system until completing Department-approved training. Training shall be documented and shall include legal limitations, authorized uses, prohibited uses, protected locations, alert-verification requirements, search documentation, retention and evidence preservation, sharing and release rules, audit trails, information security, vendor/platform procedures, and consequences of misuse. Authorized users shall complete platform-specific instruction for the ALPR systems they use, including Flock and Axon FLEET 3 functions where applicable. APD shall provide refresher training at intervals established by the ALPR Program Administrator and whenever material legal, policy, or system changes occur. Supervisors shall ensure that assigned personnel maintain current training and shall address questions about proposed ALPR use before a search or access occurs when practicable.

708.11 TRANSPARENCY, PUBLIC AWARENESS, AND AGO REPORTING

APD shall take reasonable steps to make the public aware of its ALPR program prior to or coincident with implementation of an ALPR system. APD shall publish this policy on the Department or City website and shall submit the policy web link and other required information to the AGO when required by law.

The ALPR Program Administrator shall prepare the annual report required by RCW 10.130.070, beginning no later than December 1, 2027, and shall ensure it is made conspicuously available on the Department or City website.

The report shall include, as applicable:

- The number of traffic stops and arrests assisted by ALPR data.
- The number and types of criminal prosecutions resulting from arrests assisted by ALPR data.
- The number of stolen vehicles and stolen plates recovered with ALPR assistance.
- The number of requests for data preservation, disclosure orders, intergovernmental data sharing or direct access, and judicial-warrant-related data sharing or access, including the identity of each requesting or receiving agency where required.
- Policy changes and results of APD's internal audit.
- The annual number of license plate images collected, productive searches, and alerts.
- The locations of fixed ALPR cameras.

For policy modifications or repeals occurring after December 1, 2026, APD shall provide required notice and the relevant policy materials to the AGO within 60 days, as required

by RCW 10.130.070. APD shall review this policy upon publication of the AGO model policy and, by December 1, 2027, take required action to align the policy with the model policy or submit a lawful explanation of any departure.

708.12 VIOLATIONS

Members who violate this policy may be subject to discipline, loss of ALPR access, criminal investigation or referral, civil liability, and other consequences provided by law. Willful or intentional misuse of ALPR systems or ALPR data may constitute a criminal offense. Evidence obtained in violation of applicable ALPR law may be subject to exclusion.

Members shall promptly report suspected misuse, unauthorized access, prohibited sharing, retention failure, security incident, or other material compliance concern to a supervisor or the ALPR Program Administrator.

708.13 RECORDS AND REFERENCES

Legal References: RCW Chapter 10.130; RCW 42.56.240; RCW 42.56.904; applicable Washington State Archives records-retention schedules; and other applicable federal, state, and local law.