

14.03.000 USE OF AUTOMATED LICENSE PLATE READER (ALPR) SYSTEMS

14.03.005

PURPOSE AND SCOPE: 06/26

The purpose of this policy is to establish clear, consistent, and legally compliant standards governing the use, management, and oversight of Automated License Plate Reader (ALPR) systems and ALPR data by the King County Sheriff's Office (KCSO). This policy ensures that ALPR technology is used in a manner that enhances public safety, supports legitimate law enforcement objectives, and protects the privacy and civil liberties of the public, consistent with the requirements of [ESSB 6002](#) (codified in Title 10 RCW).

This policy applies to all KCSO personnel who operate ALPR systems, access ALPR data, or participate in the administration, auditing, or oversight of ALPR-related functions. Contract agencies that independently operate ALPR systems for parking-enforcement or other authorized non-law enforcement purposes remain responsible for compliance with statutory requirements and any King County laws or policies governing KCSO operations applicable to their systems.

14.03.010

DEFINITIONS: 06/26

For purposes of this policy, the following definitions apply:

Automated License Plate Reader (ALPR): A technology that uses cameras and computer algorithms to automatically capture images of license plates, convert the images into alphanumeric characters, and compare the resulting data to lawfully authorized databases or hotlists.

ALPR System: The complete set of hardware, software, databases, networks, and administrative controls used to capture, store, query, analyze, or share ALPR data. This includes fixed, mobile, and portable ALPR units operated by KCSO or contract agencies.

ALPR Data: All data collected or generated by an ALPR system, including, but not limited to:

1. Global positioning system coordinates
2. Location
3. Date and time of capture
4. Speed of travel
5. Photograph
6. License plate number
7. Automobile characteristics
8. Other identifying information

ALPR data does not include images or video that do not contain a license plate or are not processed through ALPR analytics.

ALPR Hit / Alert: A system-generated notification indicating that a captured license plate number matches a plate number on a lawfully authorized hotlist. A hit is not confirmation of a match and must be verified by a deputy prior to any enforcement action.

Hotlist: A list of license plate numbers and/or vehicle characteristics associated with specific, legally authorized investigative purposes, including stolen vehicles, wanted persons (gross misdemeanor or felonies only), missing or endangered persons, or court-ordered entries. Hotlists may also include data from the following authorized databases:

1. WSP Criminal Justice Information System (CJIS)
2. Washington Department of Licensing (DOL)

3. FBI Kidnappings and Missing Persons List
4. National Center for Missing and Exploited Children List
5. Washington Missing Persons List

Hotlists must be maintained by an authorized agency and meet the requirements of ESSB 6002.

Authorized Use: Any use of ALPR systems or ALPR data that is expressly permitted under ESSB 6002 and this policy, including specific public safety, criminal investigation, or missing-person-related purposes.

Prohibited Use: Any use of ALPR systems or ALPR data that is expressly forbidden by ESSB 6002 or this policy, including but not limited to: immigration enforcement, civil enforcement, warrantless surveillance, or any use not tied to a statutorily authorized purpose.

Retention Period: The maximum length of time ALPR data may be stored before mandatory deletion, as defined by ESSB 6002 and this policy. Retention periods apply to both KCSO-generated data and data received from partner agencies.

Access: The ability to view, query, retrieve, analyze, or export ALPR data or system logs. Access is limited to personnel with a demonstrated need and documented authorization.

Audit Log / Audit Trail: A system-generated record documenting all access, queries, searches, modifications, or sharing of ALPR data. Audit logs must be maintained in accordance with ESSB 6002 and are subject to periodic review.

Audit Trail Data: All forms of data collected or generated by an ALPR system that identify how the system is accessed or used, including who accessed the system, when, and for what purpose.

Vendor: Any third-party company that provides ALPR hardware, software, cloud storage, or system administration services. Vendors must comply with all statutory requirements, including data security, access controls, and audit capabilities.

Reasonable Suspicion (RS): A specific, articulable set of facts that would lead a trained law enforcement officer to believe that criminal activity is occurring, has occurred, or is about to occur. RS is required for certain ALPR data queries under ESSB 6002.

Contract Agency ALPR Administrator: A designated representative of a contract agency (e.g., contract city or other contract entity) that owns or operates ALPR systems within its jurisdiction and is responsible for ensuring compliance with this policy and ESSB 6002.

