



## Kensington Community Services District

DATE: May 14, 2026

TO: Board of Directors

FROM: David Aranda, Interim General Manager (IGM)

Submitted by: Mike Gancasz, Chief of Police

Presented by: Mike Gancasz, Chief of Police

SUBJECT: Presentation on Temporary Suspension of License Plate Reader Functionality – Findings

---

### RECOMMENDATION:

The findings and related materials, including the adopted contract and approved ALPR policy are incorporated. Any future direction or Board action related to the program would return as a separate agenda item.

In the interest of time, please submit questions in advance to the General Manager. The Chief will incorporate them in his overview or answer them directly in a timely manner during our meeting.

### BACKGROUND:

Chief Gancasz will provide an overview of the Police Department's 90-day evaluation of the District's Automatic License Plate Reader (ALPR) functionality, which was temporarily paused in February 2026 to review system governance, safeguards, legal compliance, and operational integrity in the interest of transparency and public trust. That decision was not taken lightly by the Chief.

### EXHIBIT(S):

- Temporary Suspension of License Plate Reader Functionality – Findings



## **KENSINGTON POLICE COMMUNITY MESSAGE**

# **Temporary Suspension of License Plate Reader Functionality – Findings**

**Date:** May 1, 2026

On February 12, 2026, the Kensington Police Department (KPD) suspended operation of its Automated License Plate Reader (ALPR) system following reports of unauthorized or improper access to ALPR data in other jurisdictions. Concerns regarding potential federal-agency access to ALPR networks also contributed to the decision. \*There were no incidents that prompted this review that involved the KPD, and no policy or legal violations associated with the ALPR were identified at KPD before or during this review.

The 90-day suspension was implemented to examine the safeguards KPD employs, the program's technological relevance and value, and to ensure public confidence in the Department's use of public safety technology.

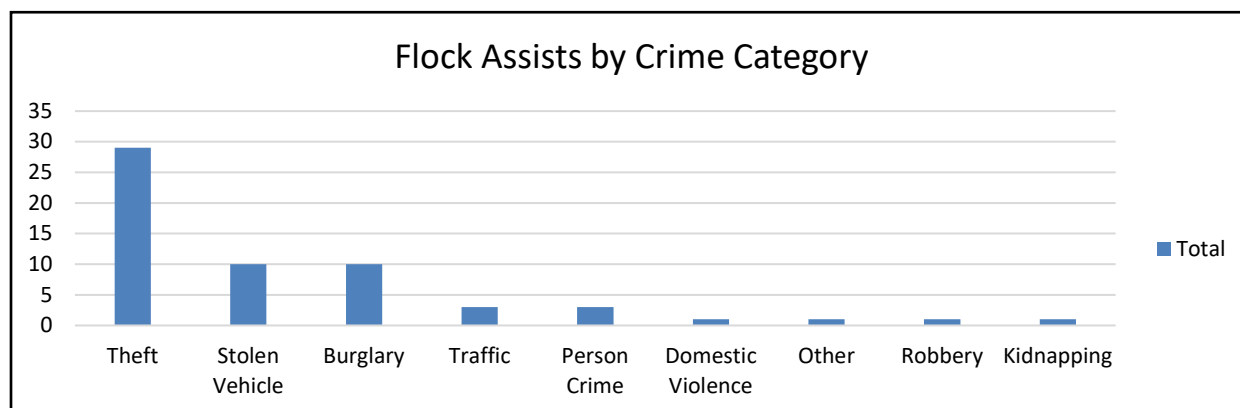
This report presents the findings of the Kensington Police Department's (KPD) 90-day evaluation of its ALPR program.

# Findings

## 1. Technological value and relevance

Since program inception, the ALPR exceeded expectations as an investigative/crime-fighting tool, contributing to criminal arrests, stolen-vehicle recoveries, warrant issuance, case development, and case closure. The system enhanced real-time officer awareness and post-incident investigative capabilities, particularly by identifying suspect vehicles and investigative leads that are not otherwise obtainable through traditional methods. Some of the successes directly attributed to the ALPR include:

- Two stolen vehicles recovered
- Fourteen arrests
- Thirty-nine investigations advanced or were successfully resolved
- Six search and arrest warrants issued by the Superior Court
- Nine cases involving the recovery of stolen property and seizure of narcotics
- Two handguns taken off the street, including one unsterilized ghost gun
- Twenty-three mutual-aid investigative hand-offs to our local police departments
- Identification of thirty-eight suspect vehicles and ten suspects who fled crime scenes
- Resolution of two hit-and-run investigations where witnesses could not provide a lead
- Detention and arrest of a suspect wanted in a stabbing
- locating a suspect and his vehicle associated with a kidnapping



The data showed clear and measurable investigative value by enhancing the Department's ability to identify suspect vehicles, develop investigative leads, support timely follow-up investigations, and improve regional information sharing. This technology, as intended, strengthens the Police Department's ability to respond timely and effectively to criminal activity, sometimes before a crime occurs, and it enhances our officers' safety and protects the community.

### 1(a) Adverse operational impact

During the suspension of the ALPR system, officers reverted to traditional legacy policing methods, relying primarily on manual observation, witness statements, notes, and reduced in-field investigative resources.

While these methods are an important component of law enforcement operations, the absence of ALPR technology resulted in a measurable reduction in the officers' ability to rapidly identify suspect vehicles, generate actionable investigative leads, and conduct timely follow-up work on open cases.

### **Investigations Adversely Impacted**

- A vehicle theft investigation stalled after officers lost the ability to conduct follow-up ALPR queries that may have identified suspect vehicles or associated locations.
- A hit-and-run investigation was significantly hindered because officers were unable to use ALPR data to identify or locate the suspect vehicle involved in the collision.
- Two separate auto burglary investigations were unable to progress due to the loss of access to Kensington and allied agency camera networks that could have provided investigative leads or suspect vehicle identification.
- A package theft investigation could not be effectively developed despite officers having estimated travel timing through areas covered by camera systems, limiting the Department's ability to identify potential suspect vehicles.
- Officers lost access to regional ALPR information-sharing and analytical tools that identify vehicles linked to crimes throughout the state, including missing or at-risk persons.
- Investigative leads, historical vehicle data, and evidentiary information were permanently lost once applicable data retention periods expired during the suspension of the system.

The pause underscored the operational value of the system as a modern force multiplier, enhancing investigative efficiency, supporting retrospective case analysis, strengthening regional information sharing among state law enforcement agencies, and improving both officer and community safety in Kensington. This cannot be understated for a small force like Kensington's

### **2. System Access Controls and Auditing Procedures**

Access to the system has remained tightly controlled through multi-factor authentication and defined user roles. All queries are logged at the system level, with access logs retained for accountability.

A system administrator conducts monthly audits of all queries, including a review of any external agency-related activity. Department policy requires every query to include a case or incident number in addition to a legitimate law enforcement purpose. Additional documentation is required for all mutual-aid-related queries.

The review established that there was no misuse or policy violations identified since the system was put in place.

### **3. Data Retention and Sharing Protocols**

ALPR data is retained for a period of thirty days to support legitimate investigative needs while balancing privacy and data-minimization considerations. System access logs are separately maintained for accountability, oversight, and audit purposes. After that, all captured data is automatically purged. Retained data is purged daily based on capture date. Thirty days after the system's pause, there was no data in Kensington's secure database. This was completely automatic by design. And as of the completion of this report, the database remains empty. This establishes that the purge process established by policy is functioning as designed.

Data sharing with the ALPR is conducted on a controlled and reciprocal basis with a limited number of regional law enforcement partners, and the Department does not provide open, unrestricted, or public access to the system. All external data-sharing requests are subject to mandatory oversight and auditing processes pursuant to policy designed to ensure that access is lawful, appropriately documented, and limited to legitimate law enforcement purposes. There were no issues identified here.

Historical records proved the department has never authorized or permitted access to the system by federal immigration authorities. Consistent with Department policy and the Flock Transparency Portal, prohibited uses include immigration enforcement, harassment or intimidation, monitoring based solely on protected-class status, personal or non-law-enforcement use, monitoring of First Amendment-protected activity, and any use related to reproductive-health activities or services. The Kensington system is set up so that outside queries must be formally requested and then access granted or denied by a supervisor. Data retention and sharing practices are deliberate and carefully controlled, balancing investigative needs with responsible data stewardship. The measures employed are tightly controlled and regulated.

### **4. Policy and Oversight**

Kensington Police use ALPR technology under the oversight of KPD Policy 426, which is a thoughtfully tailored, KPPCSD board-modified and approved policy outlining stricter controls, specific retention language, and oversight standards. This policy was reviewed and adopted by the KPPCSD board in January, 2025, six months before the ALPR system was officially turned on. Training records show that during the six months before the cameras were installed, every officer and supervisor was required to complete training on the system, its use, the rules governing sharing and accessing information, and to read, understand, and individually sign and acknowledge the new board-approved policy.

The policy has been publicly available on the Kensington Community Services District website and referenced in the Flock Transparency Portal from program inception (Feb 2025). The complete policy, produced by Lexipol, defines standards for authorized use, access controls, documentation, supervisory review, and audit procedures. Program oversight is maintained at the command level, with policies and operational safeguards routinely reviewed to ensure compliance, transparency, and accountable use of the system.

