# Automated License Plate Readers (ALPR)

## 460.1 PURPOSE AND SCOPE

The purpose of this policy is to establish requirements for the lawful, ethical, transparent, and accountable use of Automated License Plate Reader (ALPR) technology and associated data by the Arvada Police Department.

## 460.2 POLICY

The policy of the Arvada Police Department is to utilize ALPR technology to capture and store digital license plate data and images while safeguarding the established privacy rights of the public. All data and images gathered by the ALPR are restricted for official, authorized, and documented law enforcement or public safety purposes only. Authorized purposes include preventing and solving crime, locating missing, endangered, or vulnerable persons, recovering stolen property, generating investigative leads, and enhancing officer and community safety.

ALPR systems, associated databases, and ALPR data shall be managed in accordance with applicable law, Department policy and procedures, records requirements, and safeguards governing access, security, sharing, retention, privacy, civil rights, and civil liberties.

### 460.2.1 DEFINITIONS

Definitions related to this policy include:

**ALPR:** A device or system primarily designed to identify vehicles by passively recording vehicle license plates and that may also capture associated vehicle images and metadata. ALPR systems used by the Department do not use facial recognition technology and are typically not designed to collect or store personal identifying information, such as names, addresses, or dates of birth, as part of the ALPR record.

**ALPR Data:** Digital images of license plates and/or vehicles and associated metadata captured, generated, or retained by an ALPR system, which may include date, time, geographic location, camera or device identification, and related system records.

**Mobile ALPR:** ALPR cameras that are affixed, either permanently (hardwired) or temporarily (i.e. magnet-mounted), to a law enforcement vehicle or equipment for mobile deployment.

**Fixed ALPR:** ALPR cameras that are permanently affixed to a structure, such as a pole, traffic control device, or a parking structure.

**Portable ALPR:** ALPR cameras that are transportable and can be moved and deployed in a variety of venues as needed.

**Read:** Digital images of license plates and vehicles and associated metadata (e.g., date, time, and geographic coordinates associated with the vehicle image capture) that are captured by the ALPR system.

**Alert/Hit:** An auditory or visual notice that a license plate read matches a license plate on an authorized law enforcement hot list or a license plate that has been manually entered for detection. An alert or hit is an investigative lead and must be verified in accordance with this policy before enforcement action is taken.

**Hot List:** A list of license plate numbers associated with vehicles of law enforcement interest, such as stolen or wanted vehicles, vehicles associated with missing or endangered persons, vehicles connected to active investigations, or other authorized law enforcement purposes. Hot-list information may originate from authorized sources including NCIC, CCIC, other law enforcement agencies, motor vehicle records, or other approved government or law enforcement databases. Authorized users may also manually enter a license plate into a hot list for a documented law enforcement purpose.

**User/Authorized User:** Any sworn or professional staff member of the Arvada Police Department who is authorized to operate an ALPR system or access ALPR data and who has completed required training.

## 460.3 ADMINISTRATION

The Arvada Police Department shall designate a Commander to serve as the ALPR Administrator and provide administrative oversight for ALPR deployment, operations, access, data management, security, information sharing, auditing, and program compliance. The ALPR Administrator may designate trained personnel to perform administrative functions consistent with Department policy and procedure.

### 460.3.1 ALPR ADMINISTRATOR

The designated Commander serving as the ALPR administrator shall be responsible for:

(a) Maintaining and reviewing Department procedures governing ALPR deployment, access, collection, storage, retention, purging, sharing, auditing, maintenance, and management. This includes designating employees with administrative oversight for the ALPR systems.

(b) Maintaining or ensuring maintenance of a current list of authorized users and managing user accounts and permissions so access is limited to persons with a legitimate need and is removed when no longer required.

(c) Ensuring initial and refresher training for authorized users has been completed, including system operation, legal requirements, alert verification, privacy and civil-liberties protections, data security, information sharing, retention, and consequences for misuse.

(d) Establishing protocols to preserve and document ALPR reads and alerts that are acted upon in the field or become associated with investigations, prosecutions, civil matters, administrative matters, or other authorized evidentiary purposes.

(e) Coordinate with City information-technology personnel and approved vendors to ensure appropriate cybersecurity, authentication, access controls, logging, data-integrity protections, software maintenance, and security updates are implemented and maintained.

(f) Authorizing or establishing procedures for requests involving ALPR data access or sharing

and ensuring standing data-sharing relationships are documented and periodically reviewed.

(g) Ensuring regular audits of system use and data access and ensure supervisory reviews are conducted in accordance with Department procedure.

(h) Conducting periodic evaluations of system performance, policy compliance, data quality, retention compliance, and public safety value, consistent with Department guidelines and applicable law including C.R.S.§ 24-72-113.

(i) Working with the Legal Department to stay reasonably current on changes in applicable law, technology, vendor capabilities, data sources, and system functionality, and recommend policy or procedure changes when needed.

(j) Ensuring authorized personnel conduct equipment checks on a regular basis to verify functionality and camera alignment. Any equipment that does not function as expected shall be promptly documented and reported. ALPR system repairs, including hardware and software repairs, shall be performed by authorized Department personnel, City personnel, contractors, or approved vendors, as appropriate.

