CITY OF BUCKEYE POLICE DEPARTMENT

"Serving the community with courage, commitment, and excellence"

Effective Date	POLICY	Policy Number
January 26, 2015		**460**

Subject

Automated License Plate Readers (ALPR)

References	Rescinds/Replaces	Last Reviewed/Revised: August 14, 2026 -revised June 13, 2024	
CALEA Standards 41.3.9 License Plate Recognition Systems	Distribution: PowerDMS All Department Personnel	No. Pages 5.	Authorized By *Robert E. Sanders* Chief Robert E. Sanders

I. PURPOSE AND SCOPE

Automated License Plate Reader (ALPR) technology, also known as License Plate Recognition (LPR), automatically detects and records license plates. This policy established requirements governing the access to and use of ALPR systems and ALPR data by Department personnel. It applies to all ALPR systems and data accessed by Department personnel, including Department-owned, vendor-hosted, shared or externally operated systems, and governs user access, training, searches, custom hotlists, alerts, data exports, information sharing, evidence preservation, security, retention, and audits.

II. POLICY

The Buckeye Police Department authorizes the use of ALPR technology only for legitimate law-enforcement investigations or response to an imminent public-safety threat and in accordance with this policy. ALPR shall not be used solely for Department administrative investigations or civil matters.

III. DEFINITIONS

Automated License Plate Reader (ALPR)/License Plate Recognition (LPR) – A system that automatically detects and records license plates for authorized law-enforcement use.

Custom Hotlist – A user-created list of license plates associated with legitimate law-enforcement investigation that generates alerts when a listed license plate is detected.

IV. ALPR ADMINISTRATION

A. The ALPR Administrator is responsible for managing ALPR system access, equipment, data retention, system administration, and audits. The ALPR Administrator may delegate day-to-day administrative duties to qualified personnel.

B. The ALPR Administrator shall determine whether an employee has an operational need for ALPR access and shall approve access consistent with this policy.

C. The ALPR Administrator may review or audit the activity of outside-agency users who have direct access to a Department ALPR system.

V. ACCESS AND TRAINING

A. Department personnel may access or use an ALPR system only after completing Department-approved ALPR training and receiving authorization based on an operational need. Temporary access before completion of approved training is not permitted.

B. The Training Unit shall approve the Department ALPR training curriculum. Training shall address authorized and prohibited uses, alert verification, searches, custom hotlists, data security, information sharing, retention, and evidence preservation.

C. Each user shall access the ALPR system through an individually assigned account. Users shall not share login credentials or permit another person to access the system under their account.

D. ALPR access is limited to Department-approved devices and systems.

E. Patrol officers and other personnel expected to monitor or receive real-time ALPR alerts shall log in to the ALPR system at the beginning of their shifts.

F. No ALPR user may access Arizona Law Enforcement Telecommunications System (ALETS) or National Law Enforcement Telecommunications System (NLETS) information unless separately authorized to use those systems.

VI. AUTHORIZED AND PROHIBITED USES

A. ALPR shall be accessed or used only in support of a legitimate law-enforcement investigation or response to an imminent public-safety threat.

B. Historical ALPR searches and custom hotlist entries shall not be used for routine minor traffic violations unless extenuating circumstances create a legitimate investigative or public-safety need.

C. ALPR shall not be used for personal reasons, curiosity, political purposes, commercial purposes, or any purpose unrelated to a legitimate law-enforcement investigation.

D. ALPR shall not be used solely because of a person's race, ethnicity, religion, political beliefs, or participation in lawful First Amendment-protected activity.

E. Personnel shall not use, or allow others to use, ALPR equipment, accounts, or database records for an unauthorized purpose.

VII. ALPR SEARCHES

A. Every ALPR search shall include a brief investigative reason or purpose.

B. Personnel should enter the associated Department case number, CAD incident number, or other approved reference number when practical.

C. Users shall select the available ALPR search-reason category that most accurately reflects the investigation.

D. Personnel may select the geographic scope and search time period they believe could assist the legitimate law-enforcement investigation.

E. When conducting an ALPR search at the request of another law-enforcement agency, Department personnel shall verify the requestor and document the requesting agency and investigative purpose.

VIII. CUSTOM HOTLISTS

A. Any trained ALPR user may create a custom hotlist entry when the entry supports a legitimate law-enforcement investigation.

B. Each custom hotlist entry shall include a legitimate investigative reason. The creator is responsible for the accuracy of the plate information, the legitimacy of the investigative basis, and the continuing validity of the entry.

C. The creator shall assign a reasonable expiration date based on the investigative need and shall review each active entry for continuing validity at least once every 30 days.