\*Oversight and safeguards are further reinforced through annual audits of the program. The Department's first ALPR audit, covering the period from August 1, 2024, through August 1, 2025, was completed and publicly posted on the District's website in August 2025.

This further demonstrates the Department's commitment to transparency, accountability, and adherence to Policy 426. There were no issues identified here.

## **5. Alignment with Current Legal Standards and Best Practices**

The Department assessed its ALPR program against widely recognized law enforcement best practices. Program controls include restricted access, audit logging, defined retention periods, structured documentation requirements, supervisory oversight, and limitations on system use. These elements reflect established standards for the responsible use of investigative technology. The Department's internal controls are designed not only to support investigations but also to ensure that all system use is purpose-driven, documented, and reviewable. If anything, Kennington's ALPR policy 426, with added language, heightens our standards and adds a layer of security.

## **6. Community Feedback: ALPR technology in Kensington**

Community feedback given during the evaluation period reflected general support for the Department's use of ALPR technology as a public safety tool within Kensington, particularly regarding its ability to assist criminal investigations and support crime prevention efforts. Some expressed disappointment that the system was turned off without community input. Citizens have regularly engaged officers and supervisors in constructive discussions regarding the technology and how it's used.

During community outreach events, like National Night Out, ALPR technology and related privacy protections were frequent topics of discussion. Most expressed support for the system, particularly when informed of the Department's enhanced policy controls, auditing procedures, restricted access protocols, and transparency measures. Community members commonly voiced the expectation that modern law enforcement agencies utilize available technology responsibly to improve public safety while maintaining appropriate safeguards to protect privacy and civil liberties. Overall, feedback during National Night Out and other events like coffee with a cop reflected a mutual understanding that the Department's use of ALPR technology, when governed by good policy and oversight, serves as a valuable investigative and crime prevention tool for the community.

## **7. Officer Safety**

An important and often overlooked benefit of ALPR technology is that it provides officers with timely and actionable information that enhances situational awareness during traffic stops, field contacts, suspicious vehicle investigations, and ongoing criminal investigations. The system supported officers in identifying vehicles potentially associated with criminal activity, locating linked incidents, and developing critical context before officers contacted vehicle occupants. This advanced awareness capability supports safer, more informed decision-making in rapidly evolving field situations.

During the temporary suspension of the system, officers conducted patrol operations without access to this critical real-time information, resulting in a heightened operational risk environment.

While traditional policing methods are effective, the absence of ALPR technology reduces both the immediacy and depth of investigative and situational information available to officers. As a result, they were at times required to make enforcement and contact decisions without the benefit of alerts, associated vehicle history, or critical regional intelligence that may have identified elevated risks connected to serious or violent criminal activity.

When operational, ALPR technology supports a more informed, deliberate, and coordinated approach to patrol and investigative functions. Access to reliable and timely information improves workflow efficiency, enhances investigative effectiveness, strengthens officer confidence in decision-making, and increases the Department's ability to appropriately assess risk, allocate resources, and respond effectively to public safety threats.

Another benefit lost during the suspension of the ALPR system was the real-time alerts when vehicles associated with criminal activity enter Kensington. These alerts allow officers to respond proactively by locating the vehicle's last known area and increasing patrol presence before a crime occurs. For example, a vehicle associated with a robbery or other serious offense in a neighboring jurisdiction may enter Kensington and be identified near a commercial or residential area through the ALPR network. In these situations, the alert allows officers to respond immediately, often resulting in the vehicle leaving the area before additional criminal activity can occur. This proactive capability enhances crime prevention efforts, increases officer awareness, and strengthens the Department's ability to deter criminal activity.

## **Summary**

The 90-day evaluation confirms that the KPD ALPR program is:

- Operationally effective, secure, and working exactly as intended
- Governed by strong access controls and auditing procedures
- Managed through deliberate and controlled data practices
- Supported by clear policy and command-level oversight
- Aligned with established best practices
- Responsive to community expectations and concerns
- Provides an added layer of officer safety

Thank you for your continued partnership and trust.



**Mike Gancasz**  
Chief of Police  
Kensington Police Department



---

Date: December 11, 2024  
To: Board of Directors  
Submitted by: David Aranda, IGM  
Presented by: Mike Gancasz, Police Chief  
Subject: Approval of purchasing FLOCK software

---

### **Recommendation**

The General Manager recommends purchasing and entering into a two-year agreement with FLOCK at a price of \$ 18, 250 the first year. This dollar amount was not budgeted but will not impact the overall police budget.

### **Background**

This item was presented at a Board of Directors meeting a few months ago and it was decided to bring it back to the board in conjunction with a policy that would cover license plate reading with cameras for the District. Agenda Item 08 will address the policy aspect of this new tool for Kensington Police Department.

The world is becoming more dangerous and the need to assist law enforcement in stopping crimes from happening and in locating those who commit violations is important. The idea of FLOCK being present in the community will hopefully deter crime and the software/cameras will assist Kensington Police in tracking those who break the law.

The Chief and Sergeant will be present to answer any questions.

### **Exhibits**

- Flock Safety + CA + Kensington PD Agreement



## **Flock Safety + CA - Kensington PD**

---

Flock Group Inc.  
1170 Howell Mill Rd, Suite 210  
Atlanta, GA 30318

---

MAIN CONTACT:  
Jake Sherman  
jake.sherman@flocksafety.com  
8187467444

**flock safety**



EXHIBIT A  
**ORDER FORM**

Customer: CA - Kensington PD  
Legal Entity Name: CA - Kensington PD  
Accounts Payable Email: mgonzalez@keystonepacific.com  
Address: 217 Arlington Ave Berkeley, California 94707

Initial Term: 24 Months  
Renewal Term: 24 Months  
Payment Terms: Net 30  
Billing Frequency: Annual Plan - First Year Invoiced at Signing.  
Retention Period: 30 Days

**Hardware and Software Products**

Annual recurring amounts over subscription term

Item	Cost	Quantity	Total
<b>Flock Safety Platform</b>			<b>\$15,000.00</b>
<b>Flock Safety Flock OS</b>			
FlockOS™	Included	1	Included
<b>Flock Safety LPR Products</b>			
Flock Safety Falcon®	Included	5	Included

**Professional Services and One Time Purchases**

Item	Cost	Quantity	Total
<b>One Time Fees</b>			
<b>Flock Safety Professional Services</b>			
Professional Services - Standard Implementation Fee	\$650.00	5	\$3,250.00
<b>Subtotal Year 1:</b>			\$18,250.00
<b>Annual Recurring Subtotal:</b>			\$15,000.00
<b>Estimated Tax:</b>			\$0.00
<b>Contract Total:</b>			\$33,250.00

*Taxes shown above are provided as an estimate. Actual taxes are the responsibility of the Customer. This Agreement will automatically renew for successive renewal terms of the greater of one year or the length set forth on the Order Form (each, a "Renewal Term") unless either Party gives the other Party notice of non-renewal at least thirty (30) days prior to the end of the then-current term.*

## Billing Schedule

Billing Schedule	Amount (USD)
<b>Year 1</b>	
At Contract Signing	\$18,250.00
<b>Annual Recurring after Year 1</b>	\$15,000.00
<b>Contract Total</b>	\$33,250.00

\*Tax not included

## Product and Services Description

Flock Safety Platform Items	Product Description	Terms
Flock Safety Falcon ®	An infrastructure-free license plate reader camera that utilizes Vehicle Fingerprint® technology to capture vehicular attributes.	The Term shall commence upon first installation and validation of Flock Hardware.

One-Time Fees	Service Description
Installation on existing infrastructure	One-time Professional Services engagement. Includes site & safety assessment, camera setup & testing, and shipping & handling in accordance with the Flock Safety Advanced Implementation Service Brief.
Professional Services - Standard Implementation Fee	One-time Professional Services engagement. Includes site and safety assessment, camera setup and testing, and shipping and handling in accordance with the Flock Safety Standard Implementation Service Brief.
Professional Services - Advanced Implementation Fee	One-time Professional Services engagement. Includes site & safety assessment, camera setup & testing, and shipping & handling in accordance with the Flock Safety Advanced Implementation Service Brief.

