

University of Washington Bothell and Cascadia College Commuter Services

Automated License Plate Reader (ALPR) Policy

DATE: September 25, 2026

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 Bothell and Cascadia College Commuter Services in accordance with applicable law, including Washington's Driver Privacy Act (ESSB 6002).

This policy protects individual privacy while ensuring that ALPR technology is used only for legitimate parking and transportation enforcement purposes.

2. Scope

This policy applies to:

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

This policy governs the collection, access, use, retention, disclosure, and disposal of ALPR data collected through Commuter Services operations.

3. Authorized Uses

ALPR data may be used only 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
- Verification of permit configurations and statuses
- Troubleshooting with authorized vendors

- Occupancy counts and parking utilization analysis
- Transportation planning and operational analysis
- Other legitimate parking and transportation-related business purposes authorized by Commuter Services

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

4. Prohibited Uses

Employees shall not:

- Intentionally search vehicles belonging to friends, family members, coworkers, neighbors, public figures, or any person for non-business reasons.
- Access ALPR data for personal interest.
- Use ALPR data for non-work purposes.
- Share ALPR data with unauthorized persons.
- Circumvent system security controls.
- Export data except as authorized by University policy.
- 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.
- Collect, use, or retain ALPR data for the purpose of monitoring access to protected facilities or protected activities prohibited by law.
- Sell, lease, rent, distribute, or otherwise disclose ALPR data except as authorized by law and University policy.

Improper use of ALPR systems or data may result in disciplinary action.

5. System 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 Commuter Services. Where the system supports individual user accounts, employees shall use their assigned credentials. Where operational software utilizes shared application accounts, Commuter Services shall maintain administrative procedures

sufficient to identify the authorized employee operating the system during enforcement activities.

6. Data Retention

Commuter Services shall retain ALPR data in accordance with applicable law and University policy.

ALPR data associated with parking enforcement actions, citation investigations, citation processing, or appeals may be retained through final disposition of the matter as authorized by law.

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

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

7. Audit Logging

All ALPR system access and activity is subject to audit.

Audit records may include:

- User identity
- Date and time of access
- Search criteria
- Purpose of access
- Data exports
- Data sharing activity

Employees should assume all ALPR activity is reviewable and subject to audit.

8. Security and Data Requests

Users shall:

- Protect passwords and access credentials.
- Log out of ALPR systems or secure devices when not in use.
- Report suspected misuse or unauthorized access immediately.
- Protect ALPR data from unauthorized disclosure.

Employees shall immediately report suspected misuse, unauthorized access, improper disclosure, or other potential violations involving ALPR data.

Suspected violations shall be reviewed and addressed in accordance with applicable law and University policy.

Requests for ALPR data from law enforcement agencies, attorneys, members of the public, or other external parties shall be referred to the University of Washington Police Department and the University Office of Public Records.

Commuter Services employees are not authorized to release ALPR data except as specifically authorized by law and University policy.

9. Training

Employees must complete required ALPR training prior to receiving independent system access or conducting ALPR-based enforcement activities.

Training shall include:

- Appropriate use of ALPR technology.
- Applicable laws and regulations.
- Data security and confidentiality requirements.
- Department procedures governing parking enforcement activities.

Additional training or refresher training may be required when:

- Laws or regulations change.
- Policies or procedures are updated.
- New equipment or software is implemented.
- Operational needs require additional instruction.

Vendor-provided training and technical support may supplement internal training programs as authorized by Commuter Services.

10. Compliance

Failure to comply with this policy may result in:

- Revocation of ALPR access.
- Disciplinary action.

- Additional corrective measures as authorized by University policy.

Violations may also result in further administrative review as appropriate.