

Automated License Plate Readers

428.1 PURPOSE AND SCOPE

Best Practice MODIFIED

The purpose of this policy is to provide guidance for the capture, storage, and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology.

The Department recognizes ALPR technology as a valuable law enforcement tool that enhances officer and public safety by assisting in the identification of stolen vehicles, locating missing or endangered persons, apprehending wanted individuals, and supporting criminal investigations.

The Department also recognizes the importance of protecting individual privacy and civil liberties. ALPR technology shall be used only for legitimate law enforcement purposes and in a manner that promotes accountability, transparency, and public confidence.

This policy establishes minimum operational requirements for Department personnel and is intended to ensure compliance with applicable federal and Washington State law governing ALPR systems.

428.1.1 DEFINITIONS

State MODIFIED

Definitions related to this policy include (Chapter 239, § 2, 2026 Laws):

Audit trail data - All forms of data collected or generated by an automated license plate reader system that identify how and when the system is accessed or used.

Automated license plate reader data (ALPR data) - Data collected by automated license plate reader systems including but not limited to global positioning system coordinates, location, date and time, speed of travel, photograph, license plate number, automobile characteristics, or other identifying information. "Automated license plate reader data" does not include audio or video recordings generated by an in-car or body-worn camera, unless such recordings are converted into computer-readable license plate characters or associated metadata, or are indexed, made searchable, or analyzed by license plate number, individual, vehicle, biometric identifier, or other unique identifier for the purpose of identifying, tracking, or reconstructing an individual's or vehicle's location.

Automated license plate reader system (ALPR) - A system, software, or computer algorithm, whether used independently or in combination with one or more mobile or fixed automated cameras, that is used to convert images of license plates into computer-readable data.

ALPR Alert - A notification generated when a captured license plate matches a license plate contained within an authorized law enforcement database or department-approved watch list. An ALPR alert is an investigative lead only and does not independently establish reasonable suspicion or probable cause for enforcement action.

Kennewick Police Department

Policy Manual

Automated License Plate Readers

Authorized User - A Department employee who has been approved by the Chief of Police or designee to access an ALPR system after successfully completing department-approved training.

Sensitive Locations - Sensitive locations include those protected under Washington State law, including but not limited to:

- Facilities providing protected health care services as described in Chapter 7.115 RCW; Facilities conducting immigration matters as defined in RCW 19.154.020; Elementary and secondary schools consistent with RCW 9.41.280; Places of worship, defined as locations primarily used for persons to regularly assemble for religious worship and maintained or controlled by a religious organization; Courts, consistent with the definition of court facilities contained in RCW 2.28.300; and Food banks or distributing organizations as defined in RCW 69.80.020.

428.2 POLICY

Best Practice **MODIFIED**

The policy of the Kennewick Police Department is to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public.

All data and images gathered by the ALPR are for the official use of this department. Because such data may contain confidential information, it is not open to public review.

The Kennewick Police Department shall use ALPR systems only for legitimate law enforcement purposes authorized by law.

The Department shall implement reasonable safeguards to ensure ALPR technology is used in a manner that protects individual privacy while supporting public safety and effective law enforcement operations.

Department personnel shall not use ALPR systems for personal reasons, curiosity, or any purpose unrelated to official duties.

All ALPR activity is subject to audit.

Authorized users should have no expectation of privacy regarding their use of department-operated ALPR systems.

428.3 ADMINISTRATION

State **MODIFIED**

All installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Administrative Services Division Commander. The Administrative Services Division Commander will assign members under their command to administer the day-to-day operation of the ALPR.

No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.

The Administrative Services Division Commander is responsible for:

Automated License Plate Readers

- (a) Maintaining compliance with applicable law.
- (b) Coordinating registration of Department ALPR systems.
- (c) Reviewing and approving user access.
- (d) Coordinating initial and refresher training.
- (e) Monitoring vendor compliance.
- (f) Conducting or coordinating required audits.
- (g) Ensuring data retention settings comply with applicable law.
- (h) Reviewing camera placement prior to deployment.
- (i) Maintaining required compliance documentation.
- (j) Coordinating required public reporting.
- (k) Reviewing this policy as necessary and recommending revisions as necessary.

