Winchester Police Department
General Order

Order Name: **Automated License Plate Readers**	Order Number: **504**
Revision Date: 10/16/2026 (Revises 2-79 License Plate Readers)	Effective Date: 10/21/2026
Applies To: All Personnel	CALEA Standard (s): 41.3.9
By Authority Of:	Ronnie E. Lewis, Jr **Chief of Police or Designee**

I. PURPOSE

The purpose of this policy is to establish guidelines and procedures for the Winchester Police Department's Automated License Plate Reader system (ALPR).

II. POLICY

The Winchester Police Department may utilize an Automated License Plate Reader system to enhance public safety services provided by the Department and to improve citizen and officer safety. It is the policy of the Department that the ALPR system be utilized by trained department employees for official law-enforcement purposes only, as a tool to assist in gathering non-biased information related to vehicles involved in criminal investigations and missing persons. The ALPR system shall not be used to interfere with individuals engaged in lawful activities or to track individuals on the basis of lawfully protected speech. No employee shall query, access, download, retain, share, or otherwise use ALPR system data except for a purpose expressly authorized by Virginia Code § 2.2-5517(D) and this policy. All City personnel and contractors providing support or access services to the Department are subject to, and will comply with, this policy. All uses of ALPR technology shall comply with applicable federal and state laws, including VA Code § 2.2-5517, and shall be subject to strict data retention, access, and audit requirements to ensure transparency, accountability, and public trust.

III. DEFINITIONS

A. Alert- A visual and/or auditory notification that is sent out when the Automated License Plate Reader (ALPR) receives a potential match.

B. Audit Trail- All records of queries and responses in an automatic license plate recognition system, and all records of actions in which system data is accessed, entered, updated, shared, or disseminated, including:

   a. Date and time of access;

   b. License plate number or other data elements used to query the system;

   c. Specific purpose, as set forth in § 2.2-5517 (D), for accessing or querying the system, including the offense type for any criminal investigation;

   d. Associated call for service or case number; and

   e. Username of the person or persons who accessed or queried the system.

C. Notification- An alert from an automated license plate recognition system that a license plate or vehicle matches a license plate or vehicle in a database utilized by the automated license plate recognition system for comparison purposes.

D. Automated License Plate Reader (ALPR)- As defined in § 2.2-5517 (A) "A system of one or more high-speed cameras used in combination with computer algorithms to convert images of license plates, vehicles, or a combination of both into computer-readable data."

E. Audit-Trail Data - All forms of data collected or generated by an automated license plate recognition system for purposes of producing an audit trail.

F. Query - A search of ALPR system data based on information entered by the user, including a full or partial license plate number, vehicle identifying characteristics, date, time, location of an image, or other searchable system data.

G. System Data - All forms of data collected or generated by an ALPR system, including images of license plates and vehicles, vehicle identifying characteristics, and the date, time, location, and peripheral images associated with an image.

H. Vendor - A business, company, corporation, or other nongovernmental entity that contracts with a law-enforcement agency for the installation, use, or maintenance of an ALPR system.

I. Person Associated with Human Trafficking - A person who is either a suspected victim or alleged perpetrator of commercial sex trafficking or labor trafficking.

J. Publicly Post - To post on a website maintained by the Department, or another website on which the Department generally posts information, that is available to the public, or to clearly describe how the public may access such information.

K. Missing or Endangered Person - A person identified as missing or endangered based on information provided by the National Criminal Information Center, the National Center for Missing and Exploited Children, the Missing Children Information Clearinghouse, a qualifying Virginia alert program, or a substantially similar alert issued by another state, territory, the District of Columbia, or the United States.

IV. PROCEDURE

A. General

1. ALPR system access, use, and all data associated with the system are restricted for use in conducting official law enforcement business in accordance with the law.

2. Misuse of the ALPR system or the data obtained from this system may result in disciplinary action, including termination of employment. Additionally, persons found to be in violation of applicable laws are subject to criminal prosecution and/or civil actions.

3. Affected personnel and all newly hired employees who will use or access the ALPR system shall complete initial and biennial ALPR training.