(k) Establishing procedures and safeguards intended to promote the security, integrity, quality, and accuracy of data entered, captured, stored, or retained by ALPR systems.

## 460.4 ALPR OPERATIONS

Use of an ALPR system is restricted to the purposes outlined below. Department employees shall not use, or allow others to use, ALPR equipment or data for any unauthorized purpose.

(a) No ALPR user may access Department, State, or Federal data unless otherwise authorized to do so. Only authorized and trained personnel shall be permitted to access this agency's ALPR system and its associated data.

(b) ALPR equipment and associated data shall be used only for official and legitimate law enforcement purposes, as permitted by law, this policy, and Department procedure. For example, an ALPR system may be used in conjunction with an official Department investigation. Reasonable suspicion or probable cause is not required merely to use an ALPR system or query ALPR data; however, any subsequent detention, search, seizure, arrest, or other enforcement action must be supported by the legal authority required for that action.

(c) ALPR cameras shall be used to capture license plates and vehicles that are lawfully observable from public places or locations to which the Department otherwise has lawful access.

(d) ALPR technology or data shall not be used for personal, political, retaliatory, discriminatory, commercial, harassing, intimidating, or other unauthorized purposes. ALPR technology shall not be used for the sole purpose of monitoring lawful First Amendment-protected activity or other constitutionally protected conduct.

(e) No member shall operate ALPR equipment or access ALPR data without Department authorization and completion of Department-approved training.

(f) Hot lists obtained from Department-approved sources shall be updated at intervals established by the Department and system configuration to maintain reasonable currency and accuracy.

(g) An ALPR alert or hit is an investigative lead and shall not, by itself, be treated as conclusive evidence or as an independent basis for enforcement action. Before taking enforcement action based substantially on an ALPR alert, users shall verify the alert or hit. When reasonably practicable, users shall:

1. Visually verify that the vehicle plate number matches the plate number and state run by the ALPR system, including characters of the license plate and the state of issuance.
2. Determine the source of the ALPR record and, when available, who or what entity acquired the data;
3. Consider the age and source of the alert;
4. Verify the current status of the record through an appropriate law enforcement database or source;
5. Establish the lawful basis for the enforcement action;
6. Personnel shall not assume that the registered owner or person associated with a license plate is the driver or occupant of the observed vehicle. The connection between the vehicle, plate, driver, and relevant investigation shall be independently evaluated as appropriate.

(h) When conducting a search within the ALPR system, operators will document the associated case number, event number, or Bolo information, and the justification for the search.

(i) When police action is taken based on an ALPR alert, the disposition or action taken shall be documented in accordance with Department procedure.

(j) A manual hot-list or alert entry shall be supported by a documented law enforcement or public safety purpose. The user shall document the reason for the entry and establish an expiration date or review period. Manual entries shall be updated or removed when the underlying purpose expires or is no longer valid.

(k) When selecting locations for fixed or portable ALPR deployment, the Department should consider the public-safety purpose of the deployment and reasonably foreseeable privacy and civil-liberties implications, particularly when deployment may disproportionately capture activity associated with constitutionally protected or sensitive activities.

(l) While an ALPR may be used to canvass license plates around a crime scene, particular consideration should be given to using Mobile and Portable ALPR systems to canvass areas around homicides, shootings and other major incidents. Users of Mobile and Portable ALPR systems shall offload any data captured by the systems at the end of each shift. Mobile and portable ALPR data shall be transferred or offloaded in accordance with Department-approved procedures and system requirements.

## 460.5 DATA COLLECTION AND RETENTION

ALPR data obtained from external systems or databases shall originate from Department-approved public or private sources and shall be accessed only for authorized law enforcement purposes. ALPR data shall be retained, accessed, preserved, stored, and purged in accordance with applicable law, Department-approved retention requirements, and authorized operational, investigative, evidentiary, or administrative needs. All data and images gathered by ALPR systems are for the official use of the Arvada Police Department only. Such data may contain confidential information. Release of ALPR data shall be made on a case-by-case basis and in compliance with the criminal justice portion of the Colorado Open Records Act. ALPR information gathered and retained by this Department may be shared with and used by prosecutors, other law enforcement agencies, or otherwise as permitted by law. ALPR data will be held in accordance with C.R.S. §24-72-113.

(a) Mobile ALPR

1. Data collected by a Mobile ALPR system is stored on a server maintained by the City of Arvada's IT Department or by an approved third-party provider under Department agreement.
2. Unless lawfully preserved for an authorized purpose, Mobile ALPR data shall be automatically purged in accordance with the Department-approved retention period and C.R.S. § 24-72-113.

(b) Fixed ALPR

1. Fixed ALPR systems may be owned by the Arvada Police Department, the City of Arvada, leased, hosted, or supported through third-party vendors.
2. Data collected by fixed ALPR systems may be stored on City-managed infrastructure or approved vendor-hosted systems.
3. Vendor-hosted ALPR data shall be retained and automatically purged in accordance with the Department-approved retention period, applicable law, and the technical capabilities and retention limitations of the vendor system. The ALPR Administrator shall periodically verify that configured retention settings are consistent with Department and legal requirements.