## FlockOS Features & Description

### Package: Essentials

FlockOS Features	Description
Community Cameras (Full Access)	Access to all privately owned Flock devices within your jurisdiction that have been shared with you.
Unlimited Users	Unlimited users for FlockOS
State Network (LP Lookup Only)	Allows agencies to look up license plates on all cameras opted in to the statewide Flock network.
Nationwide Network (LP Lookup Only)	Allows agencies to look up license plates on all cameras opted in to the nationwide Flock network.
Direct Share - Surrounding Jurisdiction (Full Access)	Access to all Flock devices owned by law enforcement that have been directly shared with you. Have ability to search by vehicle fingerprint, receive hot list alerts, and view devices on the map.
Time & Location Based Search	Search full, partial, and temporary plates by time at particular device locations
License Plate Lookup	Look up specific license plate location history captured on Flock devices
Vehicle Fingerprint Search	Search footage using Vehicle Fingerprint™ technology. Access vehicle type, make, color, license plate state, missing / covered plates, and other unique features like bumper stickers, decals, and roof racks.
Flock Insights/Analytics page	Reporting tool to help administrators manage their LPR program with device performance data, user and network audits, plate read reports, hot list alert reports, event logs, and outcome reports.
ESRI Based Map Interface	Flock Safety's maps are powered by ESRI, which offers the ability for 3D visualization, viewing of floor plans, and layering of external GIS data, such as City infrastructure (i.e., public facilities, transit systems, utilities), Boundary mapping (i.e., precincts, county lines, beat maps), and Interior floor plans (i.e., hospitals, corporate campuses, universities)
Real-Time NCIC Alerts on Flock ALPR Cameras	Alert sent when a vehicle entered into the NCIC crime database passes by a Flock camera
Unlimited Custom Hot Lists	Ability to add a suspect's license plate to a custom list and get alerted when it passes by a Flock camera

**By executing this Order Form, Customer represents and warrants that it has read and agrees to all of the terms and conditions contained in the Master Services Agreement attached.** The Parties have executed this Agreement as of the dates set forth below.

**FLOCK GROUP, INC.**

**Customer: CA - Kensington PD**

By: \_\_\_\_\_

By: \_\_\_\_\_

Name: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

Date: \_\_\_\_\_

PO Number: \_\_\_\_\_

## Master Services Agreement

This Master Services Agreement (this “*Agreement*”) is entered into by and between Flock Group, Inc. with a place of business at 1170 Howell Mill Road NW Suite 210, Atlanta, GA 30318 (“*Flock*”) and the entity identified in the signature block (“*Customer*”) (each a “*Party*,” and together, the “*Parties*”) on this the 29 day of September 2023. This Agreement is effective on the date of mutual execution (“*Effective Date*”). Parties will sign an Order Form (“*Order Form*”) which will describe the Flock Services to be performed and the period for performance, attached hereto as **Exhibit A**. The Parties agree as follows:

### RECITALS

**WHEREAS**, Flock offers a software and hardware situational awareness solution through Flock’s technology platform that upon detection is capable of capturing audio, video, image, and recording data and provide notifications to Customer (“*Notifications*”);

**WHEREAS**, Customer desires access to the Flock Services (defined below) on existing devices, provided by Customer, or Flock provided Flock Hardware (as defined below) in order to create, view, search and archive Footage and receive Notifications, via the Flock Services;

**WHEREAS**, Customer shall have access to the Footage in Flock Services. Pursuant to Flock’s standard Retention Period (defined below) Flock deletes all Footage on a rolling thirty (30) day basis, except as otherwise stated on the *Order Form*. Customer shall be responsible for extracting, downloading and archiving Footage from the Flock Services on its own storage devices; and

**WHEREAS**, Flock desires to provide Customer the Flock Services and any access thereto, subject to the terms and conditions of this Agreement, solely for the awareness, prevention, and prosecution of crime, bona fide investigations and evidence gathering for law enforcement purposes, (“*Permitted Purpose*”).

## AGREEMENT

**NOW, THEREFORE,** Flock and Customer agree that this Agreement, and any Order Form, purchase orders, statements of work, product addenda, or the like, attached hereto as exhibits and incorporated by reference, constitute the complete and exclusive statement of the Agreement of the Parties with respect to the subject matter of this Agreement, and replace and supersede all prior agreements, term sheets, purchase orders, correspondence, oral or written communications and negotiations by and between the Parties.

### 1. DEFINITIONS

Certain capitalized terms, not otherwise defined herein, have the meanings set forth or cross-referenced in this Section 1.

1.1 “**Anonymized Data**” means Customer Data permanently stripped of identifying details and any potential personally identifiable information, by commercially available standards which irreversibly alters data in such a way that a data subject (i.e., individual person or entity) can no longer be identified directly or indirectly.

1.2 “**Authorized End User(s)**” means any individual employees, agents, or contractors of Customer accessing or using the Services, under the rights granted to Customer pursuant to this Agreement.

1.3 “**Customer Data**” means the data, media and content provided by Customer through the Services. For the avoidance of doubt, the Customer Data will include the Footage.

1.4. “**Customer Hardware**” means the third-party camera owned or provided by Customer and any other physical elements that interact with the Embedded Software and the Web Interface to provide the Services.

1.5 “**Embedded Software**” means the Flock proprietary software and/or firmware integrated with or installed on the Flock Hardware or Customer Hardware.

1.6 “**Flock Hardware**” means the Flock device(s), which may include the pole, clamps, solar panel, installation components, and any other physical elements that interact with the Embedded Software and the Web Interface, to provide the Flock Services as specifically set forth in the applicable product addenda.

1.7 “**Flock IP**” means the Services, the Embedded Software, and any intellectual property or proprietary information therein or otherwise provided to Customer and/or its Authorized End Users. Flock IP does not include Footage (as defined below).

1.8 “**Flock Network End User(s)**” means any user of the Flock Services that Customer authorizes access to or receives data from, pursuant to the licenses granted herein.

1.9 “**Flock Services**” means the provision of Flock’s software and hardware situational awareness solution, via the Web Interface, for automatic license plate detection, alerts, audio detection, searching image records, video and sharing Footage.

1.10 “**Footage**” means still images, video, audio and other data captured by the Flock Hardware or Customer Hardware in the course of and provided via the Flock Services.

1.11 “**Hotlist(s)**” means a digital file containing alphanumeric license plate related information pertaining to vehicles of interest, which may include stolen vehicles, stolen vehicle license plates, vehicles owned or associated with wanted or missing person(s), vehicles suspected of being involved with criminal or terrorist activities, and other legitimate law enforcement purposes. Hotlist also includes, but is not limited to, national data (i.e., NCIC) for similar categories, license plates associated with AMBER Alerts or Missing Persons/Vulnerable Adult Alerts, and includes manually entered license plate information associated with crimes that have occurred in any local jurisdiction.

1.12 “**Installation Services**” means the services provided by Flock for installation of Flock Services.

1.13 “**Retention Period**” means the time period that the Customer Data is stored within the cloud storage, as specified in the product addenda.

1.14 “**Vehicle Fingerprint™**” means the unique vehicular attributes captured through Services such as: type, make, color, state registration, missing/covered plates, bumper stickers, decals, roof racks, and bike racks.

1.15 “**Web Interface**” means the website(s) or application(s) through which Customer and its Authorized End Users can access the Services.



## 2. SERVICES AND SUPPORT

**2.1 Provision of Access.** Flock hereby grants to Customer a non-exclusive, non-transferable right to access the features and functions of the Flock Services via the Web Interface during the Term, solely for the Authorized End Users. The Footage will be available for Authorized End Users to access and download via the Web Interface for the data retention time defined on the Order Form (“*Retention Period*”). Authorized End Users will be required to sign up for an account and select a password and username (“*User ID*”). Customer shall be responsible for all acts and omissions of Authorized End Users, and any act or omission by an Authorized End User which, including any acts or omissions of authorized End user which would constitute a breach of this agreement if undertaken by customer. Customer shall undertake reasonable efforts to make all Authorized End Users aware of all applicable provisions of this Agreement and shall cause Authorized End Users to comply with such provisions. Flock may use the services of one or more third parties to deliver any part of the Flock Services, (such as using a third party to host the Web Interface for cloud storage or a cell phone provider for wireless cellular coverage).

**2.2 Embedded Software License.** Flock grants Customer a limited, non-exclusive, non-transferable, non-sublicensable (except to the Authorized End Users), revocable right to use the Embedded Software as it pertains to Flock Services, solely as necessary for Customer to use the Flock Services.

**2.3 Support Services.** Flock shall monitor the Flock Services, and any applicable device health, in order to improve performance and functionality. Flock will use commercially reasonable efforts to respond to requests for support within seventy-two (72) hours. Flock will provide Customer with reasonable technical and on-site support and maintenance services in-person, via phone or by email at [support@flocksafety.com](mailto:support@flocksafety.com) (such services collectively referred to as “*Support Services*”).

**2.4 Upgrades to Platform.** Flock may make any upgrades to system or platform that it deems necessary or useful to (i) maintain or enhance the quality or delivery of Flock’s products or services to its agencies, the competitive strength of, or market for, Flock’s products or services, such platform or system’s cost efficiency or performance, or (ii) to comply with applicable law. Parties understand that such upgrades are necessary from time to time and will not diminish the quality of the services or materially change any terms or conditions within this Agreement.

**2.5 Service Interruption.** Services may be interrupted in the event that: (a) Flock’s provision of the Services to Customer or any Authorized End User is prohibited by applicable law; (b) any third-party services required for Services are interrupted; (c) if Flock reasonably believe Services are being used for malicious, unlawful, or otherwise unauthorized use; (d) there is a threat or attack on any of the Flock IP by a third party; or (e) scheduled or emergency maintenance (“**Service Interruption**”). Flock will make commercially reasonable efforts to provide written notice of any Service Interruption to Customer, to provide updates, and to resume providing access to Flock Services as soon as reasonably possible after the event giving rise to the Service Interruption is cured. Flock will have no liability for any damage, liabilities, losses (including any loss of data or profits), or any other consequences that Customer or any Authorized End User may incur as a result of a Service Interruption. To the extent that the Service Interruption is not caused by Customer’s direct actions or by the actions of parties associated with the Customer, the time will be tolled by the duration of the Service Interruption (for any continuous suspension lasting at least one full day). For example, in the event of a Service Interruption lasting five (5) continuous days, Customer will receive a credit for five (5) free days at the end of the Term.