KCSO ALPR Program Administrator: The Sheriff-designated individual responsible for oversight of ALPR operations, compliance, training, auditing, and coordination with contract agencies and vendors.

Vehicle Characteristics: Descriptive attributes of a vehicle including make, model, color, body style, or other identifying features that may be entered into an ALPR database upon an officer's determination that they are material to an authorized investigation under this policy.

14.03.015

POLICY: 06/26

It is the policy of the King County Sheriff's Office to use Automated License Plate Reader (ALPR) systems in strict compliance with ESSB 6002 and all other applicable federal, state, and local laws. ALPR systems may be used only for authorized law enforcement and public safety purposes, and ALPR data shall be collected, accessed, retained, shared, and deleted solely as permitted or required by statute and by the provisions of this policy.

KCSO will implement appropriate administrative, technical, and supervisory controls to ensure that ALPR operations protect individual privacy rights, prevent unauthorized access or misuse, and maintain the integrity and security of ALPR systems and associated data. All personnel with access to ALPR systems or data are required to adhere to this policy and to complete all training required for safe and lawful operation.

Contract agencies that operate their own ALPR systems independent of KCSO are responsible for ensuring that their operations comply with ESSB 6002, including statutory requirements for authorized use, data retention, database updates, and system auditing.

14.03.020

DATA COLLECTION: 06/26

KCSO uses ALPR data only for authorized law enforcement purposes and in compliance with ESSB 6002. Data collection and use must be limited to system generated-information necessary for legitimate public safety functions and conducted in a manner that protects individual privacy. This section outlines what ALPR data may be collected, where collection is prohibited, and the limitations placed on ALPR use.

1. Authorized Data Collection:

Prior to deployment of any fixed ALPR camera, the ALPR Program Administrator shall complete and document a site-specific due-diligence review to ensure the system will not collect ALPR data on the premises, immediate surroundings, or access to or from any sensitive locations as described in ESSB 6002.

This review shall consider whether nearby facilities provide protected health care, conduct immigration matters, operate as elementary or secondary schools, places of worship, courts, or food banks. Documentation of this review shall be retained with system records.

- a. KCSO ALPR systems may collect only the following information:
 - i. License plate images.
 - ii. Alphanumeric plate reads.
 - iii. Vehicle characteristics.
 - iv. Date and time of capture.
 - v. GPS coordinates or other system-generated location data.
 - vi. Camera or device identifier.
 - vii. System metadata necessary for auditing, troubleshooting, or validating system performance.
- b. No additional personally identifiable information (PII) may be collected unless it is incidentally captured in the background of an ALPR image.
- c. Deputies shall not use ALPR systems to intentionally collect images of vehicle occupants, pedestrians, or non-vehicle related activity.

2. Prohibited Collection Locations:

- a. ALPR systems shall not collect data on the premises, immediate surroundings, or access to or from:
 - i. Facilities providing protected health care.
 - ii. Facilities conducting immigration matters.
 - iii. Elementary and secondary schools.
 - iv. Places of worship.
 - v. Courts.
 - vi. Food banks.

3. Collection Limitations:

- a. ALPR data may be collected only through:
 - i. Fixed ALPR cameras.
 - ii. Portable ALPR units deployed for authorized public safety purposes.
- b. ALPR systems shall not be used for:
 - i. General surveillance.
 - ii. Monitoring individuals or groups based on protected characteristics.
 - iii. Civil, code, or administrative enforcement.
 - iv. Immigration enforcement; or
 - v. Any purpose not expressly authorized under ESSB 6002 or this policy.

4. Verification of ALPR Hits:

- a. All ALPR “hits” or alerts must be visually verified by a deputy before any enforcement action is taken. Deputies must confirm:
 - i. The plate characters.
 - ii. The plate state.
 - iii. The vehicle make, model, and color (when available); and
 - iv. The validity and current status of the hotlist entry.
- b. A system alert alone does not constitute reasonable suspicion or probable cause.

14.03.025

DATA RETENTION: 06/26

KCSO retains ALPR data only for the time periods permitted by ESSB 6002 and this policy. All ALPR data must be managed in a manner that minimizes privacy risks, prevents unauthorized retention, and ensures timely deletion consistent with statutory requirements.

