



BRISTOL POLICE DEPARTMENT

SUBJECT: Automated License Plate Readers (ALPR) RISP Flock Camera System	GENERAL ORDER NO. 300.25
SECTION: 300. – Law Enforcement Operations	Pages: 13
SUBSECTION: 00. - General	AMENDS/SUPERSEDES: EFFECTIVE DATE: January 20th, 2026 REVISED DATE: REVIEW DATE: As Necessary

NOTE: This written directive is for the internal governance of the Bristol Police Department and is not intended and should not be interpreted to establish a higher standard of care in any civil or criminal action that would otherwise be applicable under existing law.

INDEX WORDS:

I. PURPOSE:

The purpose of this policy is to establish guidance for the authorized capture, storage, review, and use of digital data obtained through Automated License Plate Reader (ALPR) technology. The ALPR (Flock Camera system) is owned and managed by the Rhode Island Department of Public Safety (Rhode Island State Police) and was acquired through grant funding.

The Rhode Island State Police have made this technology available to twenty-one (22) municipalities throughout the State of Rhode Island for use on state roadways. In accordance with the RI Department of Public Safety (RI State Police) policy and memorandum of understanding, ALPR data shall not be used or shared for administrative immigration enforcement purposes.

II. POLICY:

It is the policy of the Bristol Police Department to utilize Automated License Plate Reader (ALPR) technology to capture digital license plate data and images for legitimate local law enforcement and public safety purposes as approved by the Chief of Police, while recognizing and protecting the established privacy rights of the public.

A. Authorized Use:

1. Access to FLOCK ALPR data is granted solely for law enforcement and public safety purposes, including but not limited to criminal investigations, active searches for stolen vehicles, missing persons, or suspects in serious crimes.

B. Prohibition and Data Sharing:

1. The Bristol Police shall not share, disseminate, forward, or otherwise provide access to any data, images, or alerts obtained from the Rhode Island State Police FLOCK ALPR system to any third party, including but not limited to:

2. Other municipal or state agencies that have not entered into a substantially similar MOU with the Rhode Island State Police;

3. U.S. Immigration and Customs Enforcement or any external agency when the purpose of that agency or request is the enforcement of potential violations of federal civil immigration law; and;

4. Any private organizations or entities.

C. Violation of Data Sharing Restrictions:

A. Any unauthorized disclosure, sharing, or use of Rhode Island State Police FLOCK ALPR data in violation of this MOU will result in immediate revocation of access privileges for the outside agency. Additional administrative or legal actions may also be pursued at the discretion of the Rhode Island State Police and/or the State of Rhode Island.

III. DEFINITIONS:

A. AUTOMATED LICENSE PLATE READERS (ALPRs): Also known as license plate readers (ALPRs)—use image-processing technology combined with sophisticated computer algorithms capable of converting the images of license plates to electronically readable data.

ALPR DATA: Scan files, alert data, and any other documents or data generated by, or obtained through, utilization of the ALPR system.

ALPR ADMINISTRATOR: The Superintendent of the Rhode Island State Police or his designee(s), serves as the ALPR Administrator for the Division. The Administrator may order the deployment of the ALPR systems for use in various efforts, for valid law enforcement purposes.

FLOCK CAMERA, INC.: The ALPR system utilized and managed by the Rhode Island State Police.

HOT LIST: A list of license plates associated with vehicles of interest compiled from one or more databases including, but not limited to, NCIC, RI DMV, Local BOLO's, etc.

VEHICLES OF INTEREST: Including, but not limited to vehicles which are reported as stolen; display stolen license plates or tags; vehicles linked to missing and/or wanted persons and vehicles flagged by the Department of Motor Vehicle Administration or law enforcement agencies.

