8.16 Automated License Plate Readers

Supersedes:	Revision:	Effective:
02 October 2025	24 November 2025	1 December 2025
Policy Affects: All Personnel		

Christopher Olson
Chief of Police

Purpose and Summary

This policy governs the deployment and use of Automated License Plate Readers ("ALPRs") and their associated software and hardware platforms. These tools support law enforcement efforts by, among other things, helping identify vehicles involved in criminal investigations, missing persons cases, welfare checks, and credible public safety threats.

The policy is intended to make ALPR use more transparent, legally compliant, purpose-driven, and subject to regular audit.

Use of ALPRs is subject to compliance with the Fourth Amendment of the United States Constitution and other applicable laws. All searches and data usage under this policy must be in support of legitimate law enforcement purposes and based on articulable facts. ALPRs will not be used for indiscriminate monitoring or to track expressive activities protected by the First Amendment.

Violations of this policy may result in disciplinary action including termination of employment.

Authorized Uses

ALPRs may be used for campus safety and security purposes, including, but not limited to:

- Locating vehicles that are stolen, wanted, or linked to missing or endangered persons (e.g., AMBER, Silver, or Missing Indigenous Person alerts)
- Identifying suspect vehicles, witnesses, or others in connection with violent or property crimes.
- Addressing credible public safety threats.

Use of ALPRs shall be based on articulable facts related to an active investigation.

Prohibited Uses

ALPRs shall not be used for:

- Personal or unofficial investigations

- General monitoring of University community members without a safety or criminal nexus
- General surveillance or monitoring unrelated to a public safety mission
- Targeting individuals based on protected characteristics

Access and Search Controls

- The UAPD Investigative and Support Services Bureau Commander serves as the ALPR system administrator
- Access to ALPR data shall be limited to those with certain job roles and responsibilities and only granted in accordance with the Authorized Uses defined above.
- All searches of campus safety technology records and data must include a query prompt tied to an active investigation, incident, or public safety issue.
- Use of ALPR records and data shall be logged by user, date, time, and justification. Logs shall be reviewed in accordance with the Auditing and Compliance Monitoring provisions of this Policy.
- The UAPD Executive Services Bureau Commander shall investigate any unauthorized use or breach of ALPRs and/or their associated data and records. All suspected incidents must be reported immediately to the Executive Services Bureau Commander and will prompt a formal investigation.
- All captured information, data, and records from campus safety technology shall be encrypted and protected in accordance with university information security standards and requirements.

Data Retention and Deletion

- The UAPD Investigative and Support Services Commander shall ensure that ALPR data and records are deleted on a regular schedule (unless particular records or data are marked for retention as described below). As of the date of this Policy's establishment, ALPR data is deleted automatically 30 calendar days from capture unless marked for storage.
- ALPR data and records related to active cases may be retained for longer periods of time with approval of the Chief of Police.

Data Sharing

- ALPR data and records may be shared only with law enforcement agencies and offices and only for approved law enforcement purposes.
- Direct access to the University of Arizona's ALPRs and their associated data and records by non-University law enforcement agencies shall be subject to all applicable federal and state laws and regulations. Direct access to the University of Arizona's campus safety technology, including data and records, may be subject to lawfully issued and applicable subpoenas, warrants, or court orders, which shall be subject to review by the University's legal counsel.
- Any sharing of ALPR data and records shall require prior approval from the UAPD Investigative and Support Services Commander.
- All ALPR data and record-sharing activity is logged with the following information: name of the individual making the request, that individual's associated agency, date of request, basis of request (i.e., description of the law enforcement purpose and accompanying authorization, such as a subpoena), and search date and time. *The Deputy Chief of Police or designee shall certify monthly that data sharing was done in accordance with the Auditing and Compliance Monitoring provisions of this policy. Deviations from these provisions shall be identified and a description of remedial steps provided in the certification notice.*

Training Requirements

- All users of ALPRs must complete department-approved training covering permitted legal uses of ALPRs and associated data and records; privacy protections; relevant University policies, procedures, protocols; and system operations.
- The UAPD Training Unit shall annually review proper application and usage of the system with users.

Auditing and Compliance Monitoring

- **Monthly audits**: The Deputy Chief or designee shall conduct a random review of searches, justifications, and data-sharing activity. The audit shall include the number of searches conducted, and which agency conducted the searches. Certification of that audit will be kept on a UAPD server and retained in accordance with University records retention requirements.

- **Annual reviews**: Annual comprehensive policy reviews will be conducted by the appropriate University units, including, but not limited to UAPD and the University's Office of General Counsel for legal, technical, and procedural compliance. The Deputy Chief of Police or designee will oversee all such policy reviews and ensure that necessary revisions are made.
- **Flock Transparency Portal**: The UAPD Investigative and Support Services Commander will maintain and update the Flock Transparency Portal. A link to the portal will be posted on the UAPD website and kept available for public review.

Ownership and Privacy Assurances

- All ALPR data and records are the exclusive property of the University and are under the stewardship of UAPD.

This Policy will remain in effect until retracted or revised by the Chief of Police.

Exceptions and Deviations

Any use of ALPRs and/or ALPR data and records outside the scope of this Policy must be pre-approved in writing by the Chief of Police or designee.