



State of Rhode Island

DIVISION OF STATE POLICE

**State Police Headquarters, 311 Danielson Pike, North Scituate, Rhode Island 02857
OFFICE OF THE SUPERINTENDENT AND DIRECTOR OF PUBLIC SAFETY**

**Colonel Darnell S. Weaver
Superintendent**

Background and Review Process

On August 18, 2026, Governor Dan McKee directed a comprehensive 60-day review to develop uniform statewide standards governing the use of Automated License Plate Readers (ALPR) technology and the data collected through that technology. As part of that process, Colonel Darnell Weaver and members of the Rhode Island Department of Public Safety convened a working group that included representatives of the Rhode Island Police Chiefs Association, the Rhode Island League of Cities and Towns, and the Providence Police Department. The working group met in person and virtually throughout the 60-day review period to evaluate existing ALPR practices and develop a Statewide Policy on Automated License Plate Readers ("Statewide Model Policy") and a Model Memorandum of Understanding governing the circumstances under which ALPR data may be shared with external law enforcement agencies.

Core Safeguards in the Statewide Model Policy

The resulting Statewide Model Policy establishes clear, uniform guardrails for the responsible use of ALPR technology by law enforcement agencies across Rhode Island, while preserving its legitimate public safety benefits. Key safeguards include:

- **Data Retention:** Unless preserved as part of an authorized investigation, ALPR data must be deleted no later than 30 days after the data was captured. Data must be owned by and remain under the control of the police department and may never be sold to third parties.
- **Data Sharing:** A police department may only share ALPR data with another law enforcement agency contingent on a memorandum of understanding in place detailing the access and use of ALPR data. There can be no sharing of data with non-law enforcement entities. Rhode Island law enforcement agencies are prohibited from sharing ALPR data with the U.S. Immigration and Customs Enforcement or with any external law enforcement agency regarding any criminal investigation that concerns a crime not recognized under Rhode Island law.
- **Authorized Uses:** ALPR technology and data must be accessed and used for valid law enforcement purposes only. All ALPR system access is limited to (i) criminal investigations of suspected violations of federal or Rhode Island law, (ii) active investigations into missing persons, endangered persons, or human trafficking, and (iii) receipt of notifications related to stolen vehicles, stolen license plates, missing persons, endangered persons, or human trafficking.

- **Prohibited Uses:** Use of ALPR technology or data for any purpose other than a valid law enforcement purpose is prohibited. Prohibited uses include use based solely on a protected characteristic or class (i.e. race, sex, religion, gender identity, etc.); personal use; interference with any individual engaged in a lawful activity, including lawfully protected speech; immigration enforcement; harassment or intimidation; U.S. Immigration and Customs Enforcement; any private organizations or entities; investigations into reproductive or gender-affirming healthcare; and any matter where the criminal investigation concerns a crime that is not recognized under Rhode Island law.
- **Training of ALPR Operators:** At a minimum, ALPR operators must receive training on the usage of the ALPR system, data sources, legal responsibilities and ramifications; as well as training on the Statewide Model Policy.
- **Supervisory Oversight of ALPR Use:** No license plate will be added to a hotlist without the approval of a supervisor. Supervisors who become aware of a violation of the Policy shall ensure appropriate remedial action or referral for disciplinary action.
- **Internal Data Security and Access:** At a minimum, security controls shall include multi-factor authentication, encrypted communications, and other reasonable physical, technological, administrative, procedural, and personnel security measures to mitigate the risks of unauthorized access to the system
- **Auditing:** At a minimum, an audit shall occur each quarter to ensure compliance with Information security and privacy laws; queries are conducted consistent with this policy's Authorized Uses; queries contain an associated reason and report number; only trained, authorized users are conducting searches; outdated information is cleared from the system.
- **Violations of Policy:** Anyone who engages in an impermissible use of the ALPR system or associated data may be subject to civil liability, criminal prosecution, and/or administrative sanctions, including termination.

Recommendations and Next Steps:

The working group recommends that law enforcement agencies across Rhode Island adopt the Statewide Model Policy as the minimum standard governing the use of ALPR technology and ALPR data. The Policy is intended to establish a consistent statewide baseline while allowing individual departments to adopt additional safeguards where appropriate.

At Governor McKee's direction, the State Police will maintain its pause on new ALPR installations.

The working group will continue to review the Statewide Model Policy on an annual basis and recommend updates as necessary to account for changes in technology, law, and law-enforcement practices.