

Automated License Plate Reader (ALPR) / Flock Safety System

Data Access and Information Sharing Policy

POL-53-1 PURPOSE.

The purpose of these policies is to establish clear standards for the lawful and transparent use of Automated License Plate Reader (ALPR) systems by the Whitman County Sheriff's Office. This policy ensures compliance with Washington State law, including SB 6002, and protects privacy, civil liberties, and constitutional rights of the public.

POL-53.2 DEFINITIONS.

2.1 Automated License Plate Reader (ALPR) System

A system of one or more cameras and associated software that automatically captures license plate numbers or vehicle characteristics and compares them to databases.

2.2 ALPR Data

Any data or metadata captured, generated, or derived from an ALPR system, including images, plate numbers, GPS coordinates, timestamps, alerts, and audit logs.

2.3 Direct Access

The ability to log into, query, retrieve, or export ALPR data without Department supervision.

2.4 Protected Facilities

Elementary and secondary schools, places of worship, courts, food banks, facilities providing protected health care services, and facilities conducting immigration matters, including their parking areas and immediate surroundings. All Automated License Plate Reader (ALPR) cameras utilized by the Whitman County Sheriff's Office will be deployed exclusively in fixed locations and will not be used in a mobile capacity.

2.5 Constitutionally Protected Activities

Activities protected by the U.S. or Washington Constitutions, including speech, association, and religious exercise.

2.6 Bona Fide Research

Research meeting the requirements of RCW 42.48, including de-identification and approval by the Sheriff.

POL-53.3 AUTHORIZED USES.

Personnel shall use ALPR systems **only** for the following purposes:

3.1 Criminal Investigations

ALPR systems may be used to compare captured data with:

(a) Databases maintained by federal or Washington State agencies, including:

- Department of Licensing
- State Criminal Justice Information System
- FBI Kidnappings and Missing Persons List
- National Center for Missing and Exploited Children
- Washington Missing Persons List

(b) License plates or vehicle characteristics entered into a Department or State ALPR database when an officer determines they are relevant and material to an investigation involving:

- A stolen vehicle;
- A missing or endangered person;
- An outstanding felony or gross misdemeanor warrant;
- A felony or gross misdemeanor.

The officer's determination shall be documented with a case number and placed in the associated case file.

3.1 Real-Time Alerts

Real-time alerts may be generated **only** for the categories listed in Section 3.1.

3.2 Data Ownership

The Department is the legal owner of all ALPR data collected by its systems.

POL-53.4 PROHIBITED USES.

Personnel shall not access, operate, or use ALPR systems or ALPR data as follows.

4.1 Unauthorized Investigations.

Personnel shall not access, operate, or use ALPR systems or ALPR data for any investigative purpose not listed in Section 3.

4.2 Immigration, Health Care, or Constitutionally Protected Activities.

Personnel shall not access, operate, or use ALPR systems or ALPR data:

- To investigate or enforce immigration laws;
- To identify, track, or monitor individuals seeking or providing protected health care services;
- To track or monitor constitutionally protected activities.

4.3 Protected Facilities.

Personnel shall not access, operate, or use ALPR systems or ALPR data to collect ALPR data on the premises, immediate surroundings, or access routes to or from protected facilities, including parking areas.

4.4 Private ALPR Data.

Personnel shall not access, operate, or use ALPR systems or ALPR data to obtain privately held ALPR data except pursuant to a valid, court-issued probable-cause warrant.

4.5 Unauthorized Sharing.

Personnel shall not access, operate, or use ALPR systems or ALPR data to disclose, share, or permit access to ALPR data except as authorized in Section 6.

4.6 Direct Access.

Personnel shall not access, operate, or use ALPR systems or ALPR data to provide direct access to any external entity unless expressly authorized by the Sheriff.

4.7 Database Integrity.

Personnel shall not access, operate, or use ALPR systems or ALPR data to use comparison databases that are not updated at least once every 24 hours.

4.8 Commercialization.

Personnel shall not access, operate, or use ALPR systems or ALPR data to sell, lease, rent, or otherwise monetize ALPR data.

