

Automated License Plate Recognition System Usage and Privacy Policy

Neighborhood: High Eagle/Pebble/Los Balcones

Policy Effective Date: 08/17/2026

Last Updated: 09/01/2026

ALPR Vendor: Flock Safety

Designated Policy Coordinator: Janet Nunan, janetnunan@aol.com

Designated Technical Administrator: Rich Niewrosfki, rich@niewroski.com

1. Purpose and Scope

High Eagle/Pebble/Los Balcones ("Neighborhood") uses an Automated License Plate Recognition ("ALPR") system provided by Flock Safety ("Flock") to enhance public safety, provide an additional layer of neighborhood security, deter crime, and assist in the investigation of criminal activity affecting the Neighborhood.

The ALPR system is a vehicle-security system. It is not intended to identify people, monitor residents' personal activities, or provide general-purpose surveillance.

This Usage and Privacy Policy establishes the purposes for which ALPR information may be collected, accessed, used, retained, and shared. It also establishes requirements concerning authorized users, training, security, monitoring, data accuracy, and the protection of privacy and civil liberties.

This policy is intended to comply with applicable California law, including California Civil Code sections 1798.90.5 through 1798.90.55.

2. Definitions

2.1 Flock

"Flock" means Flock Safety, the vendor providing the Neighborhood's Automated License Plate Recognition system and related services.

2.2 Automated License Plate Recognition System

"Automated License Plate Recognition System" or "ALPR System" means a searchable computerized database resulting from the operation of one or more mobile or fixed cameras combined with computer algorithms that read and convert images of registration plates and the characters they contain into computer-readable data.

2.3 Automated License Plate Recognition Information

"Automated License Plate Recognition Information" or "ALPR Information" means information or data collected through the use of an ALPR System.

ALPR Information may include, but is not limited to:

- License plate image;
- Vehicle image;
- Vehicle characteristics, such as color, make, model, body type, racks, stickers, or other observable characteristics;
- License plate number;
- License plate issuing state;
- Date;
- Time; and
- Camera location.

The ALPR System is designed to collect information concerning vehicles and license plates. It is not programmed or used for facial-recognition purposes and does not intentionally collect facial-recognition or biometric information.

3. Camera Location and Operation

The Neighborhood's ALPR camera is positioned to monitor vehicles entering **High Eagle Road from Stone Valley Road**.

The camera is positioned and configured to capture vehicles as they turn onto High Eagle Road. It is not intended or configured to monitor vehicles merely passing along Stone Valley Road.

The camera operates in an area visible to the public and is intended to capture vehicle and license-plate information rather than information concerning the identity of a vehicle's driver or occupants.

4. Information Collected

The Flock ALPR System captures images of vehicles and license plates and uses computer algorithms and machine-learning technology to convert portions of those images into searchable information.

Depending upon what is visible in the captured image, ALPR Information may include the license plate number and issuing state, an image of the vehicle and license plate, and observable vehicle characteristics such as color, make, model, body type, racks, stickers, alterations, or other distinguishing characteristics.

The system also records the date, time, and location associated with the ALPR observation.

The Neighborhood does not intentionally collect facial-recognition or biometric information through the ALPR System.

5. Authorized Purposes

The purpose of the ALPR System is to enhance public safety and provide an additional layer of security to the Neighborhood.

ALPR Information may be accessed and used only for legitimate security purposes, including:

1. Deterring criminal activity;
2. Assisting in the investigation of suspected criminal activity affecting the Neighborhood or its residents;
3. Identifying or locating vehicles that have been reported stolen or that are the subject of an authorized law-enforcement alert;
4. Responding to a specific security incident or suspected crime;
5. Providing relevant information to an appropriate law-enforcement agency when permitted by this policy and applicable law; and
6. Administering, maintaining, securing, and auditing the ALPR System.

ALPR Information may not be accessed or used for purposes unrelated to Neighborhood security.

In particular, ALPR Information may not be used:

- For personal curiosity;
- To monitor or track a particular resident, neighbor, visitor, employee, tenant, or other person without a legitimate authorized security purpose;
- To investigate personal disputes;

- To harass, intimidate, threaten, retaliate against, or discriminate against any person;
- For political, religious, or other unrelated purposes;
- To determine a person's whereabouts for personal reasons; or
- For any purpose prohibited by law.

An ALPR search must have a legitimate purpose consistent with this policy.

