

Police Camera Working Group

June 8, 2026

6 PM

Second Floor Meeting Room, Groton Town Hall

1. Introductions
2. Mission Statement/Goals
3. History of Cameras
4. Demo of Flock
5. Differences between Flock and Axon
6. Setting next meeting date: July/August

Meeting notes:

- Members present – Rachael Mead, GPD; Brian Callahan, Groton DPW, Christopher Reardon, Paul Garcia, Patrick Parker-Roche
- Group introduced themselves and explained their area of expertise
 - Reardon – criminal defense attorney
 - Garcia – cyber security
 - Parker-Roche – AI, cyber security, lives at one of the problem traffic intersections in town
 - Callahan – DPW Director
- Reviewed possible mission statement and goals for the group
- Discussed the history of the cameras, why the department asked for them, how they were added to the budget, what we hoped to get out of having them, and the future of the program, as well as the potential concerns with body worn cameras that we will discuss in the future
- Demo of the system was given
- Next Meeting is August 18, 2026 at 6 PM
 - Finalize the mission statement
 - Will discuss the differences between Flock and Axon – I have a meeting with Axon on June 16 at 11 AM to report back to the group.
 - Review of the department policy on the cameras
 - Anything else that comes up between now and August 18, 2026 in reference to this topic

Mission Police Camera Working Group

Option 1: Professional and Balanced

The mission of the Police Camera Working Group is to evaluate and provide informed recommendations regarding public safety camera technologies, ensuring transparency, accuracy, and community engagement. Through collaborative discussion and diverse perspectives, the group seeks to address community questions, promote understanding, and support responsible technology investments that enhance public safety and crime prevention in Groton.

Option 2: Community-Focused

The Police Camera Working Group is committed to fostering open dialogue, transparency, and public trust as Groton explores and implements camera technologies. By bringing together individuals with diverse backgrounds and viewpoints, the group will examine the benefits, challenges, and community concerns associated with these technologies and provide thoughtful guidance that serves the best interests of the town.

Option 3: Concise

To provide objective, community-informed guidance on police camera technologies by evaluating their effectiveness, addressing public concerns, and supporting transparent decision-making that enhances public safety in Groton.

Option 4: Emphasizing Public Trust

The mission of the Police Camera Working Group is to promote informed, transparent, and community-centered discussions about police camera technologies. By examining facts, addressing questions and concerns, and considering diverse viewpoints, the group will help ensure that technology investments support public safety while maintaining community trust and accountability.

Option 5: Future-Oriented

The Police Camera Working Group exists to evaluate current and emerging camera technologies, including fixed cameras, license plate readers, and body-worn cameras, through a collaborative and transparent process. The group's goal is to provide informed recommendations, address community concerns, and support technology decisions that improve public safety, accountability, and public confidence in the Groton Police Department.



Michael F. Luth
Chief of Police

GROTON POLICE DEPARTMENT

99 Pleasant Street
Groton, MA 01450
Tel: (978) 448-5555
Fax: (978) 448-5603



Rachael E. Bielecki
Deputy Chief

To: Mark Haddad, Town Manager
From: Michael F. Luth, Chief of Police
Date: January 17, 2026
RE: Flock Traffic Camera System

Mark,

The Flock Camera system was presented before and approved by the combined Select Board and Finance Committee budget review last February. The information that the system collects is used for traffic analytics, and motor vehicle crash and/or criminal investigations. There are only three members of the Department that have access to the systems: the Deputy Chief, a Sergeant and the Detective. The information collected is owned by the police department and is shared with other law enforcement agencies in Massachusetts upon request.

The system has been operational since November 2025. We have used it for a number of suspicious vehicle complaints, assisted local area police departments with criminal investigations that involved a vehicle leaving the scene of a crime, and to assist us with investigating traffic accidents. The information is treated as we would any motor vehicle information, and we follow state CJIS practices when gathering, sharing and accessing any of the data on system.

When the system has been fully operational for six months, we will begin analyzing traffic data for use in traffic enforcement and safety design.

