Sweetwater Police Department

Law Enforcement

Policies and Procedures

Subject: Automated License Plate Reader (ALPR) **Policy Number: 18.18**

Issue Date: 09-04-2026 **Revision Date: _____**

Approval Authority
Title and Signature:

CHAPTER 18.18

AUTOMATED LICENSE PLATE READER (ALPR)

1.00 PURPOSE

The purpose of this policy is to establish guidelines governing the use of Automated License Plate Reader (ALPR) technology by the Sweetwater Police Department. ALPR technology is intended to enhance public safety, assist criminal investigations, recover stolen vehicles, locate wanted or missing persons, and improve officer safety while safeguarding individual privacy, civil rights, and civil liberties.

ALPR technology shall be used as a law enforcement investigative tool and shall not be used as a means of indiscriminate or generalized surveillance.

1.10 POLICY STATEMENT

It is the policy of the Sweetwater Police Department that ALPR systems shall be used only for official law enforcement purposes and in a manner consistent with the United States Constitution, the Constitution and laws of the State of Tennessee, applicable federal law, Department policy, Department values, and legitimate public safety objectives.

All ALPR use shall be authorized, documented, auditable, and subject to supervisory review. Department personnel shall access ALPR systems only after completing required training and receiving authorization from the Chief of Police or designee.

1.20 DEFINITIONS

A. Automated License Plate Reader (ALPR) - A system consisting of cameras and software designed to capture images of vehicle license plates and convert those images into searchable data, together with associated metadata such as date, time, and location.

B. ALPR Data - Digital information collected or generated by an ALPR system, including license plate numbers, vehicle descriptors, associated images, date, time, location, direction of travel, and related metadata.

C. Hot List - A database or list of license plates associated with vehicles or persons of legitimate law enforcement interest, including stolen vehicles, wanted persons, missing or endangered persons, AMBER Alerts, Silver Alerts, BOLOs, and active investigations.

D. Authorized User - A Department member who has completed required training and has been granted access to the ALPR system.

E. ALPR Hit - A notification generated when a scanned license plate matches a plate contained in an approved Hot List.

1.30 PERMISSIBLE USES OF ALPR TECHNOLOGY

The use of ALPR technology, associated equipment, and databases is authorized only for official law enforcement and public safety purposes.

A. Attempt to identify and/or locate a vehicle related to a criminal investigation or other legitimate law enforcement activity.

B. Attempt to identify vehicle owner(s) and/or occupant(s) when there is a legitimate law enforcement basis to believe such person has committed a criminal offense, is involved in or planning criminal activity, or may be a missing person, crime victim, or witness.

C. Prevent, detect, investigate, and/or assess potential safety threats to members of the public, law enforcement officers, public officials, critical infrastructure, or public events.

D. Identify vehicles during lawful patrol or traffic enforcement that have suspended, revoked, or otherwise unlawful registrations when authorized by law.

E. Locate stolen vehicles or stolen license plates.

F. Locate wanted persons or persons who are missing, endangered, or the subject of an AMBER Alert, Silver Alert, BOLO, or similar law enforcement notification.

G. Support felony and serious misdemeanor investigations, homeland security functions, emergency response, and other legitimate criminal justice purposes.

1.40 SEARCH DOCUMENTATION

The use of ALPR technology to search license plates or vehicles shall be limited to a specific investigation or other legitimate law enforcement activity. All ALPR searches shall be documented with a corresponding case number, incident report number, citation number, CAD event number, or complaint card.

If a search initiates a new investigation and cannot be associated with an existing complaint or investigation, a complaint card or CAD event shall be created documenting the officer's actions and the reason for the search. The documented number shall accurately reflect the law enforcement purpose for which the search was conducted and shall be subject to supervisory review and periodic audit.

These requirements apply to all Department personnel, including personnel assigned to local, state, or federal task forces who access Sweetwater Police Department ALPR data or systems.

1.50 USE OF HOT LISTS AND ALPR HITS

A. Authorized personnel should ensure that the most current Hot List data available is used or uploaded when applicable.

B. When an ALPR system indicates a Hot List hit, the officer shall, prior to taking enforcement action when circumstances reasonably permit, verify that the captured plate image matches the displayed plate number and state of registration.

C. The officer shall use TIES/NCIC, departmental systems, or other authorized law enforcement databases as appropriate to determine whether further law enforcement action is warranted.

D. No enforcement action shall be based solely upon an ALPR alert without verification. Officers shall consider the totality of the circumstances and comply with all constitutional and statutory requirements before initiating a stop, detention, search, or arrest.