4.9 Secondary Use.

Personnel shall not access, operate, or use ALPR systems or ALPR data to use ALPR data collected for one purpose for any other purpose.

POL-53.5 DATA RETENTION.

5.1 Default Retention

ALPR data shall not be retained longer than **21 days**, except as provided below.

5.2 Exceptions

Retention beyond 21 days is permitted only when:

(a) Warrants and Court Orders

Data retained pursuant to a valid warrant, subpoena, or court order shall be deleted at the conclusion of the case per the applicable retention schedule.

(b) Parking Enforcement

Data may be retained until **12 hours after final disposition** of the parking case, including appeals.

(c) Traffic Studies

Data may be retained for up to **30 days**.

(d) Commercial Vehicle Enforcement

Data may be retained for up to **6 months**.

(e) Evidence of Unlawful Conduct

Data may be retained as long as needed as evidence of conduct described in Section 3.1(b).

5.3 Prohibition on Secondary Use

Data collected for one purpose may not be used for any other purpose.

POL-53.6 ACCESS, SHARING, AND DISCLOSURE.

6.1 Internal Access

Access is limited to authorized personnel with a documented need consistent with these policies.

6.2 External Sharing

ALPR data may be shared only:

- (a)** As required in a judicial proceeding;
- (b)** Pursuant to a valid court order, warrant, or subpoena;
- (c)** In discovery under applicable court rules;

(d) For bona fide research under RCW 42.48, with all data de-identified and approval by the Sheriff.

6.3 Prohibited Sharing

ALPR data shall not be shared with:

- Immigration enforcement agencies;
- Any entity for commercial purposes;
- Any entity seeking direct access unless authorized by the Sheriff.

POL53.7 PUBLIC RECORDS ACT.

ALPR data is exempt from disclosure under the Public Records Act, chapter 42.56 RCW, except for bona fide research under RCW 42.48.

Audit trail data may be subject to disclosure, but unique identifiers must be redacted.

POL-53.8 AUDIT TRAILS AND INTERNAL CONTROLS.

8.1 Required Audit Logs

The Department shall maintain audit logs documenting all access to the ALPR system, including:

- Username and affiliated agency;
- Date and time of access;
- Query data elements;
- Purpose of access, including offense type;
- Associated call for service or case number;
- Camera locations accessed;
- All exports, downloads, or sharing of ALPR data;
- Vendor-generated audit logs.

8.2 Retention

Audit logs shall be retained for **two years**.

8.3 Use of Audit Logs

Query data elements retained as audit logs may be used **solely for auditing** and may not be searched, analyzed, compiled, or indexed for investigative purposes.

8.4 Annual Internal Audit

The Department shall conduct an internal audit at least once per year to review:

- All access to and use of the ALPR system;
- Compliance with retention, purging, and sharing requirements.

8.5 Vendor Requirements

Vendor contracts shall require:

- Access to all audit logs;
- Ability to export logs;
- Prohibition on vendor retention or secondary use;
- Immediate reporting of any breach or unauthorized access.

POL-53.9 TRAINING.

All personnel with access to ALPR systems or data shall receive annual training on:

- These policies;
- SB 6002 requirements, as enacted or hereafter amended;
- Privacy and civil liberties protections;
- Audit and reporting obligations.

POL-53.10 ANNUAL REPORTING.

By **December 1** of each year, the Department shall publish a report including:

1. Number of matches resulting in traffic stops or arrests, and resulting prosecutions;
2. Number of stolen vehicles or plates recovered;
3. Number of preservation requests and disclosure orders received;
4. Number of times ALPR or audit data was shared with another government agency, including agency names;
5. Number of times ALPR data was accessed pursuant to a judicial warrant;
6. Policy changes affecting ALPR data collection, retention, access, or sharing;
7. Results of internal audits;
8. Total annual number of ALPR reads, searches, hits, and alerts;
9. Locations of ALPR cameras;
10. Any known or suspected unauthorized access, breach, or attempted breach.