1. Standard Retention Period:

- a. ALPR data collected by KCSO shall be retained only for 21 days.
- b. Unless otherwise required by law, ALPR data must be automatically deleted at the end of the statutory retention period.
- c. Retention periods apply to:
 - i. KCSO generated ALPR data.
 - ii. ALPR data received from contract agencies; and
 - iii. ALPR data shared with KCSO by partner agencies.

2. Parking Enforcement Retention:

- a. KCSO does not operate or retain ALPR data used for parking enforcement.
- b. Contract agencies that operate ALPR systems for this purpose, independent of KCSO, are responsible for ensuring their use complies with ESSB 6002, including the requirement to delete parking enforcement- ALPR data within 12 hours of final case disposition.

3. Extended Retention for Active Investigations:

- a. ALPR data may be retained beyond 21 days only when:
 - i. Retained pursuant to a valid court issued probable cause warrant, subpoena, or court order; or
 - ii. Retained as evidence of specific unlawful conduct enumerated in Sec. 3(2)(a) (stolen vehicle, missing/endangered person, felony/gross misdemeanor, or warrant).

4. Prohibited Retention:

- a. ALPR data shall not be retained for:
 - i. Intelligence gathering unrelated to a specific criminal investigation.
 - ii. Monitoring individuals, groups, or locations without a lawful investigative purpose.
 - iii. Predictive policing or algorithmic forecasting; or
 - iv. Any purpose prohibited by ESSB 6002 or KCSO policy.

5. Automatic Deletion:

- a. The ALPR system must be configured to automatically delete data upon expiration of the retention period. Manual deletion is permitted only when:
 - i. Required to correct system errors.
 - ii. Ordered by the ALPR Program Administrator; or
 - iii. Required by law or court order.
- b. All deletions must be logged in the system audit trail.

6. Audit and Verification:

- a. The ALPR Program Administrator shall conduct periodic audits to verify:
 - i. Compliance with retention timelines.
 - ii. Proper functioning of automated deletion processes; and
 - iii. Absence of unauthorized data storage or exports.
- b. Audit results shall be documented and made available to the Sheriff, contract agencies, and oversight entities as required.

14.03.030

ACCESS AND USE: 06/26

Department personnel may access and use ALPR systems and ALPR data only for statutorily authorized law enforcement purposes and in accordance with the controls, limitations, and verification requirements established in this policy and ESSB 6002.

1. Authorized Access:

- a. Access to ALPR systems and ALPR data is limited to personnel who:
 - i. Have a legitimate, statutorily authorized law enforcement purpose.
 - ii. Have completed required ALPR training; and
 - iii. Have been granted system credentials by the ALPR Program Administrator.
- b. All databases and hotlists used by ALPR systems must be checked for available updates and applied at least once every 24 hours (these updates may occur automatically through vendor managed synchronization or through a manual administrative process).

2. Authorized Use:

- a. ALPR systems and ALPR data may be used only for the following purposes:
 - i. Locating stolen vehicles or vehicles associated with felony or gross misdemeanor crimes.
 - ii. Locating vehicles associated with missing or endangered persons.
 - iii. Locating vehicles registered to an individual with an outstanding felony or gross misdemeanor warrant; or
 - iv. Locating vehicles related to or involved in a felony or gross misdemeanor.

3. Prohibited Use:

- a. ALPR systems and ALPR data shall not be used for:
 - i. Civil enforcement (code or administrative violations).
 - ii. Immigration enforcement.
 - iii. General surveillance or monitoring of individuals, groups, or locations.
 - iv. Predictive policing or algorithmic forecasting.
 - v. Personal, political, or non-law enforcement purposes; or
 - vi. Any use not expressly authorized by ESSB 6002 or this policy.

4. Query Requirements:

- a. Personnel must document the purpose of each ALPR query.
- b. Authorized professional staff may perform ALPR queries or enter data only after a commissioned officer has made and documented an individualized determination that the license plate number or vehicle characteristics are relevant and material to an investigation authorized under ESSB 6002.
 - i. Such determination must be recorded prior to any action taken by professional staff.

- c. When documenting the purpose for accessing or querying ALPR data, personnel must either:
 - i. Select a preset authorized crime established in the system; or
 - ii. Record the specific RCW title, chapter, section, and offense name associated with the investigation (e.g., RCW 9A.52.025 - Residential Burglary).
- d. The specific offense must be identified prior to any ALPR query.
- e. Queries must be tied to a CAD or case number when applicable.
 - i. All queries are logged and subject to audit.