B. Public Transparency and Awareness

1. The Department shall publicly post this policy and the Department's annual ALPR-use report, subject to redaction or exclusion of personal information, case-identifying information, information presenting an articulable safety concern, information protected by federal or state law, or sensitive criminal-justice information that could be compromised by disclosure.

2. Before or concurrent with implementing an ALPR system, the Department shall take reasonable measures to promote public awareness of the system's use.

C. Administration

1. The agency shall designate employee(s) with administrative oversight for the ALPR system. These responsibilities include the following:

a. Establishing and reviewing, on a recurring basis, protocols for access, collection, storage, and retention of ALPR data in

accordance with the law.

b. Conducting and documenting an internal audit at least once every 30 days. The audit shall review user access, queries, downloads, sharing or dissemination, data-retention exceptions, audit-trail completeness, and compliance with this policy and § 2.2-5517. The audit shall identify suspected unauthorized access or use and document corrective action, if any. Monthly audit records shall be forwarded to the Accreditation Manager for CALEA proof retention.

c. The Administrative Services Division Commander, or his/her designee shall receive the completed audit reports, ensure identified deficiencies or unauthorized uses are promptly referred for corrective action or investigation, and provide periodic summary reports to the Chief of Police or designee. Audit records shall be documented and retained in accordance with applicable records-retention requirements.

d. The designated employee shall complete and submit all ALPR data reports required by the Virginia Department of State Police (VSP) in the format, manner, and frequency prescribed by VSP on a quarterly basis, according to the VSP Memorandum titled Automated License Recognition/Reader (ALPR) Documentation dated February 27, 2026, unless superseded by VSP direction.

e. Facilitating procedures to ensure that databases used by the system provide notifications as set forth in § 2.2-5517 (D) are updated at least every 24 hours, or as soon as practicable after such updates become available.

f. Establishing protocols to preserve and document system data and audit-trail data associated with an ongoing investigation, prosecution, or civil action.

g. Serve as liaison between the department and ALPR vendor for repairs or updates as needed.

h. Remain apprised of any outages or other ALPR equipment issues and address such incidents accordingly.

i. The Administrative Services Division Commander, or designee, shall oversee the designated employee(s) assigned ALPR administrative duties.

j. Prior to querying system data, a user shall enter all information necessary to create the audit trail required by Virginia Code §

2.2-5517(D). Such information shall include the date and time of access; license plate number or other data elements used to query the system; authorized purpose, including offense type for a criminal investigation; associated call-for-service or case number; and username of the person accessing or querying the system. The Department shall not query or download system data unless the data are related to at least one purpose set forth in Virginia Code § 2.2-5517(D). Audit-trail data may be downloaded only for purposes of generating audit reports.

2. The Administrative Services Commander, or designee, shall submit the Department's annual ALPR-use report to the Department of State Police by April 1 of each year, in the format required by the Department of State Police, for the preceding calendar year. *The annual report shall* include the specific categories required by Virginia Code § 2.2-5517(I), including:

   a. The total number of ALPR cameras owned or leased by the Department at the conclusion of the calendar year, including the number designed to be affixed inside or on a motor vehicle, permanently affixed adjacent to a highway, or temporarily affixed or placed adjacent to a highway;

   b. A list of all state and federal databases against which system data were compared, unless the existence of a database is not public;

   c. The total number of times the system was queried, including the specific authorized purposes of the queries and the offense types for queries conducted as part of criminal investigations;

   d. The race, ethnicity, age, and gender of each individual identified as a suspect and charged with a criminal offense as a result of a system query conducted as part of a criminal investigation;

   e. The number of motor vehicles stopped based on ALPR notifications, including the specific reason for each notification;

   f. The race, ethnicity, age, and gender of each driver stopped based on an ALPR notification;

   g. Whether other law-enforcement agencies are permitted to access Department system data and, if so, the identity of each agency granted access;

   h. The number of identified instances of unauthorized use of or access to the system, including the nature and circumstances of each instance; and

   i. The number of subpoena duces tecum, search warrants, and other third-party requests for system data or audit-trail data,

including the identity of the requesting entity and whether any data were provided, unless disclosure of the request is prohibited by law.