D. A custom hotlist entry shall be removed as soon as the investigative reason is no longer valid or needed, even if the selected expiration date has not been reached.

E. Custom hotlist entries shall not be created for routine minor traffic violations unless extenuating circumstances create a legitimate investigative or public-safety need.

F. The creator shall select the personnel or groups who will receive alerts generated by the custom hotlist and is responsible for choosing appropriate recipients. Personnel shall not assume that other Department personnel received the same custom hotlist alert.

G. When practical, personnel acting on a custom hotlist alert shall radio the complete license plate, plate state, vehicle description, location, direction of travel, and alert type.

H. A custom hotlist entry may be modified or removed by its creator, the ALPR Administrator, or a supervisor with a legitimate operational need.

I. Department-created custom hotlist entries or alerts may be shared with outside law-enforcement personnel when the creator or ALPR Administrator determines that sharing supports the legitimate investigation.

J. Alerts generated from another agency's custom hotlist shall be handled in the same manner as Department-created custom hotlist alerts.

IX. ALERTS AND ENFORCEMENT ACTION

A. An ALPR alert is an investigative lead and, by itself, does not establish reasonable suspicion, probable cause, or the identity of a vehicle's current occupants.

B. Personnel are responsible for ensuring the accuracy of an ALPR alert before taking law-enforcement action based on the alert.

C. Before taking enforcement action, personnel should confirm that the displayed license plate and available vehicle description match the observed vehicle and verify the alert through ALETS, NCIC, or another authoritative source when practical.

D. Any enforcement action associated with ALPR information shall be independently supported by the applicable legal standard.

E. Personnel may take immediate law-enforcement action before completing database verification when delay would create an immediate officer-safety or public-safety risk. Such action shall be based on the totality of the circumstances, and verification should be completed as soon as practical.

X. REPORTING AND EVIDENCE PRESERVATION

A. When ALPR information materially contributes to an investigation, the investigating employee shall document how the information contributed in the applicable incident or supplemental report and shall add the applicable circumstance code or codes.

B. When ALPR information materially aids an investigation, the investigating employee shall export the relevant images and available CSV or report data and upload the material to the Department evidence system.

C. Personnel shall preserve only the ALPR images, records, and search results reasonably related to the investigation.

D. Personnel may download or export ALPR data only when necessary for a legitimate law-enforcement investigation, evidence preservation, or authorized information sharing.

E. Any ALPR data saved in relation to an investigation shall be stored and retained in accordance with the Department evidence-retention policy.

XI. DATA RETENTION

A. Routine ALPR data and images stored or controlled by the Department shall be retained for 30 days.

B. ALPR data accessed through a system owned or controlled by another agency shall be subject to the retention rules of the originating system.

C. ALPR information preserved in connection with an investigation shall be retained in accordance with the Department evidence-retention policy.

XII. DATA SECURITY AND SAFEGUARDS

A. ALPR information is law-enforcement-sensitive information and may be accessed, used, or disclosed only by authorized personnel for approved purposes.

B. ALPR information may be stored or transmitted only through Department-approved systems. Personal devices, personal email, unapproved cloud storage, and other non-Department systems shall not be used to store or transmit ALPR information.

C. Personnel shall promptly report suspected unauthorized access, credential compromise, improper disclosure, or loss of ALPR data to a supervisor and the appropriate Department technology or security personnel.

D. Personnel shall promptly report suspected unauthorized or improper ALPR use to a supervisor or the ALPR Administrator.

XIII. INFORMATION SHARING AND EXTERNAL ACCESS

A. Department personnel may share ALPR information with another law-enforcement agency after verifying the requestor and confirming a legitimate investigative purpose.

B. The employee sharing ALPR information shall document the requesting agency, requestor, investigative purpose, and date of release.

C. The information disclosed shall be limited to information reasonably related to the requesting agency's legitimate investigation.

D. Personnel from another law-enforcement agency may be granted direct access to a Department ALPR system when authorized by the ALPR Administrator and supported by an agreement or documented operational need.

E. Outside-agency users granted direct access shall comply with this policy and any applicable Department access restrictions.

F. All requests for ALPR information from members of the public, attorneys, media representatives, or other non-law-enforcement entities shall be referred to the Department Records Unit for processing under applicable public-records law, confidentiality requirements, and Department policy.

XIV. ACCOUNTABILITY AND AUDITS

A. The ALPR Administrator shall conduct an ALPR system compliance audit at least monthly. The scope of the audit is within the ALPR Administrator's discretion.

B. The ALPR Administrator shall document the audit results and report significant compliance issues to the Chief of Police or designee.