**2.6 Service Suspension.** Flock may temporarily suspend Customer’s and any Authorized End User’s access to any portion or all of the Flock IP or Flock Service if (a) there is a threat or attack on any of the Flock IP by Customer; (b) Customer’s or any Authorized End User’s use of the Flock IP disrupts or poses a security risk to the Flock IP or any other customer or vendor of Flock; (c) Customer or any Authorized End User is/are using the Flock IP for fraudulent or illegal activities; (d) Customer has violated any term of this provision, including, but not limited to, utilizing Flock Services for anything other than the Permitted Purpose; or (e) any unauthorized access to Flock Services through Customer’s account (“**Service Suspension**”). Customer shall not be entitled to any remedy for the Service Suspension period, including any reimbursement, tolling, or credit. If the Service Suspension was not caused by Customer, the Term will be tolled by the duration of the Service Suspension.

**2.7 Hazardous Conditions.** Flock Services do not contemplate hazardous materials, or other hazardous conditions, including, without limit, asbestos, lead, toxic or flammable substances. In the event any such hazardous materials are discovered in the designated locations in which Flock is to perform services under this Agreement, Flock shall have the right to cease work immediately.

### 3. CUSTOMER OBLIGATIONS

**3.1 Customer Obligations.** Flock will assist Customer Authorized End Users in the creation of a User ID. Authorized End Users agree to provide Flock with accurate, complete, and updated registration information. Authorized End Users may not select as their User ID, a name that they do not have the right to use, or any other name with the intent of impersonation. Customer and Authorized End Users may not transfer their account to anyone else without prior written permission of Flock. Authorized End Users shall not share their account username or password information and must protect the security of the username and password. Unless otherwise stated and defined in this Agreement, Customer shall not designate Authorized End Users for persons who are not officers, employees, or agents of Customer. Authorized End Users shall only use Customer-issued email addresses for the creation of their User ID. Customer is responsible for any Authorized End User activity associated with its account. Customer shall ensure that Customer provides Flock with up to date contact information at all times during the Term of this agreement. Customer shall be responsible for obtaining and maintaining any equipment and ancillary services needed to connect to, access or otherwise use the Flock Services. Customer shall (at its own expense) provide Flock with reasonable access and use of Customer facilities and Customer personnel in order to enable Flock to perform Services (such obligations of Customer are collectively defined as “*Customer Obligations*”).

**3.2 Customer Representations and Warranties.** Customer represents, covenants, and warrants that Customer shall use Flock Services only in compliance with this Agreement and all applicable laws and regulations, including but not limited to any laws relating to the recording or sharing of data, video, photo, or audio content.

### 4. DATA USE AND LICENSING

**4.1 Customer Data.** As between Flock and Customer, all right, title and interest in the Customer Data, belong to and are retained solely by Customer. Customer hereby grants to Flock a limited, non-exclusive, royalty-free, irrevocable, worldwide license to use the Customer Data and perform all acts as may be necessary for Flock to provide the Flock Services to Customer. Flock does not own and shall not sell Customer Data.

**4.2 Customer Generated Data.** Flock may provide Customer with the opportunity to post, upload, display, publish, distribute, transmit, broadcast, or otherwise make available, messages,

text, illustrations, files, images, graphics, photos, comments, sounds, music, videos, information, content, ratings, reviews, data, questions, suggestions, or other information or materials produced by Customer (“**Customer Generated Data**”). Customer shall retain whatever legally cognizable right, title, and interest in Customer Generated Data. Customer understands and acknowledges that Flock has no obligation to monitor or enforce Customer’s intellectual property rights of Customer Generated Data. Customer grants Flock a non-exclusive, irrevocable, worldwide, royalty-free, license to use the Customer Generated Data for the purpose of providing Flock Services. Flock does not own and shall not sell Customer Generated Data.

**4.3 Anonymized Data.** Flock shall have the right to collect, analyze, and anonymize Customer Data and Customer Generated Data to the extent such anonymization renders the data non-identifiable to create Anonymized Data to use and perform the Services and related systems and technologies, including the training of machine learning algorithms. Customer hereby grants Flock a non-exclusive, worldwide, perpetual, royalty-free right to use and distribute such Anonymized Data to improve and enhance the Services and for other development, diagnostic and corrective purposes, and other Flock offerings. Parties understand that the aforementioned license is required for continuity of Services. Flock does not own and shall not sell Anonymized Data.

## **5. CONFIDENTIALITY; DISCLOSURES**

**5.1 Confidentiality.** To the extent required by any applicable public records requests, each Party (the “**Receiving Party**”) understands that the other Party (the “**Disclosing Party**”) has disclosed or may disclose business, technical or financial information relating to the Disclosing Party’s business (hereinafter referred to as “**Proprietary Information**” of the Disclosing Party). Proprietary Information of Flock includes non-public information regarding features, functionality and performance of the Services. Proprietary Information of Customer includes non-public data provided by Customer to Flock or collected by Flock via Flock Services, which includes but is not limited to geolocation information and environmental data collected by sensors. The Receiving Party agrees: (i) to take the same security precautions to protect against disclosure or unauthorized use of such Proprietary Information that the Party takes with its own proprietary information, but in no event less than commercially reasonable precautions, and (ii) not to use (except in performance of the Services or as otherwise permitted herein) or divulge to any third person any

such Proprietary Information. The Disclosing Party agrees that the foregoing shall not apply with respect to any information that the Receiving Party can document (a) is or becomes generally available to the public; or (b) was in its possession or known by it prior to receipt from the Disclosing Party; or (c) was rightfully disclosed to it without restriction by a third party; or (d) was independently developed without use of any Proprietary Information of the Disclosing Party. Nothing in this Agreement will prevent the Receiving Party from disclosing the Proprietary Information pursuant to any judicial or governmental order, provided that the Receiving Party gives the Disclosing Party reasonable prior notice of such disclosure to contest such order. At the termination of this Agreement, all Proprietary Information will be returned to the Disclosing Party, destroyed or erased (if recorded on an erasable storage medium), together with any copies thereof, when no longer needed for the purposes above, or upon request from the Disclosing Party, and in any case upon termination of the Agreement. Notwithstanding any termination, all confidentiality obligations of Proprietary Information that is trade secret shall continue in perpetuity or until such information is no longer trade secret.

**5.2 Usage Restrictions on Flock IP.** Flock and its licensors retain all right, title and interest in and to the Flock IP and its components, and Customer acknowledges that it neither owns nor acquires any additional rights in and to the foregoing not expressly granted by this Agreement. Customer further acknowledges that Flock retains the right to use the foregoing for any purpose in Flock's sole discretion. Customer and Authorized End Users shall not: (i) copy or duplicate any of the Flock IP; (ii) decompile, disassemble, reverse engineer, or otherwise attempt to obtain or perceive the source code from which any software component of any of the Flock IP is compiled or interpreted, or apply any other process or procedure to derive the source code of any software included in the Flock IP; (iii) attempt to modify, alter, tamper with or repair any of the Flock IP, or attempt to create any derivative product from any of the foregoing; (iv) interfere or attempt to interfere in any manner with the functionality or proper working of any of the Flock IP; (v) remove, obscure, or alter any notice of any intellectual property or proprietary right appearing on or contained within the Flock Services or Flock IP; (vi) use the Flock Services for anything other than the Permitted Purpose; or (vii) assign, sublicense, sell, resell, lease, rent, or otherwise transfer, convey, pledge as security, or otherwise encumber, Customer's rights. There are no implied rights.

**5.3 Disclosure of Footage.** Subject to and during the Retention Period, Flock may access, use, preserve and/or disclose the Footage to law enforcement authorities, government officials, and/or third parties, if legally required to do so or if Flock has a good faith belief that such access, use, preservation or disclosure is reasonably necessary to comply with a legal process, enforce this Agreement, or detect, prevent or otherwise address security, privacy, fraud or technical issues, or emergency situations.

## **6. PAYMENT OF FEES**

**6.1 Billing and Payment of Fees.** Customer shall pay the fees set forth in the applicable Order Form based on the billing structure and payment terms as indicated in the Order Form. If Customer believes that Flock has billed Customer incorrectly, Customer must contact Flock no later than thirty (30) days after the closing date on the first invoice in which the error or problem appeared to receive an adjustment or credit. Customer acknowledges and agrees that a failure to contact Flock within this period will serve as a waiver of any claim. If any undisputed fee is more than thirty (30) days overdue, Flock may, without limiting its other rights and remedies, suspend delivery of its service until such undisputed invoice is paid in full. Flock shall provide at least thirty (30) days' prior written notice to Customer of the payment delinquency before exercising any suspension right.