Thank you,


Michael Luth
Chief of Police

May 27, 2026

In the year preceding the Flock System coming online there were five serious incidents that the technology would have greatly enhanced our investigative ability and case outcomes. In all the cases below the suspects(s) drove through the intersection of Main St. and Lowell Rd.

Person brandishing a firearm in a dispute at a restaurant in the center of town – case solved days later, suspect would most likely have been identified and arrested the same night.

- Major Arson investigation – case still ongoing now, months and hundreds of investigative hours later – may have led to arrests the same day.
- Male subject from Conn. sexually exposing self to teenage girls and others in a retail establishment - case solved several days later, most likely would have led to suspect being identified and arrested prior to him reaching Interstate 495. This suspect, who was already on probation for sexual crimes, cut off his GPS monitoring device after Conn. Police interviewed him on our behalf. He is currently a wanted fugitive.
- Detail Officer clipped by motor vehicle on detail – not solved.
- Dumping of a large boat and trailer costing the Town thousands to dispose of – not solved.

We are using the system for legitimate law enforcement purposes, period. We control and manage our own data. The article that you forwarded, shows the FBI is looking to contract with companies for their own system of LPR's which does not provide them with our data. It also debunks the claim that the FEDs will access our data through a "back door". Many that are a part of the online echo chamber that is against the use of the technology have repeatedly disregarded the information and answers provided by Deputy Chief Mead. It is clear that regardless of what we say or provide, they will remain nay sayers. Again, we are using the technology for legitimate law enforcement and I do not intend to sway from this because it is politically unpopular with a group in town.

We went through the proper budgetary process in 2025 to allocate for the contracting of the technology and service. At the recent Town Meeting the Police Capital Budget was cut by a margin of approximately 20 votes. The Select Board overwhelmingly approved my plan in fulfilling the current two-year agreement with Flock by votes of 5-0 and 4-1 at the recent meetings.

Deputy Chief Mead has begun the process of establishing a working group to address the use of Flock technology in the future. I have every intention in honoring the current agreement and we will get the most out of the technology that we can. In a time period where our staffing has

been cut and through the shortsighted vote to cut the capital budget, we need to leverage technology to provide the level of policing that this town has become accustomed to.

Thank you,

Mike

May 27, 2026

To echo the Chief, since having this system our case close rates have significantly increased, as I stated at the Select Board meeting. Cases we would not have been able to solve have been solved because of evidence we gathered through the system, to include: suspicious activity/vehicles, disturbances where a vehicle was involved or used, multiple crashes/leaving the scene every week (we are able to have evidence to prove reckless operation and are now able to hold those drivers responsible through our judicial system), and we are currently investigating a number of felony level cases that I am not able to discuss as they are active and ongoing and my detective unit are working them.

We are using the technology every day to help us protect the citizens and businesses in the community. In speaking with the detective unit, the only unit who has access, they have told me that this technology has been insurmountable in helping them with investigations and assisting them in having a higher case clearance rate. This will help keep the town the safe community we are and allows us to continue to provide a level of service that citizens expect, despite our declining staffing over recent years.

We chose this technology because our biggest complaint from these very citizens who are complaining about the technology, are traffic issues and traffic concerns. We listened to them and found a solution to help us better address these issues. Those few who are most vocal are continuing to spread false and debunked statements about the technology and I look forward to working with the working group to show the citizens the benefits of having this technology in our community.

Best,

Rachael Mead

Deputy Chief

Groton Police



GROTON POLICE DEPARTMENT

		DEPARTMENT MANUAL; P&P Operations	
POLICY & PROCEDURE #: 1.47		DATE OF ISSUE:	EFFECTIVE DATE:
		2/2/2026	2/2/2026
SUBJECT: Flock Safety Cameras (ALPR)		ISSUING AUTHORITY: Chief Michael F. Luth	
REFERENCE(S): Massachusetts Police Accreditation Commission # 41.3.9		☒ _X_NEW ☐ _AMENDS ☐ _RESCINDS	

I. GENERAL CONSIDERATIONS AND GUIDELINES

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.

II. POLICY

The ALPR technology, also known as License Plate Recognition (LPR), allow for the automated detection of license plates along with the vehicle make, model, color and unique identifiers through the Groton Police Department's ALPR system and the vendor's (Flock Safety) vehicle identification technology. The technology is used by the Groton 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, electronic surveillance, suspect interdiction and stolen property recovery.