428.4 ALPR CAMERA PLACEMENT

Agency Content

Prior to deployment of any fixed ALPR camera, the Department shall conduct and document a site-specific assessment to ensure the camera is not intentionally positioned to collect ALPR data from sensitive locations or their immediate surroundings.

The assessment shall consider camera orientation, field of view, nearby facilities, and whether the placement may capture vehicles entering or exiting sensitive locations. When feasible, camera placement and system configuration shall be adjusted to minimize the collection of data from such locations while preserving lawful collection from public rights-of-way.

Documentation shall be retained for compliance purposes.

428.5 MOBILE ALPR SYSTEMS

Agency Content

Mobile ALPR systems shall be operated in a manner that prohibits the collection of data from sensitive locations and their immediate surroundings.

Department personnel operating mobile ALPR systems shall avoid intentional collection of ALPR data from prohibited locations and shall immediately discontinue collection when prohibited collection is identified.

428.6 OPERATIONS

State MODIFIED

Reasonable suspicion or probable cause is not required before using an ALPR. Use of an ALPR is restricted to the following purposes (Chapter 239, § 3, 2026 Laws):

Kennewick Police Department

Policy Manual

Automated License Plate Readers

- (a) A comparison of ALPR data with data from databases maintained by the Washington 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, and the Washington missing persons list.
- (b) A comparison of ALPR data with data from a state or local government ALPR database if the officer performing the search documents that the license plate number or vehicle characteristics are relevant and material to an investigation of a vehicle that is stolen, associated with a missing or endangered person, registered to a person with an outstanding felony or gross misdemeanor warrant, or was involved in the commission of a felony or gross misdemeanor.
- (c) Enforcing parking restrictions.
- (d) Identifying vehicles in a database for impoundment or immobilization under a local ordinance, provided the database includes only license plates of vehicles subject to that ordinance.

An ALPR alert alone does not constitute reasonable suspicion to stop a vehicle. Before conducting a traffic stop, officers shall either (Chapter 239, § 3, 2026 Laws):

- Develop reasonable suspicion for the stop independent from the ALPR match.
- Immediately confirm visually that the license plate on the vehicle matches the image of the license plate displayed on the ALPR and confirm by other means that the license plate number appears in one of the databases described in this section.

428.6.1 PROHIBITED USE OF THE ALPR SYSTEM

State **MODIFIED**

Members shall not use or allow others to use the ALPR equipment or data for any unauthorized purpose, including (Chapter 239, § 3, 2026 Laws):

- (a) Investigating or enforcing federal immigration matters.
- (b) Assisting with out-of-state investigations regarding protected health care services under chapter 7.115 RCW (e.g., abortion services).
- (c) Tracking or otherwise monitoring activity protected by the state and federal constitutions (e.g., free speech, assembly, protest).
- (d) Collecting ALPR data from sensitive locations to include facilities that provide health care or conduct immigration matters as defined by RCW 19.154.020, elementary and secondary schools, places of worship, courts, or food banks.

The Kennewick Police Department shall not sell, lease, rent, or purchase ALPR data or audit trail data (Chapter 239, § 5, 2026 Laws).

428.7 CUSTOM WATCH LISTS

Agency Content

Authorized users who create custom watch lists must have determined that the license plate numbers are relevant and material to an investigation of a vehicle that is: Stolen; Associated with a missing or endangered person; Registered to an individual for whom there is an outstanding

Automated License Plate Readers

felony or gross misdemeanor warrant; or Related to or involved in a felony or gross misdemeanor investigation. Authorized users will include the following information in each custom watch list:

- Case number
- Offense category
- Investigative purpose
- Date of entry
- Authorized user entering the information

Authorized users must ensure the watch list is updated no less than once every 24 hours and should promptly remove entries that are no longer necessary.

428.8 SYSTEM ACCESS

Agency Content

Access to ALPR systems shall be restricted to authorized users who have completed department-approved training.

Each authorized user shall be assigned unique login credentials.

Employees shall not:

- (a) Share passwords.
- (b) Allow another individual to use their account.
- (c) Circumvent security controls.
- (d) Access ALPR data for personal reasons.

The Administrative Services Division Commander shall review user access permissions periodically and promptly remove or modify access when an employee:

Transfers assignments;
Separates from employment;
No longer requires access; or
Fails to comply with this policy.

428.9 TRAINING

Agency Content

The Department shall ensure that all personnel authorized to access or operate an ALPR system receive department-approved training prior to being granted access.

