



Automated License Plate Reader Policy Document

1. Purpose

The purpose of this policy is to establish standards governing the lawful, authorized, and appropriate use of Automated License Plate Reader (ALPR) technology operated by University of Washington Transportation Services in accordance with Washington's Driver Privacy Act (ESSB 6002).

The policy protects the privacy of the public while ensuring that ALPR technology is used only for legitimate parking and transportation enforcement purposes.

2. Scope

This policy applies to:

- Transportation Services employees
- Parking Enforcement Officers
- Supervisors
- Any persons granted access to ALPR data

3. Authorized Uses

ALPR data may only be used for official University business including:

- Parking permit enforcement
- Verification of permit compliance
- Enforcement of parking regulations
- Identification of vehicles associated with parking violations
- Investigation of parking-related incidents authorized by university policy
- Troubleshooting with an authorized vendor
- Verifying permit configurations and statuses
- Scanning for lot occupancy counts
- Data analysis for enforcement, occupancy counts, or other valid work-related requirements

Employees may not access ALPR data out of curiosity or for personal reasons.

4. Prohibited Uses

Employees shall not:



- Intentionally search vehicles in Security Desk or Patroller belonging to friends, family, coworkers, neighbors, or public figures.
- Access ALPR data for personal interest.
- Use ALPR data for non-work purposes.
- Share ALPR data with unauthorized persons.
- Circumvent system security.
- Export data except as authorized.
- Use ALPR data for immigration enforcement or immigration-related investigations.
- Monitor, identify, or track individuals engaged in constitutionally protected activities, including lawful political, religious, or expressive activities.
- Collecting data at or immediately surrounding protected locations prohibited by law, including elementary and secondary schools, places of worship, courts, food banks, protected health care facilities
- Sell, lease, rent, or otherwise disclose ALPR data except as authorized by law and University policy.

Improper use may result in disciplinary action.

5. Systems Access

Access to ALPR systems shall be limited to authorized personnel who have completed required training. Users shall access ALPR systems only through approved methods established by Transportation Services. Where the system supports individual user accounts, employees shall use their assigned credentials. Where operational software utilizes a shared application account, Transportation Services shall maintain administrative procedures sufficient to identify the authorized employee operating the system during each enforcement activity.

6. Data Retention

Transportation Services shall retain ALPR data in accordance with Washington law and University policy.

ALPR data shall be automatically purged after the approved retention period unless otherwise required by law.

Audit trail information shall be retained as required under ESSB 6002.

7. Audit Logging

All ALPR access is subject to audit.

Audit records include, where available:

- User identity



- Date and time
- Search criteria
- Purpose of access
- Data exports
- Sharing of data

Employees should assume all activity is reviewable.

8. Security

Users shall:

- Protect passwords.
- Log out of Security Desk on your desktop or hide Patroller with the tablet's lock screen when finished.
- Report suspected misuse.
- Employees shall immediately report suspected misuse, unauthorized access, improper disclosure, or other potential violations involving ALPR data.
- Suspected violations shall be reviewed promptly and handled in accordance with University policy and applicable law.
- Refer all law enforcement or public records requests for ALPR data to UWPD and the Office of Public Records at UW.
 - Transportation Service Employees are never authorized to provide ALPR data to law enforcement, or those making public records requests.

9. Training

Employees must complete ALPR training prior to receiving access.

Refresher training will be provided when:

- Laws change
- Policies change
- Significant software changes occur

10. Compliance

Failure to comply with this policy may result in:

- Revocation of ALPR access
- Disciplinary action
- Additional corrective measures



11. Under Management Responsibilities

- Ensure ALPR policies remain current with changes in Washington law and University policy.
- Ensure only authorized, trained personnel are granted ALPR system access.
- Periodically review audit logs and investigate suspected misuse or unauthorized access.
- Coordinate with University leadership, legal counsel, and compliance officials regarding ALPR requirements, reporting, and policy updates.

12. Policy References

- [Chapter 10.130 RCW: AUTOMATED LICENSE PLATE READER SYSTEMS](#)
- [APS 13.5 – Regulating the Installation and Use of Security Cameras](#)
- [Privacy Notice for License Plate Recognition for Parking Management](#)