**6.2 Notice of Changes to Fees.** Flock reserves the right to change the fees for subsequent Renewal Terms by providing sixty (60) days' notice (which may be sent by email) prior to the end of the Initial Term or Renewal Term (as applicable).

**6.3 Late Fees.** If payment is not issued to Flock by the due date of the invoice, an interest penalty of 1.0% of any unpaid amount may be added for each month or fraction thereafter, until final payment is made.

**6.4 Taxes.** Customer is responsible for all taxes, levies, or duties, excluding only taxes based on Flock's net income, imposed by taxing authorities associated with the order. If Flock has the legal obligation to pay or collect taxes, including amount subsequently assessed by a taxing authority, for which Customer is responsible, the appropriate amount shall be invoice to and paid by Customer unless Customer provides Flock a legally sufficient tax exemption certificate and Flock shall not charge customer any taxes from which it is exempt. If any deduction or

withholding is required by law, Customer shall notify Flock and shall pay Flock any additional amounts necessary to ensure that the net amount that Flock receives, after any deduction and withholding, equals the amount Flock would have received if no deduction or withholding had been required.

## 7. TERM AND TERMINATION

7.1 **Term.** The initial term of this Agreement shall be for the period of time set forth on the Order Form (the “**Term**”). Following the Term, unless otherwise indicated on the Order Form, this Agreement will automatically renew for successive renewal terms of the greater of one year or the length set forth on the Order Form (each, a “**Renewal Term**”) unless either Party gives the other Party notice of non-renewal at least thirty (30) days prior to the end of the then-current term.

7.2 **Termination.** Upon termination or expiration of this Agreement, Flock will remove any applicable Flock Hardware at a commercially reasonable time period. In the event of any material breach of this Agreement, the non-breaching Party may terminate this Agreement prior to the end of the Term by giving thirty (30) days prior written notice to the breaching Party; provided, however, that this Agreement will not terminate if the breaching Party has cured the breach prior to the expiration of such thirty (30) day period (“**Cure Period**”). Either Party may terminate this Agreement (i) upon the institution by or against the other Party of insolvency, receivership or bankruptcy proceedings, (ii) upon the other Party's making an assignment for the benefit of creditors, or (iii) upon the other Party's dissolution or ceasing to do business. In the event of a material breach by Flock, and Flock is unable to cure within the **Cure Period**, Flock will refund Customer a pro-rata portion of the pre-paid fees for Services not received due to such termination.

7.3 **Survival.** The following Sections will survive termination: 1, 3, 5, 6, 7, 8.3, 8.4, 9, 11.1 and 11.6.

## 8. REMEDY FOR DEFECT; WARRANTY AND DISCLAIMER

8.1 **Manufacturer Defect.** Upon a malfunction or failure of Flock Hardware or Embedded Software (a “*Defect*”), Customer must notify Flock’s technical support team. In the event of a Defect, Flock shall make a commercially reasonable attempt to repair or replace the defective Flock Hardware at no additional cost to the Customer. Flock reserves the right, in its sole discretion, to repair or replace such Defect, provided that Flock shall conduct inspection or testing within a commercially reasonable time, but no longer than seven (7) business days after Customer gives notice to Flock.

8.2 **Replacements.** In the event that Flock Hardware is lost, stolen, or damaged, Customer may request a replacement of Flock Hardware at a fee according to the reinstall fee schedule (<https://www.flocksafety.com/reinstall-fee-schedule>). In the event that Customer chooses not to replace lost, damaged, or stolen Flock Hardware, Customer understands and agrees that (1) Flock Services will be materially affected, and (2) that Flock shall have no liability to Customer regarding such affected Flock Services, nor shall Customer receive a refund for the lost, damaged, or stolen Flock Hardware.

8.3 **Warranty.** Flock shall use reasonable efforts consistent with prevailing industry standards to maintain the Services in a manner which minimizes errors and interruptions in the Services and shall perform the Installation Services in a professional and workmanlike manner. Services may be temporarily unavailable for scheduled maintenance or for unscheduled emergency maintenance, either by Flock or by third-party providers, or because of other causes beyond Flock’s reasonable control, but Flock shall use reasonable efforts to provide advance notice in writing or by e-mail of any scheduled service disruption.

8.4 **Disclaimer.** THE REMEDY DESCRIBED IN SECTION 8.1 ABOVE IS CUSTOMER’S SOLE REMEDY, AND FLOCK’S SOLE LIABILITY, WITH RESPECT TO DEFECTS. FLOCK DOES NOT WARRANT THAT THE SERVICES WILL BE UNINTERRUPTED OR ERROR FREE; NOR DOES IT MAKE ANY WARRANTY AS TO THE RESULTS THAT MAY BE OBTAINED FROM USE OF THE SERVICES. EXCEPT AS EXPRESSLY SET FORTH IN THIS SECTION, THE SERVICES ARE PROVIDED “AS IS” AND FLOCK DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A



PARTICULAR PURPOSE AND NON-INFRINGEMENT. THIS DISCLAIMER ONLY APPLIES TO THE EXTENT ALLOWED BY THE GOVERNING LAW OF THE STATE MENTIONED IN SECTION 11.6.

8.5 **Insurance.** Flock will maintain commercial general liability policies as stated in Exhibit B.

8.6 **Force Majeure.** Parties are not responsible or liable for any delays or failures in performance from any cause beyond their control, including, but not limited to acts of God, changes to law or regulations, embargoes, war, terrorist acts, pandemics (including the spread of variants), issues of national security, acts or omissions of third-party technology providers, riots, fires, earthquakes, floods, power blackouts, strikes, supply chain shortages of equipment or supplies, financial institution crisis, weather conditions or acts of hackers, internet service providers or any other third party acts or omissions.

## **9. LIMITATION OF LIABILITY; INDEMNITY**

9.1 **Limitation of Liability.** NOTWITHSTANDING ANYTHING TO THE CONTRARY, FLOCK, ITS OFFICERS, AFFILIATES, REPRESENTATIVES, CONTRACTORS AND EMPLOYEES SHALL NOT BE RESPONSIBLE OR LIABLE WITH RESPECT TO ANY SUBJECT MATTER OF THIS AGREEMENT OR TERMS AND CONDITIONS RELATED THERETO UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY, PRODUCT LIABILITY, OR OTHER THEORY: (A) FOR LOSS OF REVENUE, BUSINESS OR BUSINESS INTERRUPTION; (B) INCOMPLETE, CORRUPT, OR INACCURATE DATA; (C) COST OF PROCUREMENT OF SUBSTITUTE GOODS, SERVICES OR TECHNOLOGY; (D) FOR ANY INDIRECT, EXEMPLARY, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES; (E) FOR ANY MATTER BEYOND FLOCK'S ACTUAL KNOWLEDGE OR REASONABLE CONTROL INCLUDING REPEAT CRIMINAL ACTIVITY OR INABILITY TO CAPTURE FOOTAGE; OR (F) FOR ANY AMOUNTS THAT, TOGETHER WITH AMOUNTS ASSOCIATED WITH ALL OTHER CLAIMS, EXCEED THE FEES PAID AND/OR PAYABLE BY CUSTOMER TO FLOCK FOR THE SERVICES UNDER THIS AGREEMENT IN THE TWELVE (12) MONTHS PRIOR TO THE ACT OR OMISSION THAT GAVE RISE TO THE LIABILITY, IN EACH CASE, WHETHER OR NOT FLOCK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF

LIABILITY OF SECTION ONLY APPLIES TO THE EXTENT ALLOWED BY THE GOVERNING LAW OF THE STATE REFERENCED IN SECTION 10.6.

NOTWITHSTANDING ANYTHING TO THE CONTRARY, THE FOREGOING LIMITATIONS OF LIABILITY SHALL NOT APPLY (I) IN THE EVENT OF GROSS NEGLIGENCE OR WILLFUL MISCONDUCT, OR (II) INDEMNIFICATION OBLIGATIONS.

**9.2 Responsibility.** Each Party to this Agreement shall assume the responsibility and liability for the acts and omissions of its own employees, officers, or agents, in connection with the performance of their official duties under this Agreement. Each Party to this Agreement shall be liable for the torts of its own officers, agents, or employees.

**9.3 Flock Indemnity.** Flock shall indemnify and hold harmless Customer, its agents and employees, from liability of any kind, including claims, costs (including defense) and expenses, on account of: (i) any copyrighted material, patented or unpatented invention, articles, device or appliance manufactured or used in the performance of this Agreement; or (ii) any damage or injury to property or person directly caused by Flock's installation of Flock Hardware, except for where such damage or injury was caused solely by the negligence of the Customer or its agents, officers or employees. Flock's performance of this indemnity obligation shall not exceed the fees paid and/or payable for the services rendered under this Agreement in the preceding twelve (12) months.