6. Authorized Users and Access

Access to the Neighborhood's ALPR System is restricted to specifically authorized users.

6.1 Neighborhood Administrators

Neighborhood administrators designated by High Eagle/Pebble/Los Balcones may administer the system, manage authorized users, review ALPR Information for legitimate security purposes, respond to security incidents, and communicate with Flock and law-enforcement authorities as appropriate.

Authorized administrator(s): Rich Niewroski, Custodian /Janet Nunan, Policy Contact

6.2 Authorized Residents

Residents who participate in funding the annual Flock lease may request authorization to access the ALPR System.

Payment toward the cost of the system does not, by itself, create an automatic right of access. Access will be granted only to individuals specifically authorized by the Official ALPR Custodian.

Authorized residents may access ALPR Information only for the purposes identified in this policy.

6.3 Flock Safety

Flock may access ALPR Information as necessary to provide, maintain, secure, troubleshoot, administer, or otherwise perform its contracted services, subject to the applicable Flock agreement and terms.

6.4 Law Enforcement

The Neighborhood may share ALPR Information with:

Law-Enforcement Agency: Contra Costa Sheriff's Office

Law-enforcement access or receipt of Neighborhood ALPR Information is subject to applicable law, the Neighborhood's Flock agreement and configuration, and the policies and procedures of the applicable law-enforcement agency.

7. Training and User Requirements

All authorized users of the ALPR System will be provided training and information concerning the appropriate use of the system through Flock resources and/or Neighborhood-provided instruction.

Before receiving access, authorized users must:

- Review this policy;
- Understand the purposes and restrictions governing ALPR Information;
- Complete training required by the Neighborhood or Flock;
- Use an individual account;
- Protect their login credentials;
- Use Multi-Factor Authentication
- Never permit another person to use their account; and
- Report suspected unauthorized access, misuse, or security incidents promptly.

Access may be suspended or revoked for violation of this policy.

8. Security and Monitoring

The Neighborhood and Flock maintain administrative, technical, operational, and physical safeguards designed to protect ALPR Information from unauthorized access, use, destruction, modification, or disclosure.

Flock states that its information-security practices align with security requirements established by the National Institute of Standards and Technology ("NIST") and the Cybersecurity and Infrastructure Security Agency's ("CISA") Secure by Design principles.

Flock's safeguards include, among other measures:

8.1 Operational Safeguards

- Audit logging;
- Continuous security scanning and remediation of vulnerabilities on public-facing infrastructure; and
- Role-based access controls designed to limit access based on functional need.

8.2 Administrative Safeguards

- Processes for reporting vulnerabilities for responsible and public disclosure;
- Third-party attestations concerning SOC 2 Type II and ISO 27001 requirements; and
- Personnel screening for engineers with access to cloud infrastructure.

8.3 Technical Safeguards

- Multi-Factor Authentication, including strong TOTP authentication for customer accounts;
- Encryption of information in transit;
- Encryption of information at rest using FIPS-approved algorithms; and
- Other security measures employed by Flock as part of its information-security program.

8.4 Physical Safeguards

Flock states that ALPR Information is stored and processed in United States-based Amazon Web Services ("AWS") cloud infrastructure.

Flock also employs safeguards intended to mitigate device tampering and firmware vulnerabilities and maintains physical security measures for warehouses and other sensitive areas, including visitor controls, security personnel, and escort procedures.

9. Audit Logging and Oversight

Information concerning queries of the ALPR System is recorded in audit logs for auditing purposes.

Audit information may include:

- Username;
- Date;
- Time;
- Purpose of the query; and
- License plate or other information used to conduct the query.

The Official ALPR Custodian will review available audit logs on a regular cadence to help ensure that the ALPR System is being accessed and used appropriately.

Audit review cadence: Quarterly

The Official ALPR Custodian may conduct additional reviews when there is a complaint, suspected misuse, security incident, or other reason to believe the system has not been used in accordance with this policy.

If unauthorized use is identified, the Neighborhood may suspend or terminate access, investigate the incident, preserve relevant records, notify Flock or appropriate law-enforcement authorities when appropriate, and take other action permitted or required by law.

10. Restrictions on Sale, Sharing, and Transfer

ALPR Information gathered through the Neighborhood's ALPR System is contractually owned by the Neighborhood, subject to the terms and conditions of the Neighborhood's agreement with Flock.