D. Training Requirements

1. Employees must attend training prior to using or accessing the ALPR system.

2. Facilitation of training location and presentation of content is at the discretion of the Training Division.

3. ALPR training shall occur biennially and shall include the following:

   a. Legal update of relevant ALPR matters

   b. Administrative procedures

   c. Technical procedures

4. Agencies shall maintain a record of each employee's completion of ALPR training in accordance with existing training records policies.

E. Automated License Plate Reader System Usage

1. Only WPD personnel who have been properly trained in the ALPR system's operation shall be permitted to access the system and receive alerts. Vendor access is governed exclusively by Section IV.H.5 and the Department's contract with the vendor.

2. The ALPR system shall only be used for the following pursuant to VA Code § 2.2-5517(D):

   a. As part of a criminal investigation into an alleged violation of the Code of Virginia or any ordinance of any county, city, or town where there is a reasonable suspicion that a crime was committed;

   b. As part of an active investigation related to a missing or endangered person, including whether to issue an alert for such person, or a person associated with human trafficking; or

   c. To receive notifications related to a missing or endangered person, a person with an outstanding warrant, a person associated with human trafficking, a stolen vehicle, or a stolen license plate.

3. ALPR Alerts/Notifications: An ALPR notification alone does not

constitute reasonable suspicion for a traffic stop. Prior to stopping a vehicle based on an ALPR notification, an officer shall:

a. Develop independent reasonable suspicion for the stop; or

b. Confirm that the license plate or vehicle identifying characteristics match the database information.

c. The officer shall document in the incident report or CAD record whether the stop was based on independent reasonable suspicion or confirmation of the plate/vehicle identifying characteristics.

d. When practical, the officer should verify through an appropriate criminal-justice information source that the underlying notification remains active and valid.

4. Searches of historical ALPR data shall be completed in accordance with the law. Historical ALPR-data queries shall comply with the audit-trail requirements in Section IV.C.1.i.

5. An officer may request that a specific license plate or vehicle be entered into the ALPR system only for a purpose authorized by § 2.2-5517(D). The request shall identify the authorized purpose, associated case number or call-for-service number, applicable offense type when related to a criminal investigation, requested duration, and any required supporting documentation. The Department shall maintain a record of the request, approval, entry date, expiration date, and removal date.

F. ALPR Data Sharing and Dissemination

1. System data and audit-trail data may be shared or disseminated only as authorized by VA Code § 2.2-5517(F). Authorized disclosures include sharing with another law-enforcement agency for an authorized purpose; the attorney for the Commonwealth for a purpose authorized by § 2.2-5517(D), or for purposes of complying with discovery or a court order in a criminal proceeding; a person who is the subject of a criminal or civil proceeding, when required for discovery or by court order; pursuant to a court order or court-issued subpoena duces tecum; with the vendor for maintenance or quality-assurance purposes; or to alert the public in the event of an emergency, or regarding a missing or endangered person, person associated with human trafficking, or person with an outstanding warrant. Any law-enforcement agency receiving access to or data from the Department shall comply with all applicable provisions of § 2.2-5517.

2. A request for system data or audit-trail data from another law-enforcement agency shall include the requesting agency; the requesting

member's name, badge number, or employee identification number; the agency case number; case type; and the specific authorized purpose under Virginia Code § 2.2-5517(D). The Department shall document the request, authorization decision, information disclosed, date of disclosure, and receiving agency or recipient.

3. System data and audit-trail data are not subject to disclosure under the Virginia Freedom of Information Act. Requests from non-law-enforcement entities shall be denied unless disclosure is authorized by VA Code § 2.2-5517(F), required for criminal discovery, or compelled by a court order or court-issued subpoena duces tecum.

4. The Department shall not sell system data or audit-trail data and shall not share or disseminate such data to a database of another state, federal, private, or commercial entity, except as expressly authorized by Virginia Code § 2.2-5517(F).

5. Records shall be retained regarding requests for ALPR data in accordance with the law.

6. The Department shall report all required data to the Department of the State Police as prescribed in § 2.2-5517 (I).

G. Data Collection, Storage, and Retention

1. The Administrative Services Commander shall ensure that all ALPR data retention practices are performed in accordance with the law as prescribed in § 2.2-5517 (E).