## 10. INSTALLATION SERVICES AND OBLIGATIONS

**10.1 Ownership of Hardware.** Flock Hardware is owned and shall remain the exclusive property of Flock. Title to any Flock Hardware shall not pass to Customer upon execution of this Agreement, except as otherwise specifically set forth in this Agreement. Except as otherwise expressly stated in this Agreement, Customer is not permitted to remove, reposition, re-install, tamper with, alter, adjust or otherwise take possession or control of Flock Hardware. Customer agrees and understands that in the event Customer is found to engage in any of the foregoing restricted actions, all warranties herein shall be null and void, and this Agreement shall be subject to immediate termination for material breach by Customer. Customer shall not perform any acts which would interfere with the retention of title of the Flock Hardware by Flock. Should Customer default on any payment of the Flock Services, Flock may remove Flock Hardware at

Flock's discretion. Such removal, if made by Flock, shall not be deemed a waiver of Flock's rights to any damages Flock may sustain as a result of Customer's default and Flock shall have the right to enforce any other legal remedy or right.

**10.2 Deployment Plan.** Flock shall advise Customer on the location and positioning of the Flock Hardware for optimal product functionality, as conditions and locations allow. Flock will collaborate with Customer to design the strategic geographic mapping of the location(s) and implementation of Flock Hardware to create a deployment plan ("***Deployment Plan***"). In the event that Flock determines that Flock Hardware will not achieve optimal functionality at a designated location, Flock shall have final discretion to veto a specific location, and will provide alternative options to Customer.

**10.3 Changes to Deployment Plan.** After installation of Flock Hardware, any subsequent requested changes to the Deployment Plan, including, but not limited to, relocating, re-positioning, adjusting of the mounting, removing foliage, replacement, changes to heights of poles will incur a fee according to the reinstall fee schedule located at (<https://www.flocksafety.com/reinstall-fee-schedule>). Customer will receive prior notice and confirm approval of any such fees.

**10.4 Customer Installation Obligations.** Customer is responsible for any applicable supplementary cost as described in the Customer Implementation Guide, attached hereto as Exhibit C ("***Customer Obligations***"). Customer represents and warrants that it has, or shall lawfully obtain, all necessary right title and authority and hereby authorizes Flock to install the Flock Hardware at the designated locations and to make any necessary inspections or maintenance in connection with such installation.

**10.5 Flock's Obligations.** Installation of any Flock Hardware shall be installed in a professional manner within a commercially reasonable time from the Effective Date of this Agreement. Upon removal of Flock Hardware, Flock shall restore the location to its original condition, ordinary wear and tear excepted. Flock will continue to monitor the performance of Flock Hardware for the length of the Term. Flock may use a subcontractor or third party to perform certain obligations under this agreement, provided that Flock's use of such subcontractor or third party shall not release Flock from any duty or liability to fulfill Flock's obligations under this Agreement.

## **11. MISCELLANEOUS**

**11.1 Compliance With Laws.** Parties shall comply with all applicable local, state and federal laws, regulations, policies and ordinances and their associated record retention schedules, including responding to any subpoena request(s).

**11.2 Severability.** If any provision of this Agreement is found to be unenforceable or invalid, that provision will be limited or eliminated to the minimum extent necessary so that this Agreement will otherwise remain in full force and effect.

**11.3 Assignment.** This Agreement is not assignable, transferable or sublicensable by either Party, without prior consent. Notwithstanding the foregoing, either Party may assign this Agreement, without the other Party's consent, (i) to any parent, subsidiary, or affiliate entity, or (ii) to any purchaser of all or substantially all of such Party's assets or to any successor by way of merger, consolidation or similar transaction.

**11.4 Entire Agreement.** This Agreement, together with the Order Form(s), the reinstall fee schedule (<https://www.flocksafety.com/reinstall-fee-schedule>), and any attached exhibits are the complete and exclusive statement of the mutual understanding of the Parties and supersedes and cancels all previous or contemporaneous negotiations, discussions or agreements, whether written and oral, communications and other understandings relating to the subject matter of this Agreement, and that all waivers and modifications must be in a writing signed by both Parties, except as otherwise provided herein. None of Customer's purchase orders, authorizations or similar documents will alter the terms of this Agreement, and any such conflicting terms are expressly rejected. Any mutually agreed upon future purchase order is subject to these legal terms and does not alter the rights and obligations under this Agreement, except that future purchase orders may outline additional products, services, quantities and billing terms to be mutually accepted by Parties. In the event of any conflict of terms found in this Agreement or any other terms and conditions, the terms of this Agreement shall prevail. Customer agrees that Customer's purchase is neither contingent upon the delivery of any future functionality or features nor dependent upon any oral or written comments made by Flock with respect to future functionality or feature.

**11.5 Relationship.** No agency, partnership, joint venture, or employment is created as a result of this Agreement and Parties do not have any authority of any kind to bind each other in any respect whatsoever. Flock shall at all times be and act as an independent contractor to Customer.

**11.6 Governing Law; Venue.** This Agreement shall be governed by the laws of the state in which the Customer is located. The Parties hereto agree that venue would be proper in the chosen courts of the State of which the Customer is located. The Parties agree that the United Nations Convention for the International Sale of Goods is excluded in its entirety from this Agreement.

**11.7 Special Terms.** Flock may offer certain special terms which are indicated in the proposal and will become part of this Agreement, upon Customer's prior written consent and the mutual execution by authorized representatives ("*Special Terms*"). To the extent that any terms of this Agreement are inconsistent or conflict with the Special Terms, the Special Terms shall control.

**11.8 Publicity.** Flock has the right to reference and use Customer's name and trademarks and disclose the nature of the Services in business and development and marketing efforts.

**11.9 Feedback.** If Customer or Authorized End User provides any suggestions, ideas, enhancement requests, feedback, recommendations or other information relating to the subject matter hereunder, Agency or Authorized End User hereby assigns to Flock all right, title and interest (including intellectual property rights) with respect to or resulting from any of the foregoing.

**11.10 Export.** Customer may not remove or export from the United States or allow the export or re-export of the Flock IP or anything related thereto, or any direct product thereof in violation of any restrictions, laws or regulations of the United States Department of Commerce, the United States Department of Treasury Office of Foreign Assets Control, or any other United States or foreign Customer or authority. As defined in Federal Acquisition Regulation ("FAR"), section 2.101, the Services, the Flock Hardware and Documentation are "commercial items" and according to the Department of Defense Federal Acquisition Regulation ("DFAR") section 252.2277014(a)(1) and are deemed to be "commercial computer software" and "commercial computer software documentation." Flock is compliant with FAR Section 889 and does not contract or do business with, use any equipment, system, or service that uses the enumerated banned Chinese telecommunication companies, equipment or services as a substantial or essential component of any system, or as critical technology as part of any Flock system. Consistent with DFAR section 227.7202 and FAR section 12.212, any use, modification, reproduction, release, performance, display, or disclosure of such commercial software or commercial software documentation by the U.S. Government will be governed solely by the terms of this Agreement and will be prohibited except to the extent expressly permitted by the terms of this Agreement.

11.11 **Headings.** The headings are merely for organization and should not be construed as adding meaning to the Agreement or interpreting the associated sections.

11.12 **Authority.** Each of the below signers of this Agreement represent that they understand this Agreement and have the authority to sign on behalf of and bind the Parties they are representing.

11.13 **Conflict.** In the event there is a conflict between this Agreement and any applicable statement of work, or Customer purchase order, this Agreement controls unless explicitly stated otherwise.

11.14 **Morality.** In the event Customer or its agents become the subject of an indictment, contempt, scandal, crime of moral turpitude or similar event that would negatively impact or tarnish Flock's reputation, Flock shall have the option to terminate this Agreement upon prior written notice to Customer.

11.15 **Notices.** All notices under this Agreement will be in writing and will be deemed to have been duly given when received, if personally delivered; when receipt is electronically confirmed, if transmitted by email; the day after it is sent, if sent for next day delivery by recognized overnight delivery service; and upon receipt to the address listed on the Order Form (or, if different, below), if sent by certified or registered mail, return receipt requested.

11.16 **Non-Appropriation.** Notwithstanding any other provision of this Agreement, all obligations of the Customer under this Agreement which require the expenditure of funds are conditioned on the availability of funds appropriated for that purpose. Customer shall have the right to terminate this Agreement for non appropriation with thirty (30) days written notice without penalty or other cost.

FLOCK NOTICES ADDRESS:

1170 HOWELL MILL ROAD, NW SUITE 210

ATLANTA, GA 30318

ATTN: LEGAL DEPARTMENT

EMAIL: [legal@flocksafety.com](mailto:legal@flocksafety.com)

Customer NOTICES ADDRESS:

ADDRESS:

ATTN:

EMAIL:

---

---

---

EXHIBIT B  
**INSURANCE**

**Required Coverage.** Flock shall procure and maintain for the duration of this Agreement insurance against claims for injuries to persons or damages to property that may arise from or in connection with the performance of the services under this Agreement and the results of that work by Flock or its agents, representatives, employees or subcontractors. Insurance shall be placed with insurers with a current A. M. Best rating of no less than “A” and “VII”. Flock shall obtain and, during the term of this Agreement, shall maintain policies of professional liability (errors and omissions), automobile liability, and general liability insurance for insurable amounts of not less than the limits listed herein. The insurance policies shall provide that the policies shall remain in full force during the life of the Agreement. Flock shall procure and shall maintain during the life of this Agreement Worker's Compensation insurance as required by applicable State law for all Flock employees.

