



# Alexandria Police Department

## Directive 10.40



### LICENSE PLATE READER PROGRAM

Effective Date: 06-12-2024

Cancels: 7-30-2020

Updated Date:

Section(s):

SME Review Date:

Updated Date:

Section(s):

2028

Updated Date:

Section(s):

### CONTENTS

10.40.01	PURPOSE AND POLICY
10.40.02	DEFINITIONS
10.40.03	RESPONSIBILITIES
10.40.04	DATA ACCESS AND RETENTION
10.40.05	LPR MAINTENANCE
10.40.06	COMMUNITY OUTREACH AND ENGAGEMENT

#### 10.40.01 PURPOSE AND POLICY

The purpose of this directive is to establish guidelines for the deployment and usage of License Plate Readers (LPRs) and their associated technology by sworn law enforcement personnel.

It is the policy of this department to develop and provide the most effective, efficient and reliable technology for all members of the department. LPRs will be employed to improve the effectiveness and efficiency of locating vehicles and individuals involved in criminal activities, as well as aiding in locating missing adults and children.

LPR systems may take various forms, including stationary devices positioned at fixed locations and mobile devices affixed to law enforcement vehicles and mobile trailers.

#### 10.40.02 DEFINITIONS

**Alarm (aka Hit)** – A positive indication, by visual and/or audible signal, of a potential match between data on the hot list and a license plate scanned by the LPR system. A hit is not conclusive confirmation that a license plate is wanted, and additional investigation is always warranted when a hit is indicated.

**Electronic File Management System (EFMS):** A system consisting of recording devices (ICC, BWC, LPR, etc.) and a cloud-based storage system which houses digital evidence captured by these systems, as well as digital evidence gathered by sources outside the system. For the purposes of this directive, this solely refers to Evidence.com as our current EFMS.

**Hot List** – A database populated with items of specific concern to the investigative and/or enforcement interests of law enforcement in the City of Alexandria. This may include, but is not limited to, Terrorist Screening Center watch list, stolen/wanted vehicles and license plates, wanted and missing persons, cautions, and license plates associated with Amber Alerts or various watch lists provided for law enforcement purposes.

**License Plate Recognition (LPR) system** – Equipment consisting of one or more camera(s), computer, and computer software used to automatically recognize and interpret the characters on vehicle license plates. This data is then compared against a list of license plates bearing some significance to law enforcement.

**LPR Administrator:** Support team within the Technology Support Division (TSD) charged with administration, troubleshooting, training, repairing, and coordinating all aspects of the LPR systems for the Police Department. TSD will maintain a list of trained operators.

**LPR-Generated Data** – All information, including location, date and time of a license plate encounter, the OCR interpolated data, and any LPR-generated digital photographic image(s) of the license plate and vehicle generated entirely through the use of and by the LPR equipment.

**LPR Operator:** A properly trained user of the LPR systems.

### **10.40.03 RESPONSIBILITIES**

#### **A. LPR Operators:**

1. LPR operators shall undergo training provided by the LPR Administrator or designated trainers before operating LPR devices or accessing LPR systems. Training shall include guidelines on lawful usage, data handling, and legal considerations.
2. Operators shall prioritize safety when using LPR systems in vehicles, adhering to all relevant traffic laws and regulations. Operators must refrain from engaging in any activity that could compromise their focus on safe driving.
3. Officers assigned to patrol duties are required to activate and login to their LPR systems at the start of their shifts and maintaining system activation throughout their assigned shifts. All other sworn employees with access to LPR systems are strongly encouraged to keep the system continuously activated as well to maximize the opportunity for scanning vehicles on the hotlist.

4. Upon receiving an LPR alert, operators shall exert reasonable efforts to locate the vehicle and undertake necessary law enforcement actions when they are available and positioned to intercept the vehicle.
5. When a vehicle is located following an alarm, LPR operators must first confirm the accuracy and nature of the alarm. This includes visually matching the alarm with the vehicle's license plate and checking VCIN/NCIC to ensure the circumstance for the alarm is still active.
6. It is important to understand that while an alarm can generate reasonable suspicion, achieving probable cause requires separate and independent validation.
7. When querying the LPR database, the LPR operator shall document the law enforcement purpose in sufficient detail within the database, to include entering an incident/case number when one is available. This record-keeping is essential for establishing a transparent and comprehensive audit trail of all database queries.
8. Whenever an LPR system assists in a law enforcement investigation requiring a police report, operators must document this information within the report. They are also accountable for transferring relevant LPR evidence files from the LPR database to the EFMS. This transfer must occur before the automatic database purge, which typically happens within 30 days of the evidence being captured. Documentation of the evidence storage location should be part of the Officer's police report narrative.

**B. The LPR Administrators:**

1. The LPR Administrator is responsible for the administrative oversight, troubleshooting, training coordination, maintenance, and repair of all LPR systems within the department.
2. The LPR Administrator shall maintain a list of trained LPR operators and organize regular training sessions.
3. The LPR Administrator will oversee the installation and maintenance of LPR software and hardware.
4. The LPR Administrator will ensure that all LPR software is up-to-date and functioning optimally.