1.60 PROHIBITED USES

ALPR systems shall NOT be used for:

A. Personal, private, or non-duty purposes.

B. Monitoring individuals or groups based solely on race, color, ethnicity, national origin, religion, sex, political affiliation or beliefs, or First Amendment-protected activity.

C. Generalized surveillance or tracking without a legitimate law enforcement or public safety purpose.

D. Immigration enforcement unless directly related to a lawful criminal investigation or otherwise authorized by applicable law and Department policy.

E. Civil or administrative enforcement unrelated to public safety unless specifically authorized by law and Department policy.

F. Any purpose that violates constitutional protections, applicable law, or Department policy.

1.65 STATE LAW REFERENCE - T.C.A. § 55-10-302

Tennessee Code Annotated § 55-10-302 governs automated license plate recognition systems and captured plate data collected or retained by governmental entities. The statute defines an automated license plate recognition system, captured plate data, and governmental entity, and provides that captured plate data may not be stored for more than ninety (90) days unless the data is retained or stored as part of an ongoing investigation.

When captured plate data is retained as part of an ongoing investigation, the data shall be destroyed at the conclusion of an investigation that does not result in criminal charges being filed, or at the conclusion of any criminal action undertaken in the matter involving the captured plate data, as required by T.C.A. § 55-10-302(b). Nothing in this policy authorizes retention beyond the limits established by Tennessee law.

1.70 DATA RETENTION AND PRESERVATION

A. As a Department policy more restrictive than the ninety (90) day statutory maximum in T.C.A. § 55-10-302, ALPR data shall normally be retained for thirty (30) days, unless the data is lawfully preserved as part of an ongoing investigation or a different retention period is required by applicable law or court order.

B. ALPR data shall be deleted after the applicable retention period unless it is associated with an active investigation, has been preserved as evidence, is subject to a court order or legal hold, or must otherwise be retained by law.

C. Data preserved as evidence shall be handled in accordance with Department evidence procedures and applicable records-retention requirements.

1.80 DATA SHARING

A. ALPR data may be shared with other law enforcement agencies only for legitimate law enforcement or criminal justice purposes and in accordance with applicable law and Department policy.

B. The Department may restrict or limit external access to or sharing of ALPR data as necessary to ensure compliance with this policy, protect investigations, safeguard privacy, or maintain system security.

C. Personnel shall not disseminate ALPR information to unauthorized persons or entities.

1.90 SECURITY, AUDIT, AND ACCOUNTABILITY

A. All ALPR system access and queries shall be logged or otherwise documented in a manner that permits auditing.

B. The Sweetwater Police Department shall conduct periodic audits of ALPR usage to verify that searches and access are consistent with legitimate law enforcement purposes and this policy.

C. Misuse of ALPR systems or data may result in disciplinary action, revocation of access privileges, and/or criminal or civil penalties where applicable.

D. Authorized users shall protect usernames, passwords, and other access credentials and shall immediately report suspected unauthorized access, loss, or disclosure.

2.00 ALPR PROGRAM ADMINISTRATOR

The Chief of Police shall designate an ALPR Program Administrator who shall be responsible for:

A. System management and access control.

B. Training coordination.

C. Policy compliance.

D. Audit review.

E. Vendor coordination.

F. Periodic review of program effectiveness, data-sharing practices, and security controls.

2.10 TRAINING

Prior to receiving ALPR access, Department personnel shall complete Department-approved training concerning system operation, constitutional limitations, privacy and civil liberties, documentation requirements, verification of alerts, data security, auditing, and applicable federal and Tennessee law. Refresher training may be required as directed by the Chief of Police or designee.

2.20 PUBLIC TRANSPARENCY

The Sweetwater Police Department may provide general information to the public regarding the purpose and scope of its ALPR program, the general types of data collected, retention practices, access controls and audit safeguards, and general deployment practices.

To protect public safety, individual privacy, system security, and the integrity of law enforcement operations, the Department may withhold information from public disclosure to the extent permitted by Tennessee law, including sensitive investigative information, security-related information, and information protected by applicable statutory exemptions.

2.30 PUBLIC RECORDS REQUESTS

Requests for ALPR records shall be processed in accordance with the Tennessee Public Records Act, T.C.A. Title 10, Chapter 7, Part 5, and other applicable federal and Tennessee law. Each request shall be evaluated based upon the nature of the records requested and any applicable statutory exemption, confidentiality provision, court order, law enforcement privilege, or other lawful basis for withholding or redacting information.

Questions concerning disclosure shall be referred to the Chief of Police, the Department's records custodian, and/or legal counsel as appropriate.

2.40 POLICY REVIEW

This policy shall be periodically reviewed by the Chief of Police or designee and revised as necessary to address changes in law, technology, Department operations, vendor capabilities, and recognized law enforcement practices.