

		TITLE AUTOMATED LICENSE PLATE READER (ALPR) SYSTEMS		POLICY NUMBER 6.17
WHITE COUNTY SHERIFF'S OFFICE General Orders			EFFECTIVE DATE 08/01/2014	PAGE OF 1 9
☐ NEW ☒ AMEND ☐ RESCINDS	NUMBER N/A	SOURCE §	APPLICABLE STANDARD NUMBER	
APPROVED BY Sheriff Rick Kelley <i>Rick Kelley</i> Rick Kelley (Aug 20, 2026 10:43:47 EDT)				DATE/REVISED 08/07/2026

I. PURPOSE

The purpose of this policy is to establish guidelines for the lawful, secure, and effective use of Automated License Plate Reader (ALPR) technology, including system operation, access, data management, equipment maintenance, training, accountability, and the preservation and disposition of ALPR data.

II. POLICY

Automated License Plate Readers provide opportunities to improve investigative efficiency, operational effectiveness, and deputy safety. White County Sheriff's Office employees shall use ALPR systems and ALPR data only for legitimate law enforcement or public safety purposes and in accordance with this policy, other White County Sheriff's Office written directives, O.C.G.A. § 35-1-22, applicable federal law, and applicable Criminal Justice Information Services (CJIS) and Georgia Crime Information Center (GCIC) requirements. White County Sheriff's Office shall safeguard ALPR data against unauthorized access, use, disclosure, alteration, or retention.

III. DEFINITIONS

- A. Alert:** An audible, visual, email, text-message, or software notification generated when an ALPR detection potentially matches a hot list record. An alert is an investigative lead and is not a confirmed hit until the detection and the source record have been verified.
- B. Automated License Plate Reader (ALPR):** An electronic system that uses one or more cameras and computer algorithms to capture vehicle and license plate images, convert license plate characters into computer-readable data, and compare the resulting data with authorized law enforcement databases or hot lists.
- C. ALPR Data:** Digital information captured by or derived from an ALPR system, including a license plate number, vehicle image or description, date and time, camera location, direction of travel, and related metadata.
- D. ALPR Power User:** A designated White County Sheriff's Office ALPR user with permissions to search historical license plate or vehicle data and/or create custom hot list entries within the Flock and Fusus software platforms. Power Users must complete

agency-approved training before receiving search privileges and annually thereafter to maintain those privileges.

- E. Confirmed Hit:** An ALPR alert that has been visually verified against the captured image and independently confirmed as current and valid through GCIC, the National Crime Information Center (NCIC), the originating agency, or another authorized source.
- F. Custom Hot List:** A license plate or vehicle record manually entered by an authorized ALPR Power User for a documented law enforcement or public safety purpose based on a legitimate case, report, BOLO, CAD event, or other articulable criminal or public safety nexus. A custom entry may include case notes, photographs, reports, cautions, requested actions, and contact information.
- G. Detection:** A vehicle or license plate image read by an ALPR system in an area exposed to public view, together with related date, time, location, direction, and vehicle-description information.
- H. Fixed ALPR System:** An ALPR camera permanently or semi-permanently installed on a pole, building, bridge, traffic structure, trailer, or other stationary location.
- I. Flock:** The Flock Safety hardware and software platform used by White County Sheriff's Office for ALPR detections, alerts, searches, video, and related system functions.
- J. Hot List:** A database of license plates or vehicles associated with stolen vehicles or plates, wanted or missing persons, AMBER Alerts, Mattie's Calls, Levi's Calls, criminal investigations, officer-safety information, or other legitimate law enforcement or public safety matters. Hot list information may originate from NCIC, GCIC, another law enforcement agency, or an authorized custom entry.
- K. Mobile ALPR System:** An ALPR system mounted on or used from a law enforcement vehicle or other mobile platform.
- L. Search:** A query of current or historical ALPR data using a license plate, partial plate, vehicle description, date, time, location, or other authorized search parameter.
- M. Tentative Hit:** An ALPR alert that has been visually matched to the captured image but has not yet been independently confirmed as current and valid through GCIC, NCIC, the originating agency, or another authorized source.