Neither the Neighborhood nor Flock sells, publishes, exchanges, or discloses Neighborhood ALPR Information for commercial purposes.

Flock does not disclose or publish Neighborhood ALPR Information without authorization from the Neighborhood, except where permitted or required under the applicable contract or law.

10.1 Law-Enforcement Sharing

The Neighborhood shares ALPR Information with:

Contra Costa County Sheriff's Office

Sharing is limited to legitimate public-safety or investigative purposes and is subject to applicable law and the applicable Flock agreement and system configuration.

An ALPR read or alert is an investigative lead and is not, by itself, proof that a vehicle or its occupants have committed a crime.

10.2 Flock Access and Disclosure

In accordance with its applicable Terms and Conditions, Flock may access, use, preserve, or disclose ALPR Information to law-enforcement agencies, government officials, or other third parties:

- As permitted under the applicable contract;
- As reasonably necessary for performance or enforcement of the contract;
- For proper management and administration;
- As required by law; or
- To address the risk of imminent harm to any person.

The Neighborhood's use and sharing of ALPR Information remains subject to applicable law and this policy.

10.3 Machine-Learning Use by Flock

Flock states that it uses a fraction of ALPR images—less than one percent—for the purpose of improving Flock Services through machine learning.

According to Flock, these images are stripped of metadata and identifying information before being used for this purpose.

The Neighborhood does not authorize Flock to use identifiable Neighborhood ALPR Information for unrelated commercial purposes.

11. Law-Enforcement Alerts and Verification

The Flock System may generate alerts when a captured license plate or vehicle information matches an applicable law-enforcement hot list or other authorized alert source.

The Neighborhood does not create or control law-enforcement hot lists.

An ALPR alert is not conclusive evidence that a vehicle or its occupants are involved in criminal activity.

Users must confirm the computer-generated information and, where practicable, visually compare the result with the associated vehicle image before taking or recommending any action based on ALPR Information.

Neighborhood users are not law-enforcement officers and have no authority to stop, detain, search, or otherwise take enforcement action against a person based solely on an ALPR alert.

When appropriate, suspected criminal activity should be reported to law enforcement rather than addressed directly by a Neighborhood ALPR user.

12. Accuracy and Data Quality

Flock ALPR technology uses optical recognition and machine-learning technology to interpret license plates and identify observable vehicle characteristics.

Flock states that its machine-learning technology is continually improved over time and that its cameras self-monitor to help ensure connectivity and functionality.

Flock also states that low-confidence license-plate reads are not sent to the user as alerts.

Although infrequent, license-plate translation may be incomplete or inaccurate. False positives and other errors may occur.

Accordingly:

- ALPR Information will not be treated as conclusive proof of a vehicle's identity or involvement in criminal activity.
- Users must confirm computer-generated information before taking action based upon ALPR Information.
- Users should visually compare an ALPR result with the associated vehicle image whenever practicable.
- Users should consider the license-plate state and other available vehicle characteristics when evaluating an ALPR result.
- A suspected false positive should not be relied upon for further action.
- Users who identify an apparent error should report it to the Official ALPR Custodian and, where appropriate, to Flock for investigation or correction.

The Neighborhood will take reasonable steps to address known errors in ALPR Information.

13. Data Retention and Deletion

ALPR Information collected by the Neighborhood's ALPR System is hard deleted on a

Retention Period: 30 Days

Flock's standard retention period is **30 days on a rolling basis**. This means that ALPR images and associated metadata remain available in the Flock System for 30 days from

the date they are collected. At the end of the applicable 30-day period, the information is automatically hard-deleted in accordance with Flock's deletion procedures.

The Neighborhood does not routinely retain ALPR Information beyond the standard 30-day retention period.

The 30-day retention period means the number of days that ALPR Information remains available in the Flock System before it is subject to automatic deletion. Information is not retained indefinitely simply because it was collected by the ALPR System.

Preservation of Specific Information

Specific ALPR Information may be preserved beyond the standard 30-day retention period when there is a legitimate and documented reason to do so, including:

- A specific active criminal investigation;
- A pending or reasonably anticipated legal proceeding;
- A specific security incident requiring further investigation;
- A lawful preservation request; or
- Another circumstance in which preservation is required or expressly permitted by applicable law or the applicable Flock agreement.

Any decision to preserve ALPR Information beyond the standard 30-day retention period must be authorized by the **Official ALPR Custodian** or otherwise permitted or required by applicable law.