(c) PRESERVATION OF EVIDENCE: ALPR reads, alerts, images, or related data that are acted upon in the field or become relevant to a criminal investigation, prosecution, civil claim, administrative investigation, personnel matter, or other authorized evidentiary purpose may be preserved outside the routine ALPR retention system in accordance with applicable law and Department evidence and records-retention procedures.

(d) RETENTION AND PURGING: ALPR data shall be retained only for the period authorized by Department policy and applicable law and only while it serves a clear operational, investigative, evidentiary, administrative, or legally required purpose. Once the applicable retention period expires and there is no continuing authorized purpose for preservation, the data shall be purged promptly in accordance with established procedures

## 460.6 ACCOUNTABILITY, DATA SHARING, AND SAFEGUARDS

ALPR systems and data shall be protected by procedural, administrative, and technological safeguards designed to prevent unauthorized access, use, alteration, disclosure, loss, or misuse. All saved data will be closely safeguarded and protected by both procedural and technological means. The Arvada Police Department will observe the following safeguards regarding access to and use of stored data:

(a) Access to ALPR systems and data shall be limited to trained, authorized personnel using individually assigned credentials or other Department-approved authentication controls. Shared accounts and the use of another person's login credentials are prohibited. Persons approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relates to a specific criminal investigation or department-related official action.

(b) In accordance with C.R.S. § 24-74-103, ALPR data shall not be disclosed or made accessible, including through a database or automated network, for the purpose of investigating, participating in, cooperating with, or assisting in federal immigration enforcement, unless required by federal or state law or compelled by a court-issued subpoena, warrant, or order.

(c) ALPR systems shall maintain audit records sufficient to identify, to the extent supported by the system, the user, date and time of access, data or query accessed, purpose or justification, associated case or event identifier when applicable, and relevant dissemination activity. Audit records shall be protected from unauthorized alteration

(d) ALPR data may be used only for the authorized purpose for which access was obtained. A subsequent or secondary use must be independently authorized and documented.

(e) All non-law enforcement requests for access to stored ALPR data shall be referred to the Records Supervisor and processed in accordance with applicable law and Department procedure.

(f) All ALPR data downloaded to the mobile workstation and server shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time.

(g) ALPR data shall be shared only with authorized entities for legitimate law enforcement or public safety purposes and as permitted by law. ALPR data may be released to other authorized and verified law enforcement officials and agencies for legitimate law enforcement purposes. When practical, the release should document the requesting agency, purpose of the request, date and time, requesting individual, and, if available, the data provided.

(h) Data related to any ALPR located on a CDOT right of way will be shared with the Colorado State Patrol and/or CDOT upon request.

(i) ALPR system audits shall be conducted on a regular basis. Such audits will be conducted within the capabilities of the ALPR system and should include the following elements, when

available:

1. Review of access logs to determine who accessed ALPR data, when, and for what purpose to ensure that the ALPR system is used only by authorized personnel,for legitimate law enforcement purposes, and that all access is compliant with policy, procedures, and any state laws;
2. Review of information sharing and dissemination;
3. Review of data security, retention, and purging practices; and
4. Compliance with applicable law, policy, training, security, and authorization requirements.

(j) Suspected misuse, unauthorized access, or unauthorized disclosure of ALPR data shall be promptly reported and investigated in accordance with Department policy. Access may be restricted or suspended when appropriate. Violations may result in corrective or disciplinary action and, when warranted, civil or criminal accountability.

(k) ALPR-related complaints shall be received, documented, and reviewed through established Department complaint or internal review processes.

(l) Known or suspected security incidents, data compromise, or unauthorized disclosure involving ALPR systems or data shall be promptly reported and addressed

(m) The Department shall periodically review its ALPR program, policy, procedures, system capabilities, data sources, retention practices, information-sharing relationships, and available performance information to ensure continued compliance with law, Department objectives, privacy and civil-liberties protections, and responsible-use standards.

(n) Consistent with law, operational security, investigative needs, and records requirements, the Department should provide appropriate public information regarding the purpose, general operation, safeguards, governance, and use of its ALPR program.

## 460.7 TRAINING

(a) Personnel shall complete Department-approved ALPR training before independently accessing or using an ALPR system.

(b) Initial training shall include, at a minimum:

1. Authorized use of ALPR systems;
2. Search and documentation requirements;
3. CR, CAD, or other identifying reference entry;
4. Appropriate search-reason documentation;
5. Alert and hit verification;
6. Outcome documentation;
7. Hot-list and custom alert procedures, when applicable;

8. Data preservation and evidence procedures; and
9. System-specific operational functions.

(c) Personnel shall complete refresher training as directed by the Department. Refresher training may be required based on changes in law, Department policy or procedure, system functionality, identified audit trends, or other operational needs.

(d) Department-approved training may include internal instruction, vendor-provided training, webinars, or other approved training resources.

(e) Additional or remedial training may be required when audits or supervisory review identify recurring documentation, operational, or compliance concerns.

(f) Completion of required initial, refresher, or remedial ALPR training shall be documented in the Department-approved training system or other designated training record.