IV. PROCEDURES

A. Privacy, Authorized Use, and Prohibited Conduct

1. Employees shall use ALPR systems, equipment, detections, searches, alerts, and associated imagery only for legitimate law enforcement or public safety purposes and in conformance with applicable law and White County Sheriff's Office written directives.
2. No employee shall access, search, view, record, reproduce, retain, disclose, distribute, or permit access to ALPR data except as authorized by this policy or required by law.
3. Employees shall not intentionally position, direct, or use an ALPR camera to capture an area in which a person has a reasonable expectation of privacy unless authorized by a search warrant, exigent circumstances, consent from a person with authority to provide consent, or another lawful exception.
4. ALPR systems shall not be used for personal purposes; to harass, intimidate, or improperly track any person; or to monitor a person or group solely because of race, ethnicity, national origin, religion, sex, sexual orientation, gender identity, disability, political affiliation, or constitutionally protected speech, association, or activity.

5. An ALPR alert, a vehicle association, or a registered-owner return does not establish that the associated person is operating or occupying the vehicle. An alert shall not be the sole basis for a traffic stop, detention, search, arrest, or other enforcement action.
6. Before taking enforcement, action based on an alert, personnel shall visually verify the plate and state of issuance against the captured image, confirm the source record remains current and valid, and establish the legal basis required for the contemplated action.
7. White County Sheriff's Office ALPR systems, accounts, equipment, databases, detections, and data are agency resources intended for official business. Misuse may result in loss of access, disciplinary action up to and including termination, and criminal prosecution.

B. Administration and Responsibilities

1. Unless otherwise directed by the Sheriff or an authorized designee, the Chief Deputy shall serve as the White County Sheriff's Office ALPR System Administrator.
2. The Chief Deputy, or authorized designee, shall establish and maintain protocols for:
 - a. Access to, collection of, storage of, sharing of, and retention of ALPR data and associated media;
 - b. Preserving and documenting detections, alerts, and confirmed hits that are acted upon in the field or associated with an investigation or prosecution;
 - c. Protecting the security, integrity, availability, and confidentiality of ALPR systems and data;
 - d. Maintaining a complete inventory of White County Sheriff's Office ALPR equipment, including camera locations, status, assignment, and ownership;
 - e. Documenting ALPR use, system access, search activity, custom hot list entries, information sharing, audits, findings, and corrective action;
 - f. Approving non-routine ALPR deployments, persistent information-sharing relationships, and requests for access that fall outside normal operations;
 - g. Creating and maintaining current ALPR lesson plans, training materials, and user instructions; and
 - h. Conducting and documenting an annual review of this policy, system practices, vendor requirements, training, access lists, data-sharing relationships, retention settings, and audit procedures.
3. The Patrol Commander, or authorized designee, shall manage day-to-day ALPR administration, including user access, vendor coordination, equipment-health checks, audit production, detailed user audits, and the reporting of suspected misuse or system deficiencies.
4. An ALPR user's immediate supervisor shall ensure that the user follows this policy and shall promptly report suspected violations, access concerns, equipment problems, or other ALPR-related issues to the Chief Deputy and Patrol Commander.
5. ALPR hardware or software repairs, configuration changes, and system modifications shall be performed only by an authorized vendor or by an employee specifically authorized by the Chief Deputy or designee.

C. ALPR Operation and Authorized Uses

1. Personnel shall exercise due care when operating, viewing, or responding to an ALPR system, particularly while operating a vehicle. ALPR use shall not distract a driver from the safe operation of the vehicle.

2. ALPR systems and data may be used in conjunction with routine patrol operations, criminal investigations, missing-person investigations, stolen vehicle or stolen-plate investigations, officer-safety operations, crime analysis, critical incidents, special events, and other legitimate law enforcement or public safety activities.
3. Reasonable suspicion or probable cause is not required merely to operate an ALPR system or conduct an ALPR search; however, every use or search must have a documented law enforcement purpose, and any resulting detention, search, arrest, or enforcement action must be supported by the legal standard applicable to that action.
4. Partial license plates and unique vehicle descriptions associated with a reported crime, missing-person matter, BOLO, or other legitimate public safety need may be searched or entered into an authorized system in an attempt to identify a vehicle.
5. A valid offense or incident type, case number or CAD event number, and a complete reason shall be entered when conducting a historical search or query. Users shall not use generic or incomplete reasons when additional information is available.
6. Hot List Alert Verification
 - a. ALPR alerts may be delivered by audible or visual alarm, email, text message, Flock, Fusus, or another authorized interface.
 - b. The receiving employee shall review the captured image and verify that the plate characters and state of issuance match the alert. Vehicle make, model, color, distinguishing features, and location should also be compared when available.
 - c. If the alert does not match the image or appears inaccurate, the alert shall be rejected or otherwise documented as a misread.
 - d. If the image matches the alert, the employee shall confirm that the record remains active through GCIC, NCIC, the originating agency, or another authorized source before taking enforcement action, when circumstances reasonably permit.
7. Hit Response Procedures
 - a. A deputy responding to investigate an alert shall advise the dispatcher of the applicable call type, location, and other information needed for a safe and coordinated response.
 - b. Supervisors shall manage the number of responding resources, approach, tactics, timing, and location of any planned contact. Personnel shall follow all White County Sheriff's Office policies applicable to the type of incident encountered.
 - c. Alerts involving a sex offender, gang or terrorist association, violent person, wanted person, or missing person require careful verification because the person associated with the record may not be an occupant of the vehicle. A non-consensual detention or enforcement action requires independent reasonable articulable suspicion or probable cause, as applicable.
 - d. Before taking enforcement action based on an alleged probation restriction involving a sex offender who resides in White County, deputies shall review Odyssey for applicable restrictions. If an apparent probation violation is identified, deputies shall complete an Incident Report titled "Probation Violation," leave the report Active, and forward to the Investigative Unit. When no arrestable offense exists, any direction to leave an area shall be based on an applicable restriction and handled in accordance with law and White County Sheriff's Office procedure.
 - e. If the sex offender resides outside White County, deputies shall make reasonable efforts to contact the supervising probation officer or other authorized source to verify applicable restrictions. If an apparent violation is identified or verification cannot be completed, deputies shall document the circumstances in an Incident