IV. PROCEDURE:

- A. Department members shall not use or allow others to use the equipment or database records for any unauthorized purpose.**
- B. An ALPR shall only be used for official law enforcement business.**

V. ACCOUNTABILITY AND SAFEGUARDS:

- A. All data collected from FLOCK ALPR cameras is owned by the Rhode Island State Police and remains the property of the Rhode Island State Police. Access is granted at the sole discretion of the Rhode Island State Police and may be revoked at any time with or without cause. The Rhode Island State Police reserve the right to audit all access logs, user activity, and data usage pertaining to the FLOCK system to ensure compliance with this MOU. All data will be closely safeguarded and protected by both procedural and technological means. The Bristol Police Department will observe the following safeguards regarding access to and use of stored data:**
 - 1. Every ALPR Detection Browsing Inquiry must be documented by either the associated Bristol Police case number or an incident number and/or a reason for the inquiry.**
 - 2. Only the Chief of Police and his designee will have a username and password provided by the RI State Police for access to the Flock Camera System.**
 - 3. The Flock Camera system maintains data on any search inquiry, available for any audit of the system conducted by the RI Department of Public Safety/RI State Police.**

VI. ALPR DATA DETECTION AUDITS:

- A. The Bristol Police Department shall be subject to audits of Automated License Plate Reader (ALPR) system use conducted by the Rhode Island State Police and/or the Department of Public Safety. The Chief of Police, or designee, shall ensure compliance with and fully cooperate in any audit of ALPR system use by this agency..**
- B. All audits will be documented by the Chief of Police or his designee.**

VII. RESPONSIBILITY:

- A. It is the responsibility of all personnel to familiarize themselves and comply with this order.**
- B. All personnel must also familiarize and comply with the attached General Order and MOU from the RI Department of Public Safety for the statewide ALPR Flock System.**

**See Attached Documents:
Memorandum of Understanding
Rhode Island Department of Public Safety Police General Order 80G**

**MEMORANDUM OF UNDERSTANDING
BETWEEN
THE RHODE ISLAND STATE POLICE
AND
THE TOWN OF BRISTOL**

This MEMORANDUM OF UNDERSTANDING ("Agreement") is entered into by and between the Rhode Island State Police ("RISP") and the Town of Bristol ("Town") regarding access and Use of Flock License Plate Reader (LPR) Camera Data.

PURPOSE

The purpose of this MOU is to establish guidelines and restrictions regarding the Outside Agency's access to, and use of FLOCK automated license plate reader (ALPR) camera data owned and operated by the Rhode Island State Police. This MOU is intended to ensure responsible use of ALPR technology in accordance with the policies, procedures, and privacy expectations of the State of Rhode Island and its residents.

SCOPE

This MOU covers all access to and use of Rhode Island State Police-owned FLOCK ALPR cameras and associated data. The outside agency may be granted limited access for investigative and public safety purposes under the conditions outlined below.

CONDITIONS OF ACCESS

Authorized Use:

Access to FLOCK LPR data is granted solely for law enforcement and public safety purposes, including but not limited to criminal investigations, active searches for stolen vehicles, missing persons, or suspects in serious crimes.

Prohibition and Data Sharing:

The Outside Agency shall not share, disseminate, forward, or otherwise provide access to any data, images, or alerts obtained from Rhode Island State Police FLOCK ALPR system to any third party, including but not limited to:

Other municipal or state agencies that have not entered into a substantially similar MOU with the Rhode Island State Police;

U.S. Immigration and Customs Enforcement or any external agency when the purpose of that agency or request is the enforcement of potential violations of federal civil immigration law; and;

Any private organizations or entities.

Violation of Data Sharing Restrictions:

Any unauthorized disclosure, sharing, or use of Rhode Island State Police FLOCK ALPR data in violation of this MOU will result in immediate revocation of access privileges for the outside agency. Additional administrative or legal actions may also be pursued at the discretion of the Rhode Island State Police and/or the State of Rhode Island.

DATA OWNERSHIP AND OVERSIGHT

All data collected from FLOCK ALPR cameras is owned by the Rhode Island State Police and remains the property of the Rhode Island State Police. Access is granted at the sole discretion of the Rhode Island State Police and may be revoked at any time with or without cause.

