SOUTH KINGSTOWN POLICE DEPARTMENT

1790 KINGSTOWN RD., WAKEFIELD, RI 02879

POLICY NUMBER	ORDER TYPE	ORIGINAL ISSUE DATE	EFFECTIVE DATE
460.11	OPERATIONAL POLICY	04/19/2026	04/19/2026
CHAPTER: SUBSECTION		**TITLE**	
LAW ENFORCEMENT OPERATIONS EQUIPMENT & UNIFORMS		AUTOMATED LICENSE PLATE READERS (ALPR)	
RE-EVALUATION DATE		**REVISION DATES**	
ANNUAL		-	
DISTRIBUTION	**REFERENCE**		**PAGES**
ALL PERSONNEL	N/A		8

I. PURPOSE

The purpose of this policy is to establish clear guidelines governing the lawful, ethical, and transparent capture, storage, use, auditing, and oversight of data obtained through Automated License Plate Reader (ALPR) technology, while safeguarding privacy rights, civil liberties, and public trust.

II. POLICY

It is the policy of the South Kingstown Police Department to utilize ALPR technology solely for legitimate law enforcement purposes and in a manner consistent with applicable law, professional standards, and constitutional protections.

ALPR systems and data are the property of the Department and are for official use only. ALPR technology is used to identify vehicles, not persons, and an ALPR alert alone does not establish reasonable suspicion or probable cause for enforcement action.

III. DEFINITIONS

a) **Administrative Immigration-Related Investigation:**
A civil or non-criminal inquiry or enforcement action conducted to identify, locate, detain, or remove an individual based solely on actual or suspected immigration status, including actions undertaken by U.S. Immigration and Customs Enforcement (ICE) or officers designated under 8 U.S.C. § 287(g).

b) **Alert:**
A read matched to a license plate that has previously been identified as a vehicle license plate of interest or that has been manually registered for detection (also referred to as a hit).

c) **ALPR Access Event:**
Any instance in which a user queries, views, searches, analyzes, exports, or disseminates ALPR data.

d) **ALPR Administrator:**
A Department member designated by the Chief of Police to oversee the administration, management, compliance, auditing, and operational oversight of the Department's Automated License Plate Reader (ALPR) program.

e) **Audit:**
A documented review of ALPR access logs, searches, hot list activity, and data dissemination conducted to ensure compliance with this policy, training requirements, and applicable law.

f) **Automated License Plate Reader (ALPR):**
A system of cameras and software that passively captures images of license plates and associated vehicle characteristics and converts them into searchable digital data.

g) **Fixed ALPR System:**
ALPR cameras affixed to a permanent structure, such as a pole, traffic barrier, or bridge.

h) **FOUO (For Official Use Only):**
Information restricted to authorized personnel for official law enforcement purposes and protected from unauthorized disclosure.

i) **Historical Search:**
A search of stored ALPR data conducted to identify prior vehicle locations, movements, or travel patterns.

j) **Hot List:**
A list of license plate numbers or partial identifiers associated with vehicles of

law enforcement interest, originating from authorized sources including NCIC, state motor vehicle agencies, local or regional law enforcement agencies, or Department-generated investigative entries. All hot list entries must be supported by a legitimate law enforcement purpose, approved by a supervisor, documented with a case number or operational justification, and assigned an expiration date.

k) **Mobile ALPR System:**
ALPR cameras affixed to an authorized vehicle for mobile deployment, either permanently (hardwired) or temporarily (e.g., magnet-mounted).

l) **Portable ALPR System:**
ALPR cameras that are transportable and can be moved and deployed at various locations or venues.

m) **Read:**
A digital image of a license plate and/or vehicle, along with associated metadata (including date, time, and geographic location), captured by the ALPR system (also referred to as a detection or scan).

n) **Sensitive Location:**
A location where monitoring may implicate constitutionally protected activity, including but not limited to places of worship, medical or mental health facilities, educational institutions, or political gatherings.

o) **Unauthorized Use:**
Any access, query, analysis, dissemination, or use of ALPR data inconsistent with this policy, Department training, or applicable law.

p) **User:**
Any individual authorized to access or use the ALPR system, including sworn officers and approved professional staff.

IV. ADMINISTRATION, AUTHORIZED USE, AND OVERSIGHT

The ALPR Administrator, designated by the Chief of Police, shall be responsible for oversight, compliance, user access management, training coordination, hot list documentation review, and audit preparation associated with the Department's ALPR program..

ALPR systems may be used only for official law enforcement purposes, including but not limited to identifying stolen vehicles or plates, locating vehicles associated with missing or endangered persons, supporting active criminal investigations, enhancing officer safety, and supporting lawful public safety operations.

V. OPERATIONAL REQUIREMENTS AND HOT LIST MANAGEMENT

Prior to taking any enforcement action based on an ALPR alert, officers shall visually verify the license plate characters and vehicle descriptors, confirm the alert status through RILETS or Dispatch, and establish reasonable suspicion or probable cause independent of the ALPR alert.

Requests for the creation of ALPR hot list entries may be submitted by any sworn officer or dispatcher. All hot list entries shall require approval by the Administrative Lieutenant, Executive Command Staff member, or their designee prior to activation. Each entry must include a documented case number or operational justification and an expiration date. The ALPR Administrator shall ensure proper documentation, tracking, and auditing of all approved hot list entries in accordance with Department policy.

VI. DOCUMENTATION, DATA SHARING, AND PROHIBITED USES

All ALPR searches, enforcement actions, and data dissemination shall be documented and logged in accordance with Department policy.

ALPR data may be shared only with authorized entities for legitimate law enforcement purposes and in accordance with applicable law and approved agreements.