Report titled "Probation Violation," leave the report Active, and forward to the Investigative Unit.

- f. White County Sheriff's Office-created custom hot list alerts are frequently based on information developed by CID, Criminal Intelligence, or the RTCC and may be intended for intelligence or notification only. Personnel shall follow the requested action in the entry and shall establish an independent legal basis before any non-consensual stop, detention, search, or arrest.
 - g. In parks, school areas, event venues, and other congested locations, supervisors shall manage take-down locations, timing, and tactics for stolen vehicles, stolen plates, and wanted persons to minimize risk to pedestrians, children, deputies, and the public. When appropriate, well-planned vehicle containment or box-in tactics should be considered in accordance with White County Sheriff's Office policy.
 - h. The following dispatch signals shall be used to standardize and track calls generated by ALPR alerts:
 - (1) Plain Speech- Sex Offender (verify applicable restrictions; independent legal basis required for detention or enforcement action);
 - (2) Plain Speech- Stolen Plate;
 - (3) Plain Speech - Gang/Terrorist (independent legal basis required for detention or enforcement action);
 - (4) 10-0 - Violent Person (independent legal basis required for detention or enforcement action);
 - (5) Plain Speech- Missing Person;
 - (6) 10-29 - Stolen Auto; and
 - (7) Stat 11 - Wanted Person (the vehicle occupant may not be the wanted person associated with the alert).
8. Custom Hot Lists
- a. Only trained and authorized ALPR Power Users may create or modify custom hot list entries.
 - b. Each entry shall have a documented law enforcement or public safety nexus and shall include the license plate number and state of issuance, when known.
 - c. Each entry shall include the associated White County Sheriff's Office case number or CAD event number. An entry requested by another law enforcement agency shall include that agency's name, a valid case number, the requesting employee's name and contact information, and the stated law enforcement purpose.
 - d. The Reason field shall contain sufficient information to support the entry, identify applicable cautions, provide RTCC or entering-employee contact information, and state the requested action, such as stop and field interview, monitor only, or notify a specific employee.
 - e. Custom entries shall expire within thirty (30) days unless the nature of the investigation, crime type, or deputy-safety concern justifies a longer period. An entry with no expiration date or an expiration beyond thirty days must be approved by an and verified at least monthly by the entering employee or assigned investigator.
 - f. When a vehicle on a White County Sheriff's Office-created custom hot list is located and no longer requires monitoring, the locating employee or assigned investigator shall ensure the entry is removed or expired and shall notify the original creator. The notification shall include the case number, stop or detection details, arrests, disposition, and other pertinent investigative information.

