

	STANDARD OPERATING PROCEDURE	Reference Number MCSO-092
	Subject License Plate Readers	
	Special Instructions Replaces version effective November 18, 2024	Effective Date June 7, 2025

I. PURPOSE

Establish operational procedures for the use of the license plate reader (LPR) system and the retention of data. The intended use of the LPR system is to increase public safety, minimize the threat and risk of injury to individuals, to enhance the criminal investigatory process, and make the most effective use of public resources allocated to public safety agencies.

II. POLICY

It is the policy of the Monroe County Sheriff's Office (MCSO) to utilize LPR technology only for official and legitimate law enforcement purposes, with the goal being to increase the efficiency and effectiveness of its public safety efforts in a manner that safeguards the legitimate privacy concerns of law-abiding citizens. All data and images gathered by the LPR are for the official use of MCSO. Because such data may contain confidential information, it is not open to public review.

III. DEFINITIONS

- A. AGENCY – A law enforcement agency with access to the LPR system.
- B. LICENSE PLATE READER (LPR) – A device that uses cameras and technology to compare digital images of license plates against databases.
- C. HIT – An alert from the LPR system that a scanned license plate number may be in the National Crime Information Center (NCIC) or another law enforcement database for a reason including, but not limited to, being related to a stolen vehicle, wanted person, missing person, violent crime, or terrorist-related activity.
- D. HOT LIST – A list of license plates associated with vehicles of interest compiled from one or more databases, including, but not limited to, NCIC and other agency-maintained lists.
- E. VEHICLES OF INTEREST – Vehicles, including but not limited to those which are reported as: stolen; displaying stolen license plates or tags; linked to missing and/or wanted person; linked to violent crimes and/or flagged by law enforcement officers or agencies for an official law enforcement purpose.

IV. **PROCEDURE**

A. It is a violation of this policy to use the LPR system, associated scanned files or Hot Lists for the purpose of infringing upon First Amendment Rights, including information related to individuals or organizations based solely on their religious, political, social views or activities; their participation in a particular noncriminal organization or lawful event; or their race, ethnicity, citizenship, age, disability, gender, sexual orientation, or other classification protected by law.

B. Personnel shall not use the LPR system in violation of federal or state laws.

C. Only properly trained personnel are allowed access to the LPR system or to collect LPR information. No member of this agency shall operate LPR equipment or access LPR data without first completing department-approved training.

D. To ensure proper operation and facilitate oversight of the LPR system, all users will be required to have individual credentials for access and use of the systems and/or data, which can be fully audited.

E. Personnel shall not use or allow others to use the equipment or database records for any unauthorized purpose.

F. Personnel shall not share their username and password.

G. The Lieutenant Colonel of Operations shall monitor to ensure the security of the information and compliance with applicable privacy laws.

H. The LPR system database and capture information are to be used for official law enforcement purposes only. Personnel shall only access the database for investigative/administrative purposes only and treat all data as confidential.

I. LPR may be used in conjunction with any routine patrol operation or criminal investigation; reasonable suspicion or probable cause is not required before using an LPR.

J. All patrol deputies shall be responsible for monitoring LPR cameras while on duty. Upon receipt of an LPR notification, they will respond to the area of the capture and look for the suspect vehicle.

K. Prior to the initiation of a stop of a vehicle or other intervention based on a hit, deputies shall undertake the following:

1. Deputies shall visually verify that the license plate of interest matches identically with the image of the license plate number captured by the LPR.

2. If the source of the hit is an NCIC hotlist, deputies must confirm that the license plate is still listed in NCIC as stolen, wanted, or otherwise of interest before proceeding.

3. If the source of the hit is an agency-created hotlist, deputies must make a reasonable effort to confirm that a reasonable basis exists to stop the vehicle.

L. Deputies may utilize LPR data to assist in the identification of suspects involved in criminal activity.

M. Deputies may be granted search access to the LPR system by the Lieutenant Colonel of Operations.

N. All searches of the LPR system must include either a MCSO event number associated with the inquiry or a clearly documented reason for why the information is needed.

O. Only supervisory or investigatory personnel may create hot lists. All hot lists shall comply with the following:

1. May be utilized for any legitimate official law enforcement purpose.

2. It is the responsibility of the entering person to determine when the information is no longer necessary and ensure the entry or hot list is removed.

3. The entering person shall remove the entry or hot list immediately upon confirmation that it has been entered into NCIC.

4. Additionally, any deputy who becomes aware that an entry or hot list is no longer necessary shall notify the entering person that the entry or hot list should be removed. If the entering person is unavailable, any deputy that is aware that an entry or hot list is no longer necessary shall notify a supervisor immediately that the entry or hot list should be removed.

5. The entering person shall initially set an expiration date for seven (7) days or less. Entries must be reviewed at a minimum of every seven (7) days at which time the expiration date may be extended another seven (7) days or less.

P. All data will be closely safeguarded and protected by both procedural and technological means. MCSO will observe the following safeguards regarding access to and use of stored data:

1. All LPR data downloaded to the mobile workstation and in storage shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time.

2. Personnel granted access to LPR 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.

3. LPR system audits should be conducted on a regular basis by the Lieutenant Colonel of Operations or designee.

Q. LPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes.

R. When deputies utilize LPR data to assist in identification of a suspect or vehicle linked to criminal activity, the LPR data shall be downloaded from the system and attached to the investigative report as evidence.

S. All other LPR data shall be retained for thirty (30) days before being purged from the system.

T. This procedure is to be used in conjunction with all relevant Department regulations, rules, policies, and procedures.