5. Enforcement Actions:

- a. Before taking any enforcement action based on an ALPR alert, deputies must recognize that an ALPR system match, by itself, does not establish reasonable suspicion to stop a vehicle.
- b. Deputies are required to develop independent reasonable suspicion or immediately verify the information by visually confirming that the observed license plate matches the plate displayed in the ALPR alert.
- c. Deputies must confirm:
 - i. Plate characters and state.
 - ii. Vehicle description.
 - iii. Validity of the hotlist entry.

14.03.035

DATA SHARING: 06/26

Sharing of ALPR data is strictly limited to the circumstances authorized by ESSB 6002 and this policy.

KCSO may only share specific, actionable, and timely ALPR information (such as a license plate number, vehicle description, photograph, or direction of travel) with another law enforcement agency when necessary to locate a specific vehicle for a legitimate public safety purpose. Such sharing does not constitute providing direct system access and must not include time-series or comprehensive ALPR datasets.

1. Authorized Sharing:

- a. ALPR data may only be shared:
 - i. As required in a judicial proceeding.
 - ii. With other law enforcement agencies authorized to use an ALPR system under ESSB 6002.

2. Prohibited Sharing:

- a. ALPR data shall not be shared with:
 - i. Agencies engaged in civil or administrative enforcement.
 - ii. Federal immigration authorities.
 - iii. Private entities, except approved vendors providing system support; or

iv. Any entity not authorized to use ALPR systems under ESSB 6002.

b. KCSO shall not sell, lease, rent, or purchase ALPR data or audit trail data.

3. Secondary Dissemination:

a. Agencies receiving ALPR data are prohibited under ESSB 6002 from further disseminating that data to any other entity.

4. Privately held ALPR data:

- a. KCSO may obtain privately held ALPR data only pursuant to a valid, court-issued probable cause warrant.
- b. Voluntary or consent-based sharing of ALPR data by private businesses, homeowners, or other private parties is not an authorized basis for obtaining privately held ALPR data.
- c. Members shall not solicit, accept, access, or act on privately held ALPR data absent a court-issued probable cause warrant.
- d. If unsolicited privately held ALPR data is received, KCSO shall obtain a “nunc pro tunc” warrant before reviewing or acting upon the data.
- e. Any existing informal arrangements with private parties for voluntary ALPR data sharing are superseded by this requirement.
- f. Photographs and/or video provided by community members as evidence are not considered ALPR data and there is no requirement to screen such submissions for potential ALPR system use.

5. Documentation:

- a. All data sharing must be logged, including:
 - i. Requesting agency.
 - ii. Purpose of the request.
 - iii. Data provided; and
 - iv. Authorizing personnel.

6. Public Records Act:

- a. ALPR data is exempt from disclosure under the Public Records Act, except for bona fide research without individually identifiable information.

14.03.040

AUDIT AND OVERSIGHT: 06/26

KCSO oversees ALPR operations through required audits, documentation, and administrative controls to ensure lawful use and full compliance with ESSB 6002.

1. Program Oversight:

- a. The ALPR Program Administrator is responsible for:
 - i. Ensuring compliance with ESSB 6002 and this policy.
 - ii. Managing system access.
 - iii. Coordinating with contract agencies and vendors; and
 - iv. Maintaining documentation, training records, and audit results.

2. Audit Requirements:

- a. The ALPR Program Administrator shall conduct periodic audits to ensure:
 - i. Proper use of ALPR systems and data.
 - ii. Compliance with access controls and query documentation.
 - iii. Adherence to retention and deletion requirements.
 - iv. Accuracy and completeness of audit logs; and
 - v. Compliance with vendor obligations.
- b. Audits must occur at least annually, with interim reviews as needed.

3. Audit Trail Data Requirements:

KCSO shall require ALPR vendors to implement functionality capable of logging all exports, downloads, or sharing of ALPR data as required under ESSB 6002 audit-trail provisions. KCSO shall work with vendors to ensure timely development and deployment of these capabilities.

- a. Audit trail data must include:
 - i. Username/identity of person accessing.
 - ii. Date/time of access.
 - iii. Query data elements.
 - iv. Purpose and offense type.
 - v. Case number.
 - vi. Camera location.
 - vii. All exports/downloads/sharing.
 - viii. Vendor-generated audit data.
- b. Audit trail data must be retained for at least two years.
 - i. Access and query logs maintained under the recordkeeping requirements of this policy shall be retained for a minimum of five (5) years.
 - ii. Audit trail data documenting system access and use shall be retained for a minimum of two (2) years
- c. Query data elements retained in audit logs may be used only for auditing and may not be searched or analyzed for investigative purposes.