D. Data Access, Security, Search, and Dissemination

1. Access to ALPR systems and stored data shall be role-based and limited to employees whose assigned duties require access and who have completed the required training.
2. Each user shall access the system only through the individually assigned account. Passwords, authentication codes, or other credentials shall not be shared, and users shall not permit another person to conduct activity under their account.
3. The Chief Deputy or authorized system administrator shall promptly modify, suspend, or deactivate access when an employee separates from White County Sheriff's Office, transfers, changes duties, fails to complete required training, violates this policy, or no longer has a business need for access.
4. ALPR platforms shall maintain audit information sufficient to identify the user, date and time, search parameters, stated purpose, associated case or CAD number, custom hot list activity, and data-sharing activity, to the extent supported by the system.
5. ALPR data may be exchanged or shared with another law enforcement agency only for a documented law enforcement purpose and in accordance with O.C.G.A. § 35-1-22(c).
6. A request from another agency shall identify the requesting agency and employee, case or incident number, scope of the request, and law enforcement purpose. Persistent or network-level sharing relationships shall be approved by the Chief Deputy or authorized designee and periodically reviewed.
7. ALPR data shall not be sold or provided to a non-law-enforcement entity except as required by law or specifically authorized by the Sheriff or designee after legal review. Open records requests, subpoenas, court orders, and other legal demands shall be referred to the appropriate White County Sheriff's Office unit for review and response.
8. A vendor or contractor may access or maintain ALPR data only as necessary to provide contracted services and shall remain subject to White County Sheriff's Office policy, applicable law, contractual security and confidentiality requirements, and restrictions on sale, secondary use, or unauthorized disclosure.
9. Administrative Investigations
 - a. ALPR data may be accessed and used during an internal or administrative investigation in accordance with White County Sheriff's Office, Internal Affairs Unit.
 - b. Prior approval from the Sheriff, Chief Deputy, or Patrol Commander is required before accessing ALPR data for an administrative investigation.
 - c. The request shall be in writing and shall identify the employee under investigation, state the specific administrative allegation or purpose, and define the scope and timeframe of the requested data.
 - d. ALPR data shall not be used for routine employee location monitoring, attendance verification, productivity tracking, or other non-investigatory administrative purposes.

E. Installation, Inventory, Equipment Care, and Maintenance

1. The Sheriff, or authorized designee, shall coordinate the approval, installation, implementation, relocation, and maintenance of fixed and mobile ALPR systems.
2. New fixed ALPR cameras shall be installed by the authorized ALPR vendor or representative after required agency approval and permitting. Mobile or portable systems shall be installed or configured only by authorized personnel.

3. The Chief Deputy, or designee, shall maintain a current inventory of ALPR equipment, including camera location, assignment, operational status, ownership or funding source, and other information needed for accountability.
4. At least weekly, the Patrol Commander or designee shall review the system health of each White County Sheriff's Office ALPR device through the vendor platform. Identified failures, misalignment, connectivity problems, or other operational issues shall be reported to the vendor or authorized repair source without unnecessary delay.
5. An employee who discovers equipment damage, a required repair, a system malfunction, a security concern, or an operational problem shall promptly notify the employee's immediate supervisor and the Patrol Commander.
6. If an ALPR camera or related equipment is damaged or destroyed, the involved employee shall complete the appropriate Incident Report or Accident Report and provide the report number or a copy to the Patrol Commander.
7. Employees shall not modify, adjust, relocate, repair, or alter ALPR equipment or software unless specifically authorized.

F. Training

1. Personnel shall complete agency-approved ALPR training before operating an ALPR system, receiving system credentials, searching stored data, or creating a custom hot list entry.
2. Employees authorized to conduct searches or create custom hot list entries shall complete agency mandated training before receiving Power User privileges and annually thereafter to maintain those privileges.
3. Training shall address, as applicable, system operation; authorized and prohibited uses; privacy and constitutional considerations; O.C.G.A. § 35-1-22; alert verification; GCIC and NCIC confirmation; search-reason documentation; custom hot list requirements; account security; data sharing; retention; audits; evidence preservation; and misuse reporting.
4. Current lesson plans and supporting instructional materials shall be maintained. Individual training completion and class records shall be documented and stored in authorized agency training-record system.
5. Material changes in law, policy, vendor functionality, security requirements, or operating procedures shall be communicated to affected users and shall be accompanied by supplemental training when appropriate.

G. Data Collection, Storage, Retention, and Evidentiary Preservation

1. ALPR data generally consists of vehicle or license plate images, date, time, location, direction, and related metadata. ALPR data does not, standing alone, contain registered-owner information. Any separate access to motor vehicle registration or personal information shall be limited to permissible law enforcement purposes and governed by the Driver's Privacy Protection Act, 18 U.S.C. §§ 2721-2725, and applicable CJIS, GCIC, and White County Sheriff's Office requirements.
2. The ALPR database may reside in a vendor-hosted environment. ALPR data collected for White County Sheriff's Office remains under White County Sheriff's Office control and shall be stored and maintained using security measures required by agency contract, applicable CJIS requirements, and this policy.
3. Consistent with O.C.G.A. § 35-1-22(b), captured ALPR data shall be stored upon collection and shall not be accessed except for a law enforcement purpose.

