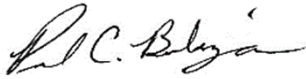


|                                                                                                                      |                               |                                         |
|----------------------------------------------------------------------------------------------------------------------|-------------------------------|-----------------------------------------|
| SUBJECT<br><b>License Plate Reader (LPR)</b>                                                                         |                               | GENERAL ORDER<br>NUMBER<br><b>1.6.1</b> |
| DCJS STANDARDS                                                                                                       |                               | EFFECTIVE DATE<br>September 4, 2025     |
| REVIEWED DATE<br>July 14, 2026                                                                                       | APPLIES TO<br>Sworn Personnel | REVISION DATE<br>August 6, 2026         |
| APPROVAL<br><br>Paul C. Burlingame  |                               |                                         |

## 1. Purpose

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

## 2. Policy

It is the policy of this department to utilize License Plate Reader 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 LPR are for official use by this department. Such data may contain confidential information and therefore is not available for public review.

## 3. Definitions

- a. License Plate Reader (LPR) – Technology that uses optical character recognition to automatically read license plate characters
- b. Hotlist – Data provided that includes license plate numbers of stolen vehicles, stolen license plates, wanted person(s) with a license plate associated with those records, and suspended or revoked registrations. This term also includes national data (i.e. NCIC) for similar categories, license plates associated with AMBER Alerts or Missing Person/Vulnerable Adult Alerts, and includes manually enters license plate information associated with crimes that have occurred in any local jurisdiction or other investigative targets.

## 4. Procedures

- a. Permissible use of LPR technology
  - i. The use of LPR technology and associated equipment and databases by law enforcement are authorized only for official public safety purposes.

- ii. Department members are only authorized to utilize LPR technology to:
  - 1. Attempt to identify and/or locate a vehicle related to an investigation; or
  - 2. Attempt to identify vehicle owner(s) and/or occupant(s) when such individual(s):
    - a. Has committed a criminal offense; or
    - b. Is involved in, or planning, criminal conduct or activity; or
    - c. Is a possible missing or vulnerable person, crime victim, or witness to criminal activity
    - d. Is a possible danger to themselves or others due to mental illness
  - 3. Prevent, detect and/or assess potential safety threats to members of the public and/or public officials.
  - 4. Regulate public parking areas and manage the flow of traffic.
  - 5. Monitor access to secured areas.
- iii. Each inquiry into LPR data must contain an appropriate investigative case number along with the reason for the inquiry. Each UPD case file should also contain a corresponding entry listing that LPR data was obtained, and the finding shall be outlined.

b. Prohibited Use

- i. The use of LPR technology is restricted to approved and legitimate law enforcement purposes and public safety related missions as outlined in this policy.
- ii. Use of LPR technology for personal or other non-official purposes is a violation of this policy.
- iii. LPR technology shall not be used for investigatory purposes:
  - 1. When the purpose is based solely upon religious, political, or social views while individual(s) participate in a non-criminal organization or lawful event.
  - 2. When the inquiry would otherwise violate an individual(s) constitutional rights.

c. Use of Hotlists

- i. Officers using LPR technology should ensure the most current Hotlist data is available and uploaded into the system.
- ii. When the LPR generates a hit from the Hotlist, the department member shall verify that the captured image matches the license plate and state of registration prior to initiating any action.

- iii. If a match is confirmed, the member will notify the shift supervisor of said Hotlist alert and the shift supervisor will determine the appropriate patrol response.

d. Data Security and Access

- i. The use of LPR data is restricted to law enforcement and public safety related missions of the department.
- ii. LPR systems, associated equipment, and databases are property of the department and are authorized for official public safety purposes only.
- iii. Data held by the LPR system shall be treated the same as eJustice Portal and NCIC information and only accessed by those authorized to view those systems.
  - 1. Unauthorized or misuse of this equipment and associated data may be subject to disciplinary action.

iv. Data Retention

- 1. Data obtained through the use of the LPR system will not be retained any longer than state minimum requirements.

v. Releasing of data

- 1. LPR data may not be released without the authorization of the Chief of Police, or their designee.
- 2. LPR data may only be shared with other law enforcement or prosecutorial agencies for official law enforcement purposes and is subject to the requirements outlined in NYS Executive Order 170 and 170.1.
- 3. The sharing of data with any external law enforcement agencies must be outlined in a Memorandum of Understanding between that agency and the New York State University Police at Albany, and the that agency's use and storage of that data must align with this General Order. The following agencies have a data sharing Memorandum of Understanding with this department:

- i. Capital Region Crime Analysis Center

e. Training

- i. All authorized personnel with authorized access to LPR technology shall receive training on the technology prior to use, which includes:
  - 1. How to properly use LPR technology and associated equipment.

2. Knowledge and understanding of the department's LPR policy and procedures.
  3. Applicable laws and privacy protections that pertain to this technology.
- f. Audit
- i. The Deputy Chief of Investigations shall conduct monthly audits of access and use of the LPR data system to ensure compliance with this policy. These audits shall be recorded and subject to review by the Chief of Police.
  - ii. Any audit that reveals possible misuse of the system or violation of the policy shall immediately be referred to the Chief of Police who shall ensure the matter is investigated as potential misconduct.