2. System data may include plate images, vehicle images/characteristics, date, time, location, and peripheral images from which analytical data may be extracted. License plate reads and notification data are encrypted, uploaded, and stored in a department-approved cloud-hosted storage solution.

3. System data shall be retained for no more than 21 days from the date of capture, unless the particular system data or audit-trail data to be retained is part of an ongoing investigation, prosecution, or civil action. For each preservation exception, the Department shall document the case number, legal purpose, records custodian, preservation date, data preserved, and disposition trigger. Preserved system data and audit-trail data shall be retained until the investigation concludes without criminal charges or until final disposition of the related criminal or civil matter, including direct appeals and applicable state or federal habeas corpus proceedings. Data shall be exported from the ALPR operating system

before automated deletion when necessary to preserve the data in accordance with this policy, the documented preservation exception, and applicable Library of Virginia records-retention requirements.

4. Any data retained for evidentiary purposes shall be maintained as part of the criminal investigative file.

5. Any data preserved for more than 21 days shall be maintained per the Library of Virginia Records Retention and Disposition Schedule.

6. Any system data not subject to a documented preservation exception under Virginia Code § 2.2-5517(E) shall be automatically purged no later than 21 days after the date of capture, or earlier at the Department's request, in a manner that destroys the data and renders it unrecoverable by both the Department and the vendor.

7. The ALPR System maintains all required audit-trail data. This information can be accessed and reviewed by the System Administrator to ensure compliance both internally and externally with agency policies, laws, and vendor contractual agreements. Audit-trail data shall be purged after two years from the date of capture in a manner that destroys the data and renders it unrecoverable by both the vendor and the Department, unless retained under a documented § 2.2-5517(E) preservation exception.

H. Data Security and Access

1. The Department shall maintain security procedures to protect the ALPR system, system data, and audit-trail data from unauthorized access, destruction, use, modification, or disclosure.

2. Access shall be limited to authorized, trained personnel with a demonstrated official need. Each user shall be assigned unique credentials. Shared accounts are prohibited.

3. The System Administrator shall establish role-based access permissions and shall review user access at least quarterly and whenever an employee transfers, separates from employment, loses authorization, or is subject to an investigation involving potential system misuse. Access shall be promptly modified, suspended, or terminated as appropriate.

4. The system shall use secure authentication and vendor-hosted or Department-hosted storage that meets applicable Virginia Information Technologies Agency information-security standards and the requirements of Virginia Code § 2.2-5517.

5. Vendor access to system data or audit-trail data shall occur only at the request of the Department and only for maintenance or quality-assurance purposes.

6. Any actual or suspected unauthorized access, use, modification, disclosure, loss, or destruction of ALPR system data or audit-trail data shall be promptly reported to the System Administrator and the appropriate chain of command. The incident shall be documented, investigated, and addressed through corrective action, disciplinary action, and notification procedures as appropriate.

7. The Department's contract with the ALPR vendor shall require immediate notice to the Department of any subpoena duces tecum, search warrant, or other third-party request for system data or audit-trail data, unless notice is prohibited by law.

8. The Department shall use only an automatic license plate recognition system approved for law-enforcement use in the Commonwealth by the Division of Purchases and Supply. The Department's contract with the vendor shall state that system data and audit-trail data are the property of the Winchester Police Department. The contract shall further specify that the system meets the requirements of Virginia Code § 2.2-5517(B) and shall require the vendor to comply with all applicable requirements of Virginia Code § 2.2-5517, including:

    a. Limitations on vendor access to, sale of, sharing of, or dissemination of system data and audit-trail data;

    b. The capability to purge system data no later than 21 days after the date of capture, or earlier at the Department's request, in a manner that renders the data unrecoverable by both the vendor and the Department;

    c. The capability to produce audit-trail data upon Department request and to purge audit-trail data two years after the date of capture in a manner that renders the data unrecoverable by both the vendor and the Department;

    d. Updates to notification databases at least every 24 hours, or as soon as practicable after updates become available;

    e. Compliance with applicable Virginia Information Technologies Agency information-security standards; and

    f. Immediate notice to the Department of any subpoena duces tecum, search warrant, or other third-party request for system data or audit-trail data, unless notice is prohibited by law.