



**City of Federal Way
Police Department**

Training Bulletin #26-002

TO:	All Police Personnel
DATE:	May 15, 2026
SUBJECT:	ESSB-6002 – Automated License Plate Reader (ALPR) Systems
APPROVED:	Andy J. Hwang, Chief of Police
AUTHOR:	Jeffrey VanderVeer, Administrative Lieutenant

Statement of Purpose:

This training bulletin provides all personnel with the legal requirements, restrictions, and operational guidance pertaining to Engrossed Substitute Senate Bill 6002 (ESSB 6002), governing the use of Automated License Plate Reader (ALPR) systems. This law took effect immediately and significantly restricts how ALPR systems may be accessed, used, and managed by law enforcement agencies.

This bulletin establishes immediate directives to ensure compliance and reduce exposure to civil liability, criminal penalties, and evidentiary suppression.

Civil and Criminal Liability

Violations of ESSB 6002 may result in:

- Gross misdemeanor criminal charges for intentional misuse
- Civil lawsuits, including damages, attorney's fees, and injunctive relief
- Administrative investigation and discipline

Additionally, any evidence obtained in violation of this law is subject to exclusion in court proceedings.

Areas Affected by ESSB 6002:

- Use of ALPR systems (fixed and mobile)
- Data access, retention, and sharing
- Traffic stops and enforcement actions
- Audit and documentation requirements
- Civil and criminal liability

Current FWPd ALPR Status:

The Federal Way Police Department currently operates:

- One Flock Safety location consisting of four fixed cameras
 - Proposed addition of two cameras at one additional location
- Four licensed Avigilon ALPR cameras within the city
- Vehicle-mounted ALPR systems (currently disabled; pending removal)

Immediate Directive:

Mobile / In-Car ALPR Systems

- All vehicle-mounted ALPR systems shall remain disabled and shall not be used at this point. Personnel are prohibited from activating, accessing, or attempting to utilize in-car ALPR systems.

Fixed ALPR Systems (Flock / Avigilon)

- Access to fixed ALPR systems is strictly limited to authorized uses as outlined below. Any use outside of these parameters is prohibited.

Summary of Law:

Authorized Uses

- ALPR systems may only be used when directly related to a specific and articulable investigation involving a vehicle that is:
 - Stolen
 - Associated with a missing or endangered person
 - Associated with a felony or gross misdemeanor
 - Registered to an individual with an outstanding felony or gross misdemeanor warrant
- All queries must be supported by a valid incident or case number and a clearly defined investigative purpose.

Prohibited Uses

Officers shall not use ALPR systems for:

- General surveillance or monitoring
- Intelligence gathering without a qualifying criminal nexus
- Tracking individuals or vehicles absent a qualifying investigation

ALPR systems shall not be used in connection with:

- Immigration enforcement
- Protected First Amendment activity (e.g., protests, religious gatherings)

ALPR systems shall not be used to monitor or collect data at or near:

- Schools
- Courts
- Places of worship
- Certain Healthcare facilities
- Immigration-related facilities
- Food banks

Traffic Stop Limitations

An ALPR “hit” **alone** does not establish reasonable suspicion.

Prior to initiating a stop, officers must:

- Visually confirm the license plate
- Verify the validity and accuracy of the database return
- Develop independent reasonable suspicion

Failure to meet these requirements may result in unlawful stops and suppression of evidence, in addition to potential for civil and/or criminal penalties for officers and/or the agency.

Data Retention Requirements

ALPR data shall not be retained longer than 21 days unless it is associated with a qualifying criminal investigation or other limited statutory exception.

Improper retention or use of ALPR data may constitute a violation of state law.

Data Sharing Restrictions

Officers shall not:

- Share ALPR data with unauthorized individuals or agencies
- Provide access to ALPR systems to unauthorized users
- Use ALPR systems for personal or non-law enforcement purposes

Access to privately held ALPR data requires a valid search warrant. This includes entities like Lowe’s, Home Depot, and HOAs.

Audit and Documentation Requirements

All ALPR system access is logged and subject to audit.

Each query must include:

- Officer identity
- Date and time of access
- Associated incident or case number
- Specific purpose for the query

Audit records are retained for a minimum of two years and will be reviewed for compliance.

Once implemented, officers will be required to enter the associated SPILLMAN code(s).

Key Takeaways for Officers:

Mobile ALPR systems are prohibited from use. Fixed ALPR systems may only be used for narrowly defined, lawful purposes. An ALPR hit alone is not sufficient for a traffic stop. All use must be tied to a legitimate investigation and properly documented. Misuse of ALPR systems creates significant personal and agency liability.

Implementation Guidance:

Supervisors shall ensure personnel understand and comply with these restrictions.

Personnel shall not access ALPR systems unless the use clearly meets the criteria outlined in this bulletin.

Questions regarding permissible use should be directed through the chain of command or professional standards prior to accessing the system.

Further policy development is ongoing and additional guidance will be issued as necessary.