III. 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 may utilize ALPR system/equipment as deemed by the ALPR administrator. 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 Deputy Chief serves 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, CJIS, MA RMV, Local BOLO's, etc.

Vehicles of Interest: Including, but not limited to, vehicles which are reported as stolen, display stolen license plates, linked to missing/wanted persons and vehicles flagged by the RMV or other law enforcement agencies.

Detection: Data obtained by an ALPR of an image within a 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 scanned a 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, relation to a stolen license plate/vehicle, wanted person, missing person, or terrorist related activity.

IV. PROCEDURES [41.3.9(3A)(3B)]

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.

1. Training – No member of this department shall operate ALPR equipment or access ALPR data without first completing department approved training.
2. Login/Logout Procedure – To ensure proper operation and to facilitate oversight of the ALPR system, all users will be required to have individual credentials for access and use of the system and/or data, which has the ability to be fully audited.
3. Permitted/Impermissible Uses – The ALPR system and all data collected is property of the Groton 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:
 - a. Harassment or Intimidation - It is a violation of this policy to use the ALPR system to harass and/or intimidate any individual group.
 - b. Use based on a protected characteristic – it is a violation of this policy to use the ALPR system or associated files or hot lists solely based on a person's or group's race, gender, religion, political affiliation, nationality, ethnicity, sexual orientation, disability, or other classification protected by law.
 - c. Personal use: it is a violation of this policy to use the ALPR system or associated files or hot lists for personal use or knowledge.

4. Anyone who engages in the impermissible use of the ALPR system or associated files and/or hot list may be subject to the following:
 - a. Criminal prosecution in accordance to applicable laws.
 - b. Civil liability
 - c. Administrative sanctions, up to and including termination, pursuant to and consistent with the relevant collective bargaining agreement and department policies.
5. Visual Verification of license plate number- the officer should verify an ALPR response through the CJIS/NCIC telecommunications system (absent exigent circumstances) before taking enforcement action that is based solely on an ALPR alert. This can be done via the MDT, dispatch or records. Once an alert has been received, the operator should confirm that the observed license plate from the system matches the license plate of the observed vehicle. Because the ALPR alert may be related 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.
6. Only properly trained sworn officers and the department's IT liaison are allowed access to the ALPR system or to collect ALPR information.
7. Departmental computers, databases, cell phone applications or other electronic devices compatible with Flock Safety may be used for ALPR monitoring in accordance with this policy.
8. Any and all hot list, hot plate, BOLO's or suspect information entered into the ALPR system shall be approved by a supervisor.

A. Data Collection and Retention [41.3.9(3D)(3E)(3G)]

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

All ALPR data downloaded to the server should be stored for no longer than thirty (30) days and in accordance with the established records retention schedule. Thereafter, ALPR data should be purged unless it has become, or it is reasonable to believe it will become evidence in a criminal or civil action or is the subject to a discovery request or other lawful action to produce records. In those circumstances the applicable data should be downloaded from the server onto portable media and booked into evidence, maintained on the investigators computer or kept within the investigator's case file.

B. Accountability and Safeguards [41.3.9(3F)]

All data will be closely safeguarded and protected by both procedural and technological means. The Groton Police Department will observe the following safeguards regarding access to and stored data

1. All non-law enforcement requests for access to stored ALPR data shall be processed in accordance with applicable procedures.
2. All ALPR data downloaded to the workstation shall be accessible only through a login/password protected system (Flock) capable of documenting all access of information by name, date and time.
3. Persons approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relates to a specific criminal investigation or department related civil or administrative action.
4. ALPR data may be released to other authorized and verified law enforcement officials and agencies for legitimate law enforcement purposes.
5. Every ALPR browsing inquiry must be documented by either an associated Groton Police Department case number or a specific reason for the inquiry. (The word 'investigation' alone is not considered specific)

C. ALPR Data Detection Browsing Audits

It is the responsibility of the Deputy Chief 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 twelve (12) month period to verify proper use in accordance with the above authorized uses. The audit shall randomly select at least ten (10) detection browsing inquiries conducted by department employees during the preceding six (6) month period and determine if each inquiry meets the requirements established.

