NELSON COUNTY SHERIFF'S OFFICE
An equal opportunity employer
P.O. BOX 36, 84 COURTHOUSE SQUARE, LOVINGSTON, VIRGINIA 22949 ~ BUSINESS 434.263.7050 ~FAX 434.263.7056

SHERIFF
M.E. EMBREY

GENERAL ORDER NO. 3-44 **LICENSE PLATE READERS**
Effective: 05/21/2025 **Revised: 05/21/2025**
VLEPSC Standards: OPR.03.03

POLICY

It is the policy of the Nelson County Sheriff's Office to utilize License Plate Readers (LPR) technology to capture and store digital license plate data and images only for legitimate law enforcement purposes while ensuring that the privacy, civil rights, and civil liberties of individuals are not violated.

This policy applies to LPR information collected or received, accessed, used, disseminated, retained, and purged by the Nelson County Sheriff's Office. It is not intended to apply, nor does it apply, to any other types of information accessed, retained, or used by the Nelson County Sheriff's Office.

All data and images gathered by the LPRs are for the official use of the Nelson County Sheriff's Office. Because such data may contain private and/or confidential information, it is not open to public review unless required by law.

PURPOSE

The purpose of this General Order is to provide sworn personnel of the Nelson County Sheriff's Office with guidance for the capture, storage, and use of digital data obtained through the use of LPR technology.

PROCEDURES

A. General

1. Information gathered or collected, and records retained by the Office's LPR Program or system will not be accessed or used for any purpose other than legitimate law enforcement or public safety purposes.

2. The Office and other law enforcement agencies authorized to collect LPR information must use the least intrusive collection and investigative techniques possible while still obtaining the necessary LPR data.

3. The Office protects all LPR information as Personally Identifiable Information (PII) because LPR information may be combined with other information to specify a unique individual (i.e., the identity of an individual could be directly or indirectly inferred by using information that is linked or linkable to that individual).

4. All deployments of the LPR system are for official use only (FOUO). All information captured, stored, generated, or otherwise produced by an LPR system is the property of the Nelson County Sheriff's Office regardless of where the information is housed or stored.

5. Any data extracted from the LPR server to be retained as evidence shall be thoroughly documented in an appropriate report within the Office's records management system.

B. Management and Administration

1. The LPR Coordinator is responsible for the management and administration of the Sheriff's Office's LPR program.

2. The Sheriff will designate an LPR Coordinator who will be directly responsible for the oversight and administration of the Sheriff's Office's LPR program.

3. Operators encountering problems with LPR equipment or programs are responsible for notifying the LPR Coordinator.

C. LPR Coordinator

1. The LPR Coordinator, or their authorized designee, will administer the day-to-day operation of the Sheriff's Office's LPR equipment and its associated data and ensure that the Sheriff's Office's policies and procedures related to the devices conform to current laws, regulations, and best practices. The LPR Coordinator will also have the following additional duties and responsibilities:

   a. Liaising with and being the Sheriff's Office's primary point-of-contact with the LPR provider.

   b. Establishing protocols for access, collection, storage, and retention of LPR data and associated LPR media files.

   c. Establishing protocols to ensure the security and integrity of data captured, stored, and/or retained by the LPR system.

   d. Identifying locations across the county for the placement of LPR cameras so as to ensure that their deployment does not disproportionately target any group or segment of the community.

   e. Coordinating the proper and efficient installation, maintenance, and deployment of the Sheriff's Office's LPRs.

   f. Ensuring that stored LPR information is automatically purged from the LPR database within established timeframes, unless determined to be of evidentiary value.

   g. Acting as the authorizing official for individual access to and data retention of the LPR information.

   h. Ensure that all members with authorized access to LPR information receive the appropriate initial and any required refresher/recurrent training.

   i. Updating authorized users of any technological, legal, or other changes that affect the use of LPR system.

j. Ensuring that inspections and maintenance of the Sheriff's Office's LPRs are completed to ensure their continued operational readiness.

k. Ensuring that any of the Sheriff's Office's LPRs or its associated equipment that is damaged or not functioning properly is taken out of service, and promptly repaired and/or replaced.

l. Investigate any alleged misuse or inappropriate application of LPR operations, information, data, or software in accordance with applicable laws and Sheriff's Office policy.

2. Requests for LPR data by members of outside agencies shall be directed to the LPR Coordinator who will take into consideration the exigency and totality of each request.

