

Automated License Plate Readers (ALPR)

345.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the deployment, use, maintenance, data handling, and oversight of Automated License Plate Reader (ALPR) systems by the Centralia Police Department in full compliance with Washington State law, including Engrossed Substitute Senate Bill 6002 (ESSB 6002, Chapter 239, Laws of 2026, effective March 30, 2026; the "Driver Privacy Act"), the Washington Association of Sheriffs and Police Chiefs (WASPC) ALPR Interim Guidance (May 29, 2026), and existing department policies, particularly Policy 321 (Information Technology Use) and Policy 804 (Protected Information).

This policy ensures that ALPR technology is used only for legitimate law enforcement and public safety purposes while protecting individual privacy, civil liberties, and constitutional rights. It applies to all members who operate, access, maintain, or oversee ALPR systems or data.

Until the Attorney General's Office (AGO) publishes its Model Policy (expected July 1, 2027), this policy incorporates the requirements of ESSB 6002 and follows the practical interpretations and recommendations in the WASPC Interim Guidance. Any future AGO Model Policy will supersede or supplement this policy as required.

345.2 DEFINITIONS

The following definitions apply (drawn from ESSB 6002 §2 and WASPC Interim Guidance):

- **Agency:** Any state or local agency as defined in ESSB 6002.
- **ALPR Data:** All data collected by an ALPR system, including GPS coordinates, location, date/time, speed, photograph, license plate number, vehicle characteristics, or other identifying information. Does not include audio/video from body-worn or dashboard cameras unless converted/indexed by license plate or used for tracking.
- **ALPR System:** Any system, software, or algorithm (fixed or mobile) that converts images of license plates into computer-readable data. Excludes certain traffic safety cameras and toll systems as specified in ESSB 6002.
- **Audit Trail Data:** Records of who accesses/uses the system, when, how, purpose (including offense type), case number, camera location, exports, downloads, and sharing. Retained for at least two years.
- **Sensitive Locations** (prohibited collection zones per ESSB 6002 §3(4)): Facilities providing protected health care services (gender-affirming treatment or reproductive health care per chapter 7.115 RCW), facilities conducting immigration matters (per RCW 19.154.020), elementary and secondary schools (consistent with RCW 9.41.280 premises), places of worship (locations primarily used for regular religious worship and controlled by a religious organization), courts (per RCW 2.28.300), and food banks (as "distributing organizations" per RCW 69.80.020). "Facilities" are limited to the building(s) used for these purposes and immediately adjacent parking lots primarily or exclusively used for them. "Premises," "immediate surroundings," and "access to or from" are interpreted per ordinary meaning and WASPC guidance (detailed in §345.6).

Automated License Plate Readers (ALPR)

- Other terms as defined in ESSB 6002, WASPC guidance, Policy 321, and Policy 804.

345.3 POLICY

It is the policy of the Centralia Police Department to:

- Use ALPR technology only when it supports legitimate law enforcement purposes authorized by ESSB 6002 (e.g., stolen vehicles, missing/endangered persons, felony/gross misdemeanor investigations or warrants, parking enforcement where authorized).
- Strictly prohibit use for immigration enforcement/investigation, protected health care services, or monitoring protected First Amendment/Washington Constitution activities.
- Never collect ALPR data on the premises, immediate surroundings, or access to/from sensitive locations.
- Maintain strict data retention limits (generally no longer than 21 days unless extended by court order, warrant, or specific exception in ESSB 6002).
- Ensure all data is treated as protected information consistent with Policy 804 and CJIS requirements.
- Register all ALPR systems with the AGO as required.
- Adopt and maintain written policies, documented training, and robust audit processes.
- Conduct annual internal audits and submit required reports.
- Promote public awareness of ALPR use.

ALPR data, images, and metadata are department property and shall be handled as confidential criminal intelligence/investigative information. A positive ALPR match alone does **not** constitute reasonable suspicion for a stop; officers must develop independent reasonable suspicion or visually confirm and verify via authorized databases.

345.4 ADMINISTRATION, REGISTRATION, AND OVERSIGHT

The Chief of Police (or designee) is the ALPR Program Administrator. Responsibilities include:

- Overseeing deployment, maintenance, vendor contracts, and compliance.
- Maintaining an inventory of all ALPR hardware, software, cameras (fixed/mobile), and associated databases.
- Coordinating with vendors to ensure technical controls prevent unauthorized sharing (especially to federal immigration enforcement).
- Ensuring compliance with Policy 321 (IT Use) for all system access, logging, and security.