**C. Supervisors and Commanders:**

1. All supervisors, irrespective of their training in the LPR system, are accountable for ensuring that the LPR system is utilized by their subordinate officers in a manner consistent with this policy and all applicable laws. Any deviations from these guidelines shall be promptly addressed.

2. Patrol supervisors are tasked with ensuring that both themselves and their subordinate officers receive training and access to LPR systems. These supervisors shall collaborate with the LPR Administrator to facilitate officer enrollment in LPR training at the earliest available opportunity.
3. Patrol supervisors are responsible for ensuring that officers activate their LPR systems at the start of their shifts, and the systems remain active throughout the entirety of the shift.
4. Patrol supervisors must ensure that officers who receive an LPR alert and are available and in a position to intercept the vehicle make reasonable efforts to intercept it and take necessary law enforcement action.

#### **10.40.04 DATA ACCESS AND RETENTION**

##### **A. LPR Data Storage:**

1. LPR equipment may collect and store LPR-generated data during the license plate detection and identification phase of use.
2. The LPR databases will be configured to adhere to legal regulations regarding data retention.
3. LPR data will be transmitted to a centralized database and retained for a duration aligning with state law, legal precedent, and vendor policies. An automatic deletion process will follow this period. Legal precedent allows LPR data storage for up to 364 days, but APD often chooses a shorter retention period due to storage limitations. Operators must stay updated on the current retention schedule for various LPR systems through training. They ensure prompt retention of relevant data within the EFMS upon learning its significance to an investigation. Operators should remain mindful that many LPR files are purged after 30 days.
4. Operators are responsible for transferring LPR database files to the EFMS when the data pertains to an ongoing law enforcement investigation and before the automatic purge of the database.

##### **B. Data Access:**

1. Access to the database shall be limited to trained law enforcement officers with specific needs related to a criminal investigation. Additionally, professional staff employees assigned to the Crime Analysis Section shall have similar access privileges for the purpose of supporting criminal investigations.

2. The LPR database used for law enforcement purposes will be maintained separately from any other databases used for non-law enforcement purposes (e.g., parking enforcement).

### **C. Data Security:**

1. The supervisor of the Tactical Computers Unit is responsible for completing a weekly system audit of the Flock Safety database. In the event that a weekly audit cannot be completed due to leave or extenuating circumstances, an extension may be granted, provided that the query is completed at the first available opportunity.
2. Utilizing the provided auditing feature, the supervisor must review system queries to ensure that APD employees are using the system for legitimate law enforcement purposes, in accordance with their training, and following the relevant departmental directives.
3. Discrepancies discovered during the weekly audit must be addressed promptly. For discrepancies related to training issues, such as insufficient documentation of query reasons, the supervisor should handle these directly with the officer involved, which may include providing additional training. If the same discrepancy occurs repeatedly, it should be addressed with the employee's supervisor. Any discrepancies related to unlawful, inappropriate, or egregious misuse must be immediately reported to the Commander of the Technology Services Division and/or the Commander of the Office of Professional Responsibility for further guidance.
4. All weekly audits, along with documentation of discovered discrepancies and actions taken, must be documented on the designated audit log form and sent to the Commander of the Technology Services Division for final review. The Commander of the Technology Services Division will be responsible for maintaining these audits for a period of three years, unless they become part of a formal Unit Level Inquiry or Internal Investigation, in which case they should be retained in accordance with the related policies.

### **D. Data Sharing:**

1. LPR data may be shared with other law enforcement agencies to assist with accomplishing law enforcement objectives. APD officers and crime analysts can access LPR databases of other law enforcement agencies when access is available and necessary to achieve a law enforcement objective.
2. APD reserves the right to terminate or suspend any data-sharing agreement with an external agency.

**10.40.05 LPR MAINTENANCE**

1. LPR operators shall not make any modifications to the LPR equipment or software operating system without explicit direction from the LPR Administrator.
2. LPR camera lenses may be cleaned using a soft, non-abrasive cloth.
3. Damage to LPR equipment should be promptly reported to a supervisor, and a documented report will be forwarded to the LPR Administrator for necessary action.
4. The LPR Administrator shall be notified of any LPR equipment requiring maintenance or repair, and appropriate measures shall be taken to ensure timely maintenance and repairs.

**10.40.06 COMMUNITY OUTREACH AND ENGAGEMENT**

The Alexandria Police Department recognizes the importance of transparency and open communication with the community regarding the utilization of LPR technology. The Alexandria Police Department is committed to ensuring that the public is well-informed about the purpose, benefits, and privacy protections associated with LPR usage. This section outlines our efforts to engage with the community:

**A. Community Education and Awareness:**

1. The Alexandria Police Department shall proactively engage in community education and awareness initiatives to inform the public about the role and benefits of LPR technology in enhancing public safety and assisting law enforcement agencies.
2. The Alexandria Police Department shall provide easily accessible information to explain how LPR systems function, their potential impact on crime prevention, and the safeguards in place to protect the privacy of individuals.
3. The Alexandria Police Department shall make its LPR policy publicly accessible. This accessibility ensures that the public can review and understand the guidelines governing LPR usage within the department.

**BY AUTHORITY OF:**

**Raul Pedroso**  
Chief of Police, Interim