Training shall include, at a minimum:

- (a) Applicable federal and Washington law governing ALPR systems.
- (b) Department policy and procedures.
- (c) Privacy and civil liberties protections.

Automated License Plate Readers

- (d) Authorized and prohibited uses.
- (e) Proper operation of ALPR equipment and software.
- (f) Alert verification procedures.
- (g) Data retention and preservation requirements.
- (h) Data sharing restrictions.
- (i) Public records considerations.
- (j) Reporting suspected misuse.

The Administrative Services Division Commander shall ensure refresher training is provided as necessary to address changes in law, Department policy, technology, or identified deficiencies.

Authorized users whose ALPR access has been suspended due to misuse or noncompliance may be required to complete remedial training before access is restored.

The Department shall maintain records documenting completion of all required ALPR training.

428.10 DATA COLLECTION AND RETENTION

State **MODIFIED**

The Administrative Services Division Commander is responsible for ensuring systems and processes are in place for the proper collection and retention of ALPR data. Data will be transferred from vehicles to the designated storage in accordance with department procedures.

All stored ALPR data shall not be retained for more than 21 days unless it is (Chapter 239, § 4, 2026 Laws):

- (a) Retained pursuant to a warrant issued by a court in a felony or gross misdemeanor case.
- (b) Retained as permitted by court order in civil or criminal cases.
- (c) Reasonable to believe it will become evidence in a criminal or civil action or is subject to a discovery request, subpoena, or other lawful action to produce records. In those circumstances, the applicable data should be downloaded onto portable media and booked into evidence.
- (d) Retained for the purpose of parking enforcement, provided that the data is deleted within 12 hours of the final disposition of the enforcement case.

When no longer needed, ALPR data shall be deleted according to the established records retention schedule. Additional information regarding the access, storage, use, and sharing of ALPR data is addressed in Policy 805 - Protected Information and Public Safety Technology Data Governance.

428.11 ACCOUNTABILITY

State **MODIFIED**

Kennewick Police Department

Policy Manual

Automated License Plate Readers

All data will be closely safeguarded and protected by both procedural and technological means. All ALPR data collected by department-operated systems is the property of the Kennewick Police Department. The Kennewick Police Department will observe the following safeguards regarding access to and use of stored data:

- (a) All ALPR data downloaded to the mobile workstation and in storage shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date, and time.
- (b) Members approved to access ALPR data under these guidelines are permitted to access the data only for lawful purposes.
- (c) ALPR system audits shall be conducted annually at a minimum and include a review of all access to and use of the ALPR system and the Department's compliance with the data retention, purging, and sharing requirements of this policy (Chapter 239, § 8, 2026 Laws).
 - 1. Data elements used to query the ALPR and retained as audit trail data shall be used solely for auditing purposes and may not be searched, analyzed, compiled, or indexed for investigative purposes.
 - 2. Audit trail data shall be retained for two years and shall contain the information required by Chapter 239, § 8, 2026 Laws.
 - 3. Suspected misuse shall be promptly investigated.
 - 4. Confirmed misuse may result in the following to include but not limited to: Revocation of ALPR access; Remedial training; Disciplinary action up to and including termination; and/or Criminal penalties.

428.12 RELEASING ALPR DATA

State **MODIFIED**

The ALPR data may be disclosed, shared, or accessed by other law enforcement or prosecutorial agencies only as required in a judicial proceeding or as otherwise permitted by law, using the following procedures (Chapter 239, § 5, 2026 Laws):

- (a) The agency makes a written request for the ALPR data that includes:
 - 1. The name of the agency.
 - 2. The name of the person requesting.
 - 3. The intended purpose of obtaining the information.
- (b) The request is reviewed by the Administrative Services Division Commander or the authorized designee and approved before the request is fulfilled.
- (c) The approved request is retained on file.

ALPR data is exempt from disclosure to non-law enforcement or non-prosecutorial agencies under Washington State public records law. ALPR audit data is subject to disclosure by "bona fide researchers" as defined in RCW 42.48.010, provided that it does not include individually identifiable information. Additional information regarding the access, storage, use, and sharing

Kennewick Police Department

Policy Manual

Automated License Plate Readers

of ALPR data is addressed in Policy 805 - Protected Information and Public Safety Technology Data Governance.