345.5 AUTHORIZED USES

ALPR use is strictly limited to the purposes authorized under ESSB 6002 §3(2). The Centralia Police Department may use ALPR systems and data only for the following:

Centralia Police Department

Policy Manual

Automated License Plate Readers (ALPR)

(a) **Comparison Against Authorized Databases** ALPR data may be compared against the following databases for authorized law enforcement purposes:

- Washington State Department of Licensing records;
- State criminal justice information system records;
- Federal Bureau of Investigation records related to kidnappings and missing persons;
- National Center for Missing and Exploited Children records; and
- Washington state missing persons lists.

(b) **Investigations Involving Specific Vehicle-Related Matters** ALPR data may be used in connection with investigations where a vehicle has been:

- Determined to be stolen;
- Associated with a missing or endangered person;
- Registered to an individual who is related to or involved in a **felony or gross misdemeanor case**; or
- Registered to an individual who has an outstanding **felony or gross misdemeanor warrant**.

(c) **Parking Enforcement** Where the department is authorized by local ordinance or law, ALPR data may be used to enforce parking restrictions or to identify vehicles subject to impoundment or immobilization, provided the data is limited to plates associated with those enforcement actions.

(d) **Transportation and Commercial Vehicle Purposes (Limited)** ALPR data may be used by authorized transportation agencies for real-time traffic information, traffic modeling/studies, or enforcement of commercial vehicle requirements at designated Washington State Patrol sites, subject to the specific retention limits in ESSB 6002.

Important Limitations

- A positive ALPR match or "hit," by itself, does **not** constitute reasonable suspicion to conduct a traffic stop or detention. Officers must develop independent reasonable suspicion or visually confirm the match and verify it against one of the authorized databases listed above before taking enforcement action.
- ALPR data shall **not** be used for general investigative fishing expeditions, misdemeanor-only matters (except as expressly authorized for parking enforcement or specific database comparisons), or any purpose not listed in this section.
- All use must comply with the sensitive location prohibitions in §345.6 and the data retention and sharing rules in §345.7.

345.6 PROHIBITED USES AND SENSITIVE LOCATIONS

It is **unlawful** to:

- Use ALPR for immigration investigation or enforcement.

Automated License Plate Readers (ALPR)

- Use for protected health care services or to track/monitor protected constitutional activities.
- Collect data on the premises or immediate surroundings/access to or from sensitive locations (see definitions).

Interpretation of Sensitive Location Prohibitions (per WASPC Interim Guidance):

Agencies must conduct site-specific due diligence for fixed cameras and document it. For mobile/vehicle-mounted ALPRs, vendors should geofence to public rights-of-way only. "Premises" and "facilities" are not fully synonymous; "facilities" is narrower. Collection is prohibited in areas on the premises/attached parking lots, recording ingress/egress, or directly around buildings used for the listed sensitive purposes. ALPR may capture images beyond computer-readable data, but only computer-readable license plate data is governed by the law.

A vehicle on a public right-of-way turning into a sensitive location may trigger the prohibition—human review of context (photo + location) is required before using data in investigations or prosecutions.

345.7 DATA COLLECTION, RETENTION, SHARING, AND ACCESS

- **Collection:** Only as authorized. Positive matches require independent verification.
- **Retention:** Generally # 21 days unless extended by valid court order/warrant/subpoena for felony/gross misdemeanor cases (delete at case conclusion per records retention schedule) or specific exceptions. Parking enforcement data deleted no later than 12 hours after final disposition. Audit trail data retained # 2 years.
- **Sharing/Access:** Prohibited except as required in judicial proceedings or authorized inter-agency sharing among registered agencies. No direct access by third parties except for authorized vendor support. Private ALPR data requires a probable cause warrant. Data is generally exempt from Public Records Act requests (with limited research exceptions). Vendors must have controls preventing unauthorized access/sale/sharing.
- All access, queries, exports, and sharing must be logged in audit trails (who, when, purpose, case number, etc.).
- Comply fully with Policy 804 (Protected Information) and Policy 321 (IT Use) for security, access controls, and logging.

345.8 AUDITS, ACCOUNTABILITY, AND TRAINING

- Maintain comprehensive audit trail data for # 2 years.
- Conduct annual internal audits of all access/use, retention/purging compliance, and policy adherence.
- All personnel who access, operate, or use ALPR systems must complete documented training on this policy, ESSB 6002, WASPC guidance, sensitive locations, privacy protections, and system operation before use. Training records must be maintained.

Automated License Plate Readers (ALPR)

- The ALPR Program Administrator will ensure ongoing training and updates.

345.9 ANNUAL REPORTING AND PUBLIC AWARENESS

The department shall submit required annual reports on ALPR practices and usage to the appropriate legislative committees and post them (along with this policy) on the department's public website, with a link provided to the AGO. Reports must include required elements per ESSB 6002 §7.

Prior to or coincident with any new ALPR deployment or significant change, the department will promote public awareness.