The Rhode Island State Police reserve the right to audit all access logs, user activity, and data usage pertaining to the FLOCK system to ensure compliance with this MOU.

TERM AND TERMINATION

This MOU shall remain in effect until terminated by either party with written notice. The Rhode Island State Police may terminate this agreement immediately if the outside agency is found to be in violation of any terms outlined herein.

ACKNOWLEDGMENT

By signing below, the Outside Agency acknowledges and agrees to abide by all terms, including the prohibition on sharing FLOCK LPR data with any external or federal agencies.

GOVERNING LAW

The terms and conditions of this agreement will be governed by and construed in accordance with the laws of the State of Rhode Island.

IN WITNESS WHEREOF, the Rhode Island State Police and the Town of Bristol have each caused this Agreement to be duly executed by its authorized officer as of the day and year first written below.

Rhode Island State Police:

Name: _____ Title: _____

Signature: _____

Date: _____

[Outside Agency Name]:

Name: _____ Title: _____

Signature: _____

Date: _____



Rhode Island State Police
General Order - 80G

<i>Section</i>	Law Enforcement Operations - Investigations
<i>Article</i>	80 - Miscellaneous
<i>Title</i>	Automated License Plate Readers (ALPR)
<i>Special Instructions</i>	

I. PURPOSE

To establish guidelines and procedures for the proper use and application of Automated License Plate Reader (ALPR) data, to include the access, use, and dissemination of LPR information. This policy is to ensure all information is utilized for legitimate law enforcement purposes only and the privacy, civil rights, and civil liberties of individuals are not violated.

II. DEFINITIONS

AUTOMATED LICENSE PLATE READERS (ALPRs): Also known as license plate readers (LPRs)—use image-processing technology combined with sophisticated computer algorithms capable of converting the images of license plates to electronically readable data.

ALPR DATA: Scan files, alert data, and any other documents or data generated by, or obtained through, utilization of the ALPR system.

ALPR ADMINISTRATOR: The Superintendent of the Rhode Island State Police or his designee(s), serves as the ALPR Administrator for the Division.

ALPR OPERATOR: Trained Division employees who may utilize ALPR system/equipment. ALPR Operators may be assigned to any position within the Division, and the ALPR Administrator may order the deployment of the ALPR systems for use in various efforts, for valid law enforcement purposes.

FLOCK CAMERA, INC.: The ALPR system utilized and managed by the Rhode Island State Police.

HOT LIST: A list of license plates associated with vehicles of interest compiled from one or more databases including, but not limited to, NCIC, RI DMV, Local BOLO's, etc.

VEHICLES OF INTEREST: Including, but not limited to vehicles which are reported as stolen; display stolen license plates or tags; vehicles linked to missing and/or wanted persons and vehicles flagged by the Department of Motor Vehicle Administration or law enforcement agencies.

DETECTION: Data obtained by an ALPR of an image (such as a license plate) within public view that was read by the device, including potential images (such as the plate and description of the vehicle on which it was displayed), and information regarding the location of the ALPR system at the time of the ALPR's read.

HIT: Alert from the ALPR system that a scanned license plate number may be in the National Crime Information Center (NCIC), National Center for Missing and Exploited Children (NCMEC), or other law enforcement database for a specific reason including, but not limited to, being related to a stolen car, wanted person, missing person, domestic violation protective order, or terrorist-related activity.

VALID LAW ENFORCEMENT PURPOSE: A purpose for information/intelligence gathering development, or collection, use, retention, or sharing that furthers the authorized functions and activities of a law enforcement agency, which may include the prevention of crime, ensuring the safety of the public, furthering officer safety, and homeland and national security, while adhering to law and agency policy designed to protect the privacy, civil rights, and civil liberties of Americans.

III. POLICY

Rhode Island State Police will utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public. This policy allows for automated detection of license plates along with vehicle make, model, color, and unique identifiers through vehicle identification technology. ALPR technology shall not be used for traffic violations, outstanding fines or any civil infractions.