The ALPR system shall not be used for administrative immigration-related investigations. No officer from any agency trained or designated under 8 U.S.C. § 287(g) shall be permitted to access or utilize the Department's ALPR system or data for such purposes.

VII. PRIVACY, AUDITING, AND COMPLIANCE

ALPR systems shall not be intentionally used to monitor constitutionally protected activities absent a legitimate, documented law enforcement purpose.

Operational Security and Public Disclosure

To protect the integrity of law enforcement operations and the effectiveness of ALPR technology, the specific locations of fixed, portable, or mobile ALPR deployments shall not be publicly disclosed.

Public disclosure of specific ALPR locations can compromise investigative effectiveness, reduce the deterrent value of the technology, and enable individuals to avoid or circumvent detection. Additionally, disclosure of camera locations increases the risk of vandalism or intentional damage to ALPR equipment, resulting in avoidable repair costs and unnecessary expense to the Town.

The Department may provide general information regarding the use and purpose of ALPR technology; however, information that would reveal specific camera locations, deployment patterns, or operational capabilities shall be considered law enforcement sensitive and shall not be released, except as required by law or court order.

Equitable Deployment and Community Impact

The Department recognizes that transparency and fairness are essential to maintaining public trust.

ALPR placement decisions are based on objective, data-driven public safety considerations, including traffic flow, roadway safety, crime trends, and investigative effectiveness, and are not based on the socioeconomic status, race, ethnicity, or demographic composition of any neighborhood or population.

ALPR technology is deployed strategically to support town-wide public safety objectives and investigative outcomes. All ALPR deployment decisions shall be subject to approval by the Chief of Police and shall be guided by strategic planning and ongoing review to ensure fair, lawful, and effective use consistent with this policy.

Auditing and Compliance

The Department shall conduct regular audits of ALPR system access and use to ensure compliance with this policy, training requirements, and applicable law.

Quarterly audits shall be conducted by the ALPR Administrator or designee and shall include a random review of no less than ten percent (10%) of all ALPR access events during the audit period or fifty (50) records, whichever is greater.

In addition to random sampling, audits shall include targeted review of any ALPR access that appears inconsistent with this policy, including undocumented searches, unusual access patterns, external data sharing, or access associated with a public complaint or internal inquiry.

Immediate audits shall be conducted upon receipt of a public complaint, identification of irregular system access, detection of a system anomaly, or direction from command staff.

Audit findings shall be documented and retained in accordance with Department records retention requirements and protected as official Department records. Audit procedures are further detailed in Addendum A – ALPR Audit Standard Operating Procedure.

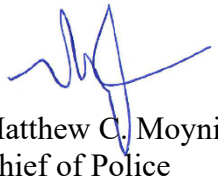
VIII. PUBLIC COMPLAINTS, MISUSE, AND TRAINING

Any member of the public who believes their information was accessed or used improperly may file a complaint with the Department. Complaints shall be investigated, and findings communicated to the complainant to the extent permitted by law.

Unauthorized use or misuse of ALPR systems or data may result in disciplinary action up to and including termination, as well as potential civil or criminal liability.

Only personnel who have completed Department-approved ALPR training may access or operate the ALPR system. Refresher training shall be provided as required.

By Order of:



Matthew C. Moynihan
Chief of Police

ADDENDUM A

ALPR Audit Standard Operating Procedure

Audit Standard
Quarterly audits shall include a review of no less than ten percent (10%) of all ALPR access events or fifty (50) records, whichever is greater, with full review of all defined high-risk access categories. Audit findings shall be documented and retained for a minimum of five (5) years.

1) PURPOSE

a) This addendum establishes standardized procedures for auditing ALPR system access and use to ensure compliance with Department policy, training, and applicable law.

2) RESPONSIBILITY

a) The Chief of Police or designee serves as the ALPR Audit Authority. Audits shall be conducted by the ALPR Administrator or a command-level designee who does not routinely operate the system when practicable.

3) AUDIT FREQUENCY

a) Quarterly audits shall be conducted each calendar year. Immediate audits shall be conducted when triggered by a public complaint, identified irregular access, system anomaly, or direction from command staff.

4) AUDIT SCOPE AND SAMPLING

a) Each quarterly audit shall include a random review of no less than ten percent (10%) of all ALPR access events during the audit period or fifty (50) records, whichever is greater.

b) In addition to random sampling, audits shall include targeted review of any ALPR access that may be inconsistent with this policy, including but not limited to:

1. Searches conducted without a documented case number or operational justification
2. Historical searches of stored ALPR data reviewing multiple prior detections of a vehicle over a defined period of time
3. Manual or custom hot list entries
4. Searches involving sensitive locations
5. External data sharing or dissemination
6. Access by supervisors, administrators, or analysts
7. Access related to public complaints or internal inquiries
8. After-hours or irregular access patterns

5) **RECORD REVIEW CRITERIA**
   a) Each audited record shall be reviewed for user identity, date and time of access, documented purpose, associated case number, policy compliance, enforcement action taken, data sharing activity, and retention status.
6) **FINDINGS AND CLASSIFICATION**
   a) Audit findings shall be classified as compliant use, training deficiency, policy violation, or system/technical issue.

7) **CORRECTIVE ACTION**
   a) Training deficiencies shall result in documented retraining. Policy violations shall be referred for administrative review or internal investigation. Corrective actions shall be documented.

8) **DOCUMENTATION AND RETENTION**
   a) Audit summaries shall be documented and retained for a minimum of five (5) years and protected as official Department records.

9) **CONFIDENTIALITY**
   a) Audit materials are for official use only and shall be safeguarded in accordance with Department policy.