4. White County Sheriff's Office uses a thirty (30) day operational retention period for vendor-hosted Flock ALPR detection data, after which the vendor shall automatically purge the data unless it has been lawfully preserved for an investigation, prosecution, toll matter, litigation hold, or other documented law enforcement purpose. In no event shall unpreserved captured data be retained beyond the maximum period permitted by Georgia law.
5. ALPR data used in an open or ongoing investigation or prosecution shall be treated as evidence or investigative material, properly documented, and preserved in accordance with White County Sheriff's Office, Property-Evidence Unit, and the applicable records retention schedule.
6. Downloaded images, reports, exports, screenshots, or other preserved ALPR material shall be stored only in an authorized case, evidence, records, or investigative system and shall not remain solely on a local computer, personal device, removable media, or email account.
7. Pursuant to O.C.G.A. § 35-1-22(f), captured license plate data collected by a law enforcement agency is not subject to public disclosure under the Georgia Open Records Act. Requests for ALPR records, camera-location information, system contracts, audit records, or related materials shall be forwarded to the White County Sheriff's Office Open Records Unit for review under applicable law.

H. Accountability, Audits, and Annual Review

1. The Chief Deputy shall produce and review available ALPR audit reports monthly to assess compliance with this policy, identify irregular or incomplete searches, and verify that users have a documented law enforcement purpose.
2. In addition to the monthly system-level review, the Chief Deputy shall conduct a detailed random audit of at least five (5) ALPR users each month. Detailed audits should examine search reasons, case or CAD numbers, query parameters, custom hot list entries, data sharing, and any other activity necessary to determine compliance.
3. Audit findings, follow-up inquiries, corrective action, training, access restrictions, and referrals for investigation shall be documented and retained in accordance with the applicable records retention schedule.
4. Suspected misuse, unauthorized access, security incidents, or violations shall be reported immediately to the employee's supervisor, the Patrol Commander, and the Chief Deputy. When appropriate, the matter may also be referred to the Office of Professional Standards.
5. The Chief Deputy, or authorized designee, shall complete and document an annual review of this policy and the ALPR program. The review shall address user access, training, audits, equipment inventory and health, retention settings, vendor compliance, information-sharing relationships, legal changes, and recommended policy or operational revisions.

I. Privately Owned or Privately Funded ALPR Systems

1. White County Sheriff's Office recognizes that residents, homeowners' associations, businesses, or other entities may seek to purchase or fund privately owned ALPR systems and share detections with White County Sheriff's Office.
2. A privately owned or funded ALPR system shall not be linked to the White County Sheriff's Office network or shared with White County Sheriff's Office without prior approval from the Sheriff or authorized designee and an appropriate written agreement

addressing access, security, ownership, retention, costs, maintenance, and termination.

3. ALPR data received, accessed, downloaded, or retained by White County Sheriff's Office through a linked private system shall be treated as White County Sheriff's Office ALPR data for purposes of this policy and applicable law.
4. White County Sheriff's Office shall be provided the search and administrative capabilities necessary to support authorized law enforcement use and accountability. A linkage shall not provide a private owner or non-law-enforcement user access to White County Sheriff's Office hot lists, searches, alerts, investigative data, or other restricted information.
5. Unless otherwise established by written agreement, White County Sheriff's Office shall not be responsible for the acquisition, subscription, installation, maintenance, repair, replacement, connectivity, or other costs associated with a privately owned or funded system.
6. White County Sheriff's Office will not continuously monitor a privately-owned ALPR or video system and may suspend or terminate a connection when continued access is inconsistent with law, security requirements, agency policy, operational need, or the written agreement.

J. Disciplinary and Criminal Consequences

1. Alleged violations of this policy shall be investigated in accordance with White County Sheriff's Office, Internal Affairs Unit, or another applicable written directive.
2. An employee who intentionally or negligently misuses an ALPR system, account, database, detection, alert, search, custom hot list, or data may be disciplinary action up to and including termination.
3. Under O.C.G.A. § 35-1-22(d)(1), a person who knowingly requests, uses, obtains, or attempts to obtain captured license plate data under false pretenses or for a purpose other than a law enforcement purpose may be guilty of a misdemeanor of a high and aggravated nature.
4. Nothing in this section limits referral for criminal investigation or prosecution under any other applicable law.