IV. PROCEDURES

A. ALPR ADMINISTRATORS

The ALPR Administrators shall be responsible for compliance with the following:

1. Only properly trained sworn officers, analysts, and telecommunicators are allowed access to the ALPR system or to collect ALPR information.
2. Ensuring that initial and in-service training requirements are completed for authorized users.
3. ALPR system monitoring to ensure the security of the information and compliance with applicable privacy laws.
4. Maintaining the title and name of the current designee overseeing the ALPR operation and all ALPR Operators.

Rev. 01/16/2026

B. AUTHORIZED COLLECTION, PURPOSES AND USE OF ALPR DATA/GUIDELINES FOR USE

1. The Rhode Island State Police is authorized to query approved government or commercial databases with respective sharing agreements, memorandums of understanding, or intergovernmental agreements in place.
2. All ALPR queries shall be in furtherance of a valid law enforcement purpose.
3. ALPR data may be utilized by Rhode Island State Police personnel for law enforcement/public safety purposes including, but not limited to, the following:
 - a. Locate stolen, wanted, and subject of investigation vehicles;
 - b. Locate and apprehend individuals subject to arrest warrants or otherwise lawfully sought by law enforcement;
 - c. Locate witnesses and victims of violent crime;
 - d. Locate missing children, elderly, and at-risk individuals, including responding to Amber, Silver, and Purple Alerts;
 - e. Support local, state, federal, and tribal public safety departments in the identification of vehicles associated with targets of criminal investigations, including investigations of serial crimes;
 - f. Protect participants at special events; and
 - g. Protect critical infrastructure sites.

C. PROHIBITED USERS

The ALPR system, and all data collected, is the property of the Rhode Island State Police and not Division personnel. Division personnel may only access and use the ALPR system for official and legitimate law enforcement purposes consistent with this policy. The following uses of the ALPR system are specifically prohibited:

1. **Invasion of Privacy:** The ALPR system shall only be used to record license plates exposed to public view (e.g., vehicles on a public road or street, or that are on private property but whose license plate(s) are visible from a public road, street, or a place to which members of the public have access, such as the parking lot of a shop or other business establishment) except as authorized through the issuance of a court order such as a search warrant.
2. **Harassment or Intimidation:** It is an explicit violation of this policy to use the ALPR system to harass and/or intimidate any individual or group.

3. Use Based on a Protected Characteristic or Class: It is a violation of this policy to use the ALPR system or associated scan files or hot lists solely because of a person's, or group's race, color, gender, gender identity, religion, political affiliation, nationality, ethnicity, sexual orientation, disability, age, disability or other classification protected by law.
4. Personal Use: It is a violation of this policy to use, or allow others to use, the ALPR system or associated scan files or hot lists for any personal purpose. The ALPR shall only be used for official law enforcement business.
5. First Amendment Rights: It is a violation of this policy to use the ALPR system or associated scan files or hot lists for the purpose or known effect of infringing upon First Amendment rights.
6. Determination of Immigration Status: It is a violation of this policy to use the ALPR system or associated scan files or hot lists for the purposes of determining an individual's legal status within the United States or assisting with the enforcement of potential violations of federal civil immigration law.
7. Anyone who engages in an impermissible use of the ALPR system or associated scan files, or hot lists may be subject to criminal prosecution, civil liability, and/or administrative sanctions pursuant to and consistent with the collective bargaining agreement and Division policies.

D. AUTHORIZATION TO SHARE ALPR INFORMATION

1. Division employees are prohibited from sharing, disseminating, forwarding, or otherwise providing access to any data, images or alerts to U.S. Immigration and Customs Enforcement or any external agency when the purpose of that agency or request is the enforcement of potential violations of federal civil immigration law.
2. Division employees are prohibited from sharing, disseminating, forwarding, or otherwise providing access to any data, images, or alerts to any third party that has not entered into an MOU with the Rhode Island State Police.
3. Division employees are prohibited from sharing, disseminating, forwarding, or otherwise providing access to any data, images, or alerts to any private citizen or entity without the express authorization of the Superintendent.