**Types and Amounts Required.** Flock shall maintain, at minimum, the following insurance coverage for the duration of this Agreement:

- (i) **Commercial General Liability** insurance written on an occurrence basis with minimum limits of One Million Dollars (\$1,000,000) per occurrence and Two Million Dollars (\$2,000,000) in the aggregate for bodily injury, death, and property damage, including personal injury, contractual liability, independent contractors, broad-form property damage, and product and completed operations coverage;
- (ii) **Umbrella or Excess Liability** insurance written on an occurrence basis with minimum limits of Ten Million Dollars (\$10,000,000) per occurrence and Ten Million Dollars (\$10,000,000) in the aggregate;
- (iii) **Professional Liability/Errors and Omissions** insurance with minimum limits of Five Million Dollars (\$5,000,000) per occurrence and Five Million Dollars (\$5,000,000) in the aggregate;
- (iv) **Commercial Automobile Liability** insurance with a minimum combined single limit of One Million Dollars (\$1,000,000) per occurrence for bodily injury, death, and property coverage, including owned and non-owned and hired automobile coverage; and



(v) **Cyber Liability** insurance written on an occurrence basis with minimum limits of Five Million Dollars (\$5,000,000).



---

Date: February 8, 2024  
To: Board of Directors  
From: David Aranda, Interim General Manager  
Subject: Approval of the Automated License Plate Reader Policy

---

### **Recommendation**

Approval of the Automated License Plate Readers Policy (ALPRs).

### **Background**

At the January 11, 2024, Board of Directors meeting, the agenda consisted of purchasing a software program that allows license plate reading to assist the Police Department in dealing with various potential crimes in the community. The Board approved the purchase with a company called FLOCK, subject to the proper contract wording as presented by legal. FLOCK agreed to using the contract wording presented and the contract has been executed.

The Board also requested a policy to address this software and the use and distribution of what the software generates. The motion that was approved in January was to make some changes to the policy that was presented and to bring the policy back to the Board. Below is the motion that was made in January noting the changes that staff was directed to make.

- Motion by Director Hacaj, seconded by Director Duggan, that the Board of Directors adopted the policy before us with the following modifications which we will need to see back before us and those modifications are a correction on Section 426.3.1 outlined by Vice-President Aquino-Fike which is to strike the second sentence and turn the third sentence into a new subsection F and renumber F to G to clarify the first paragraph on page 5 that begins with all "ALPR data downloaded to the server" in particular to understand which server they are referring to, and lastly to reference the civil code for the records release and maintenance policy under 426.6, carried (5-0) by the following roll call vote: AYES (Aquino-Fike, Duggan, Gough, Hacaj and Spath); NOES (None); ABSTAINED (none); ABSENT (none).

The attached draft policy highlights those changes in yellow.

### **Exhibit(s)**

- Automated License Plate Readers Policy 426

## Automated License Plate Readers (ALPRs)

### 426.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance for the capture, storage and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology.

### 426.2 DEFINITIONS

- Automated License Plate Reader (ALPR) : A device that uses cameras and computer technology to compare digital images to lists of known information of interest.
- ALPR Operator : Trained Department members who may utilize ALPR system/equipment. ALPR operators may be assigned to any position within the Department, and the ALPR Administrator may order the deployment of the ALPR systems for use in various efforts.
- ALPR Administrator : The Chief of Police or their designee, serve as the ALPR Administrator for the Department.
- Hot List : A list of license plates associated with vehicles of interest compiled from one or more databases including, but not limited to, NCIC, CA 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 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) 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.

### 426.3 ADMINISTRATION

The ALPR technology, also known as License Plate Recognition (LPR), allows for the automated detection of license plates along with the vehicle make, model, color and unique identifiers through the Kensington Police Department's ALPR's system and the vendor's vehicle identification technology. The technology is used by the Kensington Police Department to convert data associated with vehicle license plates and vehicle descriptions for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates and missing persons. It may also be used to gather information related to active warrants, suspect interdiction and stolen property recovery.

All installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Chief of Police who will assign members under his/her

# Kensington Police Department

## Kensington Police Department Policy Manual

### *Automated License Plate Readers (ALPRs)*

---

command to administer the day-to-day operation of the ALPR equipment and data.

#### **426.3.1 ALPR ADMINISTRATOR**

The Chief of Police shall be responsible for compliance with the requirements of Civil Code § 1798.90.5 et seq. This includes, but is not limited to (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

- (a) Only properly trained sworn officers, crime analysts, communication operators, records clerks and police assistants are allowed access to the ALPR system or to collect ALPR information.
- (b) Ensuring that training requirements are completed for authorized users.
- (c) ALPR system monitoring to ensure the security of the information and compliance with applicable privacy laws.
- (d) Ensuring that procedures are followed for system operators and to maintain records of access in compliance with Civil Code § 1798.90.52.
- (e) The title and name of the current designee in overseeing the ALPR operation is maintained.
- (f) Continually working with the Custodian of Records on the retention and destruction of ALPR data.
- (g) Ensuring this policy and related procedures are conspicuously posted on the department's website.

#### **426.4 OPERATIONS**

Use of an ALPR is restricted to the purposes outlined below. Department members shall not use, or allow others to use the equipment or database records for any unauthorized purpose (Civil Code § 1798.90.51; Civil Code § 1798.90.53).

- (a) An ALPR shall only be used for official law enforcement business.
- (b) An ALPR may be used in conjunction with any routine patrol operation or criminal investigation. Reasonable suspicion or probable cause is not required before using an ALPR.
- (c) Partial license plates and unique vehicle descriptions reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.
- (d) The officer should verify an ALPR response through the California Law Enforcement Telecommunications System (CLETS) or dispatch before taking enforcement action based solely on an ALPR alert. Because the ALPR alert may relate to a vehicle and may not relate to the person operating the vehicle, officers are reminded that they need to have reasonable suspicion and/or probable cause to make an enforcement stop of any vehicle. (For example, if a vehicle is entered into the system because of its association with a wanted individual, Officers should attempt to visually match the

# Kensington Police Department

## Kensington Police Department Policy Manual

### *Automated License Plate Readers (ALPRs)*

---

driver to the description of the wanted subject prior to making the stop or should have another legal basis for making the stop.

- (e) Designation of hot lists to be utilized by the ALPR system shall be made by the Chief of Police or their designee. Hot lists shall be obtained or compiled from sources as may be consistent with the purposes of the ALPR system set forth in this policy. Hot lists utilized by the Department's ALPR system may be updated by agency sources more frequently than the Department may be uploading them and thus the Department's ALPR system will not have access to real time data. Occasionally, there may be errors in the ALPR system's read of a license plate, therefore an alert alone shall not be a basis for a police action (other than following the vehicle of interest).

Prior to initiation of a stop of a vehicle or other intervention based on an alert, Department members shall undertake the following:

- (a) Verification of status on a hot list; An officer must receive confirmation, from a Police Department Communications Dispatcher or other Department computer device, that the license plate is still stolen, wanted, or otherwise of interest before proceeding (absent exigent circumstances).
- (b) Visual verification of license plate number; Officers shall visually verify that the license plate of interest matches the image of the license plate number captured (read) by the ALPR, including both the alphanumeric characters of the license plate, state of issue, and vehicle descriptors before proceeding. Department members alerted to the fact that an observed motor vehicle's license plate is entered as a hot plate (hit) in a specific BOLO (be on the lookout) list are required to make a reasonable effort to confirm that a wanted person is actually in the vehicle and/or that a reasonable basis exists before a Department member would have a lawful basis to stop the vehicle.

Department members will clear all stops from hot list alerts by indicating the positive ALPR hit, i.e., with an arrest or other enforcement action. If it is not obvious in the text of the call as to the correlation of the ALPR hit and the arrest, then the Department member shall update with the Communications Dispatcher and original person and/or a crime analyst inputting the vehicle in the hot list (hit).

General hot lists (SVS, SFR, and SLR) will be automatically downloaded into the ALPR system a minimum of once a day with the most current data overwriting the old data.

- (a) All entries and updates of specific hot lists within the ALPR system will be documented by the requesting Department member within the appropriate general offense report. As such, specific hot lists shall be approved by the ALPR Administrator (Lieutenant or Chief of Police designee) before initial entry within the ALPR system. The updating of such a list within the ALPR system shall thereafter be accomplished pursuant to the approval of the Department member's immediate supervisor. The hits from these data sources should be viewed as informational; created solely to bring the officers attention to specific vehicles that have been associated with criminal activity.

All hot plates and suspect information entered into the ALPR system will contain the following information as a minimum:

- (a) Entering Department member's name

# Kensington Police Department

## Kensington Police Department Policy Manual

### Automated License Plate Readers (ALPRs)

---

- (b) Related case number.
- (c) Short synopsis describing the nature of the originating call.

#### Login/Log-Out Procedure.

- (a) To ensure proper operation and facilitate oversight of the ALPR system, all users will be required to have individual credentials for access and use of the systems and/or data, which has the ability to be fully audited.