Only the specific ALPR Information reasonably necessary for the authorized purpose will be preserved. Preservation of specific information does not extend the retention period for unrelated ALPR Information and does not authorize access to, use of, or disclosure of the preserved information for any purpose outside this policy.

Once the reason for extended preservation no longer exists, the preserved ALPR Information will be deleted in accordance with applicable law and the Flock System's deletion procedures.

The Neighborhood will not use preservation procedures as a means of routinely circumventing the standard 30-day retention period.

Automatic Deletion

At the end of the applicable retention period, ALPR Information is automatically deleted through the Flock System's deletion process. Flock's standard retention policy provides for hard deletion of ALPR Information on a rolling 30-day basis, subject to information

that has been specifically preserved for an authorized investigative, legal, or other lawful purpose.

The Neighborhood's standard practice is therefore to maintain ALPR Information for **30 days and no longer**, unless a specific preservation exception described in this section applies.

14. Privacy and Civil Liberties

The Neighborhood recognizes that vehicles traveling on public roads may belong to residents, visitors, service providers, delivery personnel, employees, and members of the public who have no connection to criminal activity.

The existence of an ALPR record does not imply that the vehicle owner, driver, or occupants have committed a crime or engaged in suspicious activity.

The Neighborhood will use ALPR Information in a manner consistent with applicable privacy laws and respect for individual privacy and civil liberties.

The ALPR System will not be used as a means of profiling, harassment, intimidation, discrimination, or generalized surveillance.

15. Prohibited Uses and Misuse

Unauthorized access, use, disclosure, copying, or dissemination of ALPR Information is prohibited.

Examples of prohibited conduct include:

- Searching for a vehicle without a legitimate authorized purpose;
- Searching for information about a person because of a personal dispute;
- Sharing ALPR Information with unauthorized persons;
- Using ALPR Information for harassment or intimidation;
- Allowing another person to use an authorized user's account;
- Attempting to circumvent access controls or security measures;
- Using ALPR Information for political, religious, or other unrelated purposes; or
- Using ALPR Information for any purpose not authorized by this policy.

A user who violates this policy will have access immediately suspended or revoked and may be subject to other appropriate action.

Nothing in this section limits any rights, remedies, or obligations provided by applicable law.

16. Official ALPR Custodian

The Official ALPR Custodian responsible for implementation and oversight of this policy is:

Name: Rich Niewroski

Job Title/Role: Custodian

Email: Rich@niewroski.com

Telephone: [Telephone Number]- **lets remove this**

The Official ALPR Custodian is responsible for:

- Implementing this policy;
- Administering or overseeing access to the ALPR System;
- Authorizing users;
- Coordinating user training;
- Reviewing audit logs;
- Maintaining appropriate security safeguards;
- Responding to reported misuse;
- Coordinating with Flock when necessary;
- Coordinating with law enforcement when appropriate; and
- Periodically reviewing this policy for compliance with applicable law and actual system practices.

17. Complaints and Questions

Questions, concerns, or complaints concerning the Neighborhood's ALPR System or this policy may be directed to:

High Eagle/Pebble/Los Balcones

Attention: [Official ALPR Custodian]

Email: [Email Address]

Telephone: [Telephone Number] - **lets remove this**

Mailing Address: [Address, if applicable] - **lets remove this**

Reports of suspected unauthorized access or misuse should be made promptly so that the Neighborhood can investigate and take appropriate action.

18. Public Availability and Policy Review

This Usage and Privacy Policy will be made publicly available on the Neighborhood's website.

The Neighborhood will review this policy periodically and revise it when appropriate to reflect changes in:

- The ALPR System;
- The Flock agreement or system configuration;
- Neighborhood practices;
- Applicable law; or
- Data-security requirements.

The current version of this policy will be maintained on the Neighborhood's website.

Policy Effective Date: 08/17/2026

Last Reviewed: 09/01/2026

Next Scheduled Review: TBD

Important Notice to Residents and the Public

The ALPR System provides information that may assist with neighborhood security and criminal investigations. It does not determine whether a person has committed a crime.

An ALPR read or alert should not be treated as conclusive evidence of criminal activity. ALPR information should be independently reviewed and, when practicable, visually confirmed before any action is taken based upon it.

The Neighborhood's ALPR System is intended to provide an additional security resource while maintaining reasonable safeguards for privacy, civil liberties, data security, and responsible use.