
UCLA Policy 134: Automated License Plate Recognition Systems and Information

Issuing Officer: Administrative Vice Chancellor
Responsible Department: UCLA Events & Transportation
Effective Date: June 17, 2019
Supersedes: New

I. PURPOSE & SCOPE

II. DEFINITIONS

III. POLICY STATEMENT

IV. ALPR INFORMATION REQUIREMENTS

V. PRIVACY

VI. REFERENCES

I. PURPOSE & SCOPE

UCLA utilizes Automated License Plate Recognition (ALPR) technology to support management of campus parking facilities.

This Policy:

- Specifies the allowable uses of and requirements for ALPR Systems and ALPR Information at UCLA;
- Designates the Administrative Vice Chancellor as the Campus ALPR Authority; and
- Provides authorization for UCLA Events & Transportation to operate ALPR Systems and use ALPR Information.

This Policy also serves as the usage and privacy policy required by CA Civil Code §§ 1798.90.51 and 53 to ensure that the collection, use, maintenance, sharing, and dissemination of ALPR Information is consistent with federal, State, and local law. All UCLA departments that manage their own parking separate from Events & Transportation and who use ALPR for the purposes described herein shall also comply with this Policy.

II. DEFINITIONS

For the purposes of this Policy:

Automated License Plate Recognition (ALPR) Information means information or data collected through the use of an ALPR system.

Automated License Plate Recognition (ALPR) System means a searchable computerized database resulting from the operation of one or more mobile or fixed cameras combined with computer algorithms to read and convert images of registration plates and the characters they contain into computer-readable data.

The above terms have the same meaning as defined in [CA Civil Code § 1798.90.5](#)

Campus ALPR Authority is the campus official authorizing operation of ALPR Systems and use of ALPR Information.

III. POLICY STATEMENT

The Administrative Vice Chancellor is designated as the Campus ALPR Authority. The Administrative Vice Chancellor may delegate the role of Campus ALPR Authority, but the role may not be further redelegated.

A. Authorized Uses

Operation of ALPR Systems and/or access to or use of ALPR Information must only be for legitimate, official business purposes:

- *Parking Services*: For the purpose of parking management, occupancy counting, violation location, and rule enforcement. ALPR Information is retained in both anonymized and raw form for these business purposes.
- *Campus Safety*: For use in detecting a vehicle that enters a campus parking facility that is owned by or known to be used by an individual who has been issued an official campus stay away order, court ordered restraining order, law enforcement bulletin, or poses a threat to one or more members of the campus community.

Any other use must have prior written approval by the Campus ALPR Authority.

B. Authorized Users

Operation of ALPR Systems and/or access to or use of ALPR Information requires prior written authorization by the Campus ALPR Authority. Applicable background checks must be in compliance with [UCLA Procedure 21 – Appointment](#).

Authorized personnel must operate ALPR Systems or access or use ALPR Information only for the purpose(s) specified in the authorization. Any other operation, access, or use is unauthorized and may result in disciplinary action under University policies or, as applicable, collective bargaining agreements.

All authorized personnel must complete training on ALPR Systems and Information prior to active use and be provided with applicable University policies and procedures. Training must include:

- Systems operations to ensure the safeguarding of ALPR Information;
- Specific uses for which ALPR Systems and/or ALPR Information has been authorized;
- The requirements for ALPR Information set forth in Section IV and the procedures to implement them; and
- Annual UC Cyber Security training certification.

C. Authorization for UCLA Events & Transportation

The Campus ALPR Authority authorizes the following roles within UCLA Events & Transportation to operate ALPR Systems and use ALPR Information: Parking Enforcement Officer, Parking Enforcement Manager/Assistant Manager, and positions required for the continued operation of normal parking enforcement, event, and occupancy counting operations; and UCPD sworn personnel and emergency dispatchers. Any additional positions must be authorized as per Section III.B.

IV. ALPR INFORMATION REQUIREMENTS

ALPR Information is classified at Protection Level 3 ([UC Protection Level Classification Guide](#)). UCLA departments with authorized personnel who utilize ALPR Information are responsible for ensuring systems and processes are in place for its proper collection, storage, and disposal.

ALPR Information is defined as personal information by CA Civil Code § 1798.29(g)(1)(F). A breach of the security of an ALPR System is subject to UCLA Policy 420, Breaches of Computerized Personal Information. Any suspected unauthorized acquisition of ALPR Information that compromises its security, confidentiality, or integrity must be immediately reported to the campus Information Security Office or the Office of Compliance Services, UCLA Health.

A. Retention

ALPR Information is to be retained for no longer than 60 days unless it is specifically necessary to do so in support of parking violation enforcement, citation appeal adjudication, scofflaw enforcement, or law enforcement investigation. Storage duration limitations and data destruction will be facilitated via settings in the ALPR System and/or through the destruction of physical media, conformant with the [UC Institutional Information Disposal Standard](#).

B. Anonymization

ALPR Information will be anonymized on a scheduled basis for legitimate business needs. ALPR Information that has been anonymized is not subject to the 60-day retention limit.

C. Record Keeping

A record must be kept of access to non-anonymized ALPR Information, including who received access, the date and time of access, the purpose for the access, and the license plate number or other data element(s) used to query the ALPR System.

D. Sharing

ALPR Information may be shared within UCLA as well as with law enforcement agencies and other public agencies in accordance with applicable law and at the discretion of the Campus ALPR Authority, in support of law enforcement investigations, academic research, or other legal purpose.

Any sharing of ALPR Information requires (a) written authorization from the Campus ALPR Authority and (b) a written agreement between requestor and ALPR Information holder that complies with the provisions of UC Appendix DS – Data Security and Privacy with Protection Level 3 requirements.

E. Prohibition on Sale

ALPR Information will not be sold under any circumstances. The provision of data hosting or towing services shall not be considered the sale, sharing, or transferring of ALPR Information (CA Civil Code § 1798.90.55).

F. Audit

UCLA departments with authorized personnel must conduct periodic audits to review access rules, logs, configuration, and to confirm active individual accounts.

V. PRIVACY

This Policy governs the ALPR System operated by University of California, Los Angeles, and applies to its employees, customers, and camera and data hosting affiliates.

The images stored in the system are collected from areas visible to the public where there is no reasonable expectation of privacy.

Compliant with CA Civil Code 1798.90.53, this Policy shall be implemented and publicly published on [UCLA's Administrative Policies and Procedures website](#).

VI. REFERENCES

1. [CA Civil Code §§ 1798.90.5 – 1798.90.55](#)
2. [UCLA Procedure 21 – Appointment](#)
3. [UCLA Policy 420, Breaches of Computerized Personal Information](#)
4. [UC Protection Level Classification Guide](#)
5. [UC Institutional Information Disposal Standard](#)

Issuing Officer

/s/ Michael J. Beck

Administrative Vice Chancellor

**Questions concerning this policy or procedure should be referred to
the Responsible Department listed at the top of this document.**