D. Guidelines for Use of the LPR System

1. **An LPR alert does not create reasonable suspicion to justify a traffic stop or the detention of an individual. The deputy must develop independent reasonable suspicion for the stop.** The following are guidelines only, but should assist a deputy in determining when reasonable suspicion exists concerning various types of LPR alerts:

   a. Stolen Vehicles and Stolen License Plates – Requires confirmation.

   b. Wanted Persons – Must have a reasonable belief the person sought is in the vehicle and the warrant or pick-up is valid.

   c. BOLO Only – This alert is information only for deputies, and reasonable suspicion may or may not exist based on the alert alone. The narrative of the alert will assist deputies in determining the level of reasonable suspicion. Independent reasonable suspicions may or may not be required in order to detain.

   d. Officer Safety, Suspected Gang Member, Sexual Offender, Past Offender, Associate Only, and Information Only – These alerts are information only for deputies; reasonable suspicion should be obtained in order to detain.

2. Before initiating any enforcement action, the deputy shall:

   a. Make a visual confirmation that the license plate actually matches the information captured by the LPR and reported in the corresponding alert.

   b. Confirm the license plate information with NCIC/VCIN.

   c. Ensure the hit conforms to the parameters set forth in this directive.

3. Proactive/manual entry into an LPR Hot List in the field is permitted in the following circumstances, however no PII will be entered, uploaded, and/or transmitted:

   a. Dispatch reports of crimes, BOLOs, alerts in which a license plate number is part of the broadcast.

   b. A deputy queries the LPR system to ascertain if there is a prior read of the license plate which is the subject of the particular alert, bulletin, or alarm.

c. An authorized user may request certain license plate characters, complete or partial, to be entered into the Hotlist. Examples of entries include: gang members/associates, sex offenders, crime suspects, fugitives, search warrant targets.

d. In order to enter a license plate into the Hotlist, there should be reasonable suspicion to believe the vehicle is directly associated with:

(1) The person sought (owner, regular driver, or regular passenger); or

(2) Criminal activity.

e. The alert should immediately be removed when the alert is no longer valid.

4. Proactive/manual entry into an LPR Hot List in the field is required for AMBER or Missing Child Alerts. Additionally, deputies must query their LPR to ascertain if there is a prior read of the license plate which is the subject of the alert.

5. Deputies must log alert results in the IBR report and note the use of "FLOCK" in the circumstances drop down option.

E. Security and Accountability Safeguards

1. All LPR data will be closely safeguarded and protected by both procedural and technological means against network intrusions. The Nelson County Sheriff's Office will observe the following security and accountability safeguards regarding access to and use of stored data:

a. 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.

b. Each authorized user will have a unique log-in identification and password to access the LPR database and its associated data. Usernames and passwords to LPR information are not transferrable, must not be shared, and must be kept confidential.

c. Personnel approved to access LPR 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. All user access and queries are subject to review and audit.

d. Access to LPR information will be granted only to members whose positions and job duties require such access and who have successfully completed the required training.

2. If any member reasonably believes that another law enforcement agency has used or is using the Sheriff's Office's LPR systems or data in a manner that violates this General Order, the member shall promptly report that information to the LPR Coordinator who shall then investigate the allegation and determine if sharing LPR data with the outside agency will continue.

3. When a deputy takes any action due to an LPR alert/hit, but it is later discovered that they acted on the wrong vehicle due to an error in data entry, fictitious, or swapped license plates, or a

misinterpretation of the license plate, the deputy shall email the incident details to their Supervisor and the LPR Coordinator before the end of their shift.

F. Audits

1. LPR audit logs will be maintained and stored indefinitely. All access to the system will be logged. FLOCK will maintain an audit trail of requested and accessed information, including the purpose of the query. Periodic, random audits will be conducted by the LPR Coordinator to ensure and evaluate compliance with system requirements and with the provisions of this general order and applicable law.

G. LPR Information Retention and Purging

1. Data will be stored for 21 days except in the following circumstances:

   a. Records associated with an ongoing criminal or administrative investigation will be maintained until a final disposition has been reached in the particular case.

   b. Alerts associated with an arrest will be maintained in the criminal case file and retained for the maximum period of time associated with such record.

   c. Alerts associated with felony investigations will be maintained in the criminal case file and retained for the maximum period associated with such record.

   d. Whenever directed by the LPR Coordinator.

H. Training

1. Any authorized person using the LPR system shall complete initial training on the policies and restrictions regarding LPR use, data handling, and processing requests for LPR data.