4. Supervisor Responsibilities:

- a. Supervisors shall:
 - i. Review ALPR use by personnel under their command.
 - ii. Ensure queries are tied to authorized purposes; and
 - iii. Address misuse or policy violations promptly.

5. Reporting and Corrective Action:

- a. Audit findings shall be documented and reported to the Sheriff or designee. Violations may result in:
 - i. Revocation of ALPR access.
 - ii. Corrective training.
 - iii. Administrative investigation; and/or
 - iv. Disciplinary action consistent with department policy.

14.03.045

ANNUAL REPORTING REQUIREMENT: 06/26

KCSO shall maintain transparency in its use of ALPR systems consistent with ESSB 6002, including making required summaries and audit information available to appropriate oversight bodies and the public.

By December 1, 2027, and annually thereafter, KCSO shall submit a report on its ALPR practices and system usage to the appropriate committees of the Legislature, and shall conspicuously post the report on the KCSO public website. The annual report shall include:

1. The number of matches that resulted in arrest and prosecution.
2. The number of stolen vehicles and stolen license plates recovered through use of the system.
3. The number of preservation requests and disclosure orders received.
4. The number of times that ALPR data or audit trail data was shared with or accessed by another governmental entity, and the identity of each such entity.
5. The number of times that ALPR data was shared or accessed pursuant to a judicial warrant.
6. Any changes in policy that affect data collection, retention period, access, or sharing.
7. Results from KCSO's internal audit of its ALPR system; and
8. The total annual number of ALPR reads, hits, matches, and alerts.

14.03.050

ATTORNEY GENERAL REGISTRATION AND POLICY SUBMISSION REQUIREMENTS: 06/26

KCSO shall only access and use data from systems where contract agencies have complied with the registration, policy submission, and public transparency requirements established under ESSB 6002.

1. **ALPR System Registration and Policy Updates:**
 - a. Within 180 days of the effective date of ESSB 6002 (September 25, 2026), contract agencies shall register all ALPR systems with the Washington Attorney General and certify that all ALPR use and training meet the requirements of the new law.
 - b. After December 1, 2026, KCSO shall submit notice and copies of any ALPR policies that are modified or repealed to the AGO within 60 days following such modification.
2. **Adoption of Model Policies and Reporting Requirements:**
 - a. By December 1, 2027, the King County Sheriff's Office (KCSO) shall adopt ALPR policies that are fully consistent with the model policies issued by the Washington State Attorney General's Office (AGO). Finalized policies shall be submitted to the AGO by this date.
 - b. KCSO, in collaboration with its contract agencies, shall submit the first annual ALPR report to the Legislature by December 1, 2027. This report will cover the preceding 12-month period (November 1 through October 31).
 - c. Contract agencies shall provide KCSO all required ALPR data, documentation, and compliance attestations no later than November 5 of each reporting year to ensure timely compilation, validation, and submission.

3. Public Awareness Measures:

- a. KCSO shall maintain an ALPR transparency webpage that includes the ALPR policy, plain-language explanations, examples of authorized uses, disclosures of prohibited uses, and required annual reports.

14.03.055

TRAINING: 06/26

All personnel who operate ALPR systems or access ALPR data must complete training before receiving system credentials, and that training must be documented and certified as required under ESSB 6002.

1. Training Content:

Training shall include, at a minimum:

- a. Proper system-use procedures, including user authentication, secure login practices, approved search parameters, documentation requirements, and steps for verifying that each ALPR query or action is tied to a lawful and authorized purpose.
- b. The lawful uses of ALPR systems as defined by ESSB 6002, including locating stolen vehicles, vehicles associated with missing or endangered persons, and vehicles involved in felony or gross misdemeanor investigations.
- c. The prohibited uses of ALPR systems, including any form of tracking protected activities, conducting immigration enforcement, or engaging in surveillance around sensitive locations.

2. Training Documentation:

- a. Completion of required training shall be documented and retained in accordance with KCSO training-record requirements.
- b. Personnel who fail to complete required training shall have ALPR access suspended until all training requirements are met.