E. ACCOUNTABILITY AND SAFEGUARDS

Rev. 01/16/2026

All data will be closely safeguarded and protected by both procedural and technological means. The Rhode Island State Police will observe the following safeguards regarding access to and use of stored data:

1. All non-law enforcement requests for access to stored ALPR data shall be processed in accordance with applicable law.
2. All ALPR data downloaded to a mobile device, computer or MDT shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date, and time.
3. Persons approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relates to a specific criminal investigation or Division-related civil or administrative action.
4. ALPR data may be released to other authorized and verified law enforcement officials and agencies for legitimate law enforcement purposes with the approval of the ALPR administrator, or designee.
5. Every ALPR Detection Browsing Inquiry must be documented by both the associated law enforcement agency case number, or incident number, and a reason for the inquiry.
6. The APLR Administrator or his/her designee will ensure that information entered into any custom hot lists is removed from the system at the conclusion of the investigation, or whenever evidence suggests that it is no longer relevant to the investigation.

F. SECURITY OF INFORMATION

1. Division personnel assigned to the Management Information Systems Unit (MIS) will maintain usernames and passwords to access ALPR information. Usernames and passwords are not transferable, shall not be shared by ALPR Operators, and must be kept confidential. Access is limited to law enforcement staff in good standing who have completed law enforcement background investigations and serve in a position that the Division has deemed necessary to conduct investigations.
2. Flock automatically purges captured plate data after 30 days.
3. Any information identified as criminal in nature that is obtained during an investigation from accessible ALPR data will be collected and retained

Rev. 01/16/2026

using printouts and screenshots and shall be saved in the Evidence.com platform consistent with Records Retention Schedules.

4. Information collected by ALPR Operators using ALPR data will be stored in a secured law enforcement facility with multiple layers of physical security and 24/7 security protections.
5. ALPR Operators will utilize strong multi-factor authentication, encrypted communications, firewalls, and other reasonable physical, technological, administrative, procedural, and personnel security measures to mitigate the risks of unauthorized access to the system.
6. ALPR data will be maintained by the Division in accordance with the Secretary of State's Records Retention Schedules.

G. RELEASING ALPR DATA

1. The ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law. The requesting agency must provide a written request for the ALPR data that includes:
 - a. The name of the agency requesting the data;
 - b. The name of the person requesting the data;
 - c. The intended purpose of obtaining the data.
2. The request is reviewed by the ALPR Administrator or the authorized designee and approved before the request is fulfilled.
3. The approved request is retained on file. Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will not be processed unless directed to by legal counsel .

V. TRAINING

- A. The designated ALPR Administrator(s) shall coordinate with the Commandant of the Training Academy to ensure that prior to being authorized to use or access the ALPR system, members receive Division-approved training consistent with the manufacturer's recommendations that will include, at a minimum, training on the usage of the ALPR system, data sources, legal responsibilities and ramifications; as well as training on this policy.
- B. Training shall be updated as technological, legal, and other changes that affect the Rhode Island State Police ALPR Policy occur and will be provided to RISF personnel.

Rev. 01/16/2026

VI. POLICY REVIEW

- A. The ALPR Administrator shall review this General Order annually and will update as necessary to ensure changes in data sources, technology, data use and/or sharing agreements, and other relevant considerations are accurately reflected.
- B. All employees with access to the ALPR system shall review this policy on an annual basis.

VII. AUDITS

The Administrator or designee shall conduct a documented, quarterly audit of the ALPR system. This audit shall include a random sampling of ten (10) browsing inquiries to ensure that each meets the requirements established by this policy. The audit shall ensure compliance with the following:

- a. Information security and privacy laws;
- b. Queries are conducted consistent with this policy's Authorized Uses;
- c. Queries contain an associated reason and report number;
- d. Only trained, authorized users are conducting searches;
- e. Outdated information is cleared from the system.

By Order of Colonel Weaver



A handwritten signature in cursive script that reads "Darnell S. Weaver".

Darnell S. Weaver
Colonel
Superintendent