#### Permitted/Impermissible Uses.

- (a) The ALPR system, and all data collected, is the property of the Kensington Police Department. Department 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*: Except when done pursuant to a court order such as a search warrant, it is a violation of this policy to utilize the ALPR to record license plates except those of vehicles that are 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).
  2. *Harassment or Intimidation*: It is a 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*: 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, gender, religion, political affiliation, nationality, ethnicity, sexual orientation, disability, or other classification protected by law.
  4. *Personal Use*: It is a violation of this policy to use the ALPR system or associated scan files or hot lists for any personal purpose.
  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.

Anyone who engages in an impermissible use of the ALPR system or associated scan files or hot lists may be subject to:

- (a) criminal prosecution,
- (b) civil liability, and/or
- (c) administrative sanctions, up to and including termination, pursuant to and consistent with the relevant collective bargaining agreements and Department policies

#### **426.5 DATA RETENTION AND COLLECTION**

The Chief of Police is responsible for ensuring systems and processes are in place for the proper collection and retention of ALPR data. Data will be transferred from vehicles to the designated storage in accordance with Department procedures.

# Kensington Police Department

Kensington Police Department Policy Manual

## *Automated License Plate Readers (ALPRs)*

---

In the event ALPR data must be downloaded from the Flock server to the police department server for an ongoing criminal investigation, it shall be stored for no longer than one year in accordance with the established records retention schedule. Thereafter, all ALPR data shall be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a discovery request or other lawful action to produce records. In those circumstances, the applicable data shall be downloaded from the police department server onto a separate secure media device and placed into evidence.

The ALPR vendor, Flock Safety, will store all captured KPD data on their servers and ensure proper maintenance and security of the information is kept. Flock Safety shall purge all KPD data at the end of the 30 days of storage.

Restrictions on use of ALPR data:

- (a) Information gathered or collected, and records retained by Flock Safety cameras or any other Department ALPR system will not be sold, accessed, or used for any purpose other than legitimate law enforcement or public safety purposes.

### **426.6 ACCOUNTABILITY AND SAFEGUARDS**

All data will be closely safeguarded and protected by both procedural and technological means. The Kensington Police Department will observe the following safeguards regarding access to and use of stored data (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

- (a) All non-law enforcement requests for access to stored ALPR data shall be processed in accordance with applicable law.
- (b) All ALPR data downloaded to the mobile workstation shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date, and time.
- (c) 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 relate to a specific criminal investigation or Department related civil or administrative action.
- (d) Such ALPR data may be released to other authorized and verified law enforcement officials and agencies for legitimate law enforcement purposes.
- (e) Every ALPR detection browsing inquiry must be documented by either the associated Kensington Police case number or incident number, and/or a reason for the inquiry.

For security or data breaches, see the Records Release and Maintenance Policy.

### **426.7 POLICY**

The policy of the Kensington Police Department is to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public. All data and images gathered by the ALPR are for the official use of this Department. Because such data may contain confidential information, it is not open to public review.

# Kensington Police Department

Kensington Police Department Policy Manual

## *Automated License Plate Readers (ALPRs)*

---

The Kensington Police Department does not permit the sharing of ALPR data gathered by the KPPCSD or its contractors/subcontractors for purpose of federal immigration enforcement, pursuant to the California Values (Government Code § 7282.5; Government Code § 7284.2 et seq) – these federal immigration agencies include Immigrations and Customs Enforcement (ICE) and Customs and Border Patrol.

### **426.8 ALPR DATA DETECTION BROWSING AUDITS**

It is the responsibility of the Chief of Police to ensure that an audit is conducted of ALPR detection browsing inquiries at least once during each calendar year. The Department will audit a sampling of the ALPR system utilization from the prior 12-month period to verify proper use in accordance with the above authorized uses. The audit shall randomly select at least 10 detection browsing inquiries conducted by Department employees during the preceding six-month period and determine if each inquiry meets the requirements established in policy section 462.6(e).

The audit shall be documented in the form of an internal Department memorandum to the Chief of Police. The memorandum shall include any data errors found so that such errors can be corrected. After review by the Chief of Police, the memorandum and any associated documentation shall be filed and retained by PSD.

### **426.9 RELEASING ALPR DATA**

The ALPR data may be shared only with other law enforcement or prosecutorial agencies when there is a need to know, a right to know or legal obligation to provide the information.

The agency request for the ALPR data must be in writing and include:

- (a) The name of the agency.
- (b) The name of the person requesting.
- (c) The intended purpose of obtaining the information.

The request is should be reviewed and approved by the Chief of Police or the authorized designee before the request is fulfilled.

The Chief of Police will consider the California Values Act (Government Code § 7282.5; Government Code § 7284.2 et seq), before approving the release of ALPR data. The Kensington Police Department does not permit the sharing of ALPR data gathered by the KPPCSD or its contractors/subcontractors for purpose of federal immigration enforcement, these federal immigration agencies include Immigrations and Customs Enforcement (ICE) and Customs and Border Patrol (CPB).

The Chief of Police will also consider the California Reproductive Privacy Act (Health and Safety Code § 123460 - § 123469) before approving the sharing of ALPR data for the purpose of investigating any person seeking to exercise their reproductive health care rights within California. The Kensington Police Department does not permit the sharing of ALPR data gathered by the District or its contractors/subcontractors for the purpose of prosecuting, investigating or initiating



# Kensington Police Department

Kensington Police Department Policy Manual

## *Automated License Plate Readers (ALPRs)*

---

any legal proceeding against any person for the exercise of reproductive health care rights as defined by California law.

The approved request is retained on file. Requests for ALPR data by non-law enforcement or nonprosecutorial agencies will be processed as provided in the Records Maintenance and Release Policy (Civil Code § 1798.90.55).

Agencies outside of California that request to access ALPR data through Flock Safety Portal must agree to abide by all applicable Federal and California State Laws as well as Department policy.

- (a) The Department will send a data sharing request to the agency which must be completed and returned prior to the granting of access
- (b) The ALPR Administrator (Lieutenant or Chief of Police designee) will maintain these documents for the entirety of the shared data agreement
- (c) Access to KPD ALPR data can be stopped at anytime by authorized KPD Command Staff.

### **426.10 TRAINING**

The Training Sergeant should ensure that members receive department-approved training for those authorized to use or access the ALPR system (Civil Code § 1798.90.51; Civil Code §1798.90.53).

No member of this Department shall operate ALPR equipment or access ALPR data without first completing Department-approved training.



# KENSINGTON POLICE COMMUNITY MESSAGE

## Temporary Suspension of License Plate Reader Functionality

**Date:** February 12, 2026

The Kensington Police Department temporarily suspended the Automatic License Plate Reader (ALPR) functionality associated with the District's community safety camera system for a 90-day evaluation period. This pause began on February 12, 2026, and will remain in place through approximately May 12, 2026.

This decision was not made lightly.

The ALPR system has proven to be a valuable public/officer safety tool. It assisted in identifying stolen vehicles, locating vehicles associated with crimes, and enhancing officer awareness during field contacts and investigations. Our personnel have used this technology responsibly, ethically, and in accordance with established policy.

However, recent reports involving alleged unauthorized access to camera data in other jurisdictions have raised concerns. While those reports do not involve Kensington and there has been no evidence of misuse within our system, public confidence is foundational to any public safety program. Out of an abundance of caution — and in recognition of the public's interest — we believe it is appropriate to conduct a thorough review.

### What We Are Evaluating

During these 90 days, the Department will:

- Re-examine technological value & relevance for Kensington
- Review system access controls and auditing procedures
- Re-examine data retention and sharing protocols
- Evaluate policy language and oversight mechanisms
- Ensure alignment with current legal standards and best practices
- Assess community feedback and questions regarding privacy, transparency, and retention

This evaluation is focused on governance and safeguards, not on the operational integrity of the equipment itself.

## **Commitment to Transparency and Public Trust**

Technology in policing must be both effective and trusted. The Kensington Police Department remains committed to:

- Ethical collection and analysis of data
- Compliance with all applicable laws
- Strong internal oversight and accountability
- Clear communication with the community we serve

We recognize that misinformation contributes to confusion about how license plate reader technology functions and how data is controlled. As part of this review, we will ensure that our policies and safeguards are clearly explained and accessible to the public.

## **Officer Safety and Public Safety Considerations**

While the ALPR alert functionality is paused, officers will continue to rely on traditional investigative methods and heightened situational awareness during traffic stops and field contacts. We remain vigilant in our mission to protect the community and ensure officer safety.

## **What Happens Next**

At the conclusion of the 90-day review, a determination will be made regarding the reinstatement of the ALPR functionality. That decision will be guided by:

- The results of our policy and systems evaluation
- Any recommended enhancements to safeguards
- Our confidence in maintaining both effectiveness and public trust

Public safety initiatives must balance innovation, accountability, and community confidence. This temporary pause reflects our commitment to getting that balance right.

We appreciate the professionalism of our officers, the engagement of our community, and the importance of thoughtful dialogue regarding the use of technology in policing.

Thank you for your continued partnership and trust.



**Mike Gancasz**  
Chief of Police  
Kensington Police Department