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.

D. Releasing ALPR Data

The ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law. The agency makes a written request for the ALPR data that includes:

Name of agency

Name and position of person requesting

Intended purpose for obtaining the information

The request is reviewed by a supervisor and approved prior to the request being fulfilled.

E. Training [41.3.9(3C)]

The Deputy Chief is responsible for and should ensure that members receive department approved training for those authorized to use or access the ALPR System.

Flock Questions and Answers for Select Board

1. Is this mass surveillance?

- a. The system is designed around vehicle evidence with limited retention, we have complete local control, and there are full audit trails so every search that is done is accountable, reviewable, and tied to a legitimate investigative use.
- b. LPR cameras read license plates and vehicle attributes, they do not read faces. People are not a searchable category.
- c. Flock does not have access to personally identifiable information. They can't see what is on our system due to its encryption.
- d. Vehicle based searches reduce reliance on subjective descriptions alone
- e. The Groton Police controls access. We have opted out of external sharing, therefore, no outside police departments, both local and federal, have any access. GPD owns the data outright and for any data, the outside agency has to request the information, as they would with any town owned camera.
- f. Audits are done regularly by the Deputy Chief of Police per policy. Only three officers have access to the system. Every search that officers do is logged and is reviewable through the audit.
- g. Data retention is very limited per our policy

2. Will residents' data be shared with federal agencies, or sold?

- a. The Groton Police controls access. We have opted out of external sharing, therefore, no outside police departments, both local and federal, have any access. GPD owns the data outright and for any data, the outside agency has to request the information, as they would with any town owned camera.
- b. Data is encrypted, so only the authorized officers with accounts can view it. Flock does not have access to the data, so they can't share it or sell it.

3. How is the system used?

- a. There are 2 types of cameras, LPRs and live cameras. LPRs are the searchable cameras, the live camera is like a traditional surveillance camera. The LPRs an officer can search by vehicle attributes or license plate. People are not captured by the LPR. The LPR is taking a picture of the front or back of the vehicle, depending on the direction of travel. The live cameras are video recordings of select intersections and officers must search this manually by date and time, not by vehicle attributes. I.E. if we know an accident occurred at an intersection, we have a date and time and can pull that up. We cannot search the live cameras any other way, and people are not searchable in any way.
- b. All comparisons of license plates/vehicle attributes are done by an actual user, not the system. The system takes pictures, the pictures are searchable, and it is

up to the officer to confirm the accuracy of the picture per policy, and best practices in criminal investigations.

4. Who is reviewing how the system is used?
 - a. We only have three officers who have access to the system.
 - b. The system is audited regularly per policy by the Deputy Chief of Police.
 - c. Searches are tied to the individual users, have a time stamp, information searched and the case it is tied to.
 - d. Searches are done following MA CJIS regulations. Officers must have a valid criminal justice reason to conduct a search.
5. What about ICE and the Shield Law?
 - a. We do not share nationwide or federally. We share with two agencies outside of Groton, MA State Police and NESPIN – they are the regional crime intelligence clearing center. We regularly use them to help us solve cases
 - b. Immigration detainers and civil warrants do not constitute a need to share our data with those federal agencies per Massachusetts Law.
 - c. Per our policy, and MA law, there are search filters in place that automatically flag and block officers from searching vehicles that would violate the shield law.
6. Is Flock data secure?
 - a. Flock cameras have no public IP, therefore, are not addressable remotely to access footage.
 - b. All data collection points are equipped with secure communication protocols to protect data in transit from interception and tampering.
 - c. All data is encrypted using industry-standard algorithms (AWS Key Management Service or KMS) before being transmitted to our servers.
 - d. CJIS data is stored in the AWS GovCloud.
 - e. Flock is CJIS certified as well as NDAA, SOC2 (Type II), SOC3, ISO 27001, Higher Education Community Vendor Assessment Tool (HECVAT), HIPAA, and FERPA complaint. They are also aligned with security protocols established by NIST Cybersecurity as well as Cloud Security Alliance's CAIQ framework.