

A. PURPOSE. To establish procedures and guidelines for the proper use of license plate recognition (LPR) systems, and the collection, maintenance, and archiving of related data.

1. Ensure LPR system use respects individuals' constitutional and statutory rights.
2. Provide government accountability.
3. Deter criminal behavior and, when appropriate, assist in criminal investigations and prosecutions.
4. Allow for appropriate cooperation with business entities or groups seeking safety and security for specifically identified property.

B. GOALS. License Plate Recognition systems seek to enhance the department's efficiency and effectiveness, and to enhance community and officer safety with the deployment and use of LPR systems.

C. DEFINITIONS

1. *LPR*. License Plate Recognition/License Plate Reader.
2. *Alert*. A visual and/or auditory notice that is triggered when the LPR system receives a potential "hit" on a license plate.
3. *Fixed LPR System*. LPR cameras which are affixed to a structure, such as a pole, traffic barrier, or bridge.
4. *Hit*. A read matched to a plate that has previously been registered on an agency's "hot list" of vehicle plates related to stolen vehicles, wanted vehicles, or other factors supporting investigation, or which has been manually registered by a user for further investigation.
5. *Hotlist*. License plate numbers of stolen cars, vehicles owned by persons of interest, and vehicles associated with AMBER Alerts that are regularly added to "hot lists" circulated among law enforcement agencies. Hot list information can come from a variety of sources, including stolen vehicle information from the National Insurance Crime Bureau (NICB) and the National Crime Information Center (NCIC), as well as national AMBER Alerts and Department of Homeland Security watch lists. Departments of motor vehicles can provide lists of expired registration tags, and law enforcement agencies can interface their own, locally compiled hot lists to the LPR system. These lists serve an officer

safety function as well as an investigatory purpose. In addition to agency supported hot lists, users may also manually add license plate numbers to hot lists in order to be alerted if and when a vehicle license plate of interest is “read” by the LPR system.

6. *Read.* Digital images of license plates and vehicles and associated metadata (e.g., date, time, and geographic coordinates associated with the vehicle image capture) that are captured by the LPR systems.

#### D. AUTHORIZED USES

1. LPR systems, LPR data, and associated media are the property of this agency and are to be used only in conducting the agency’s official business.
2. Only trained officers and civilians authorized by an Administrator may access LPR systems. LPR data and associated media and all their access must comply with this policy.
3. The use of LPR systems is restricted to public safety-related missions of this agency.
4. Except when done pursuant to a court order, the LPR may be used only to record license plates of vehicles that are exposed to public view (e.g., vehicle on a public road or street, or that are on private property but whose license plate(s) are visible from a public road, street, or a place to which members of the public have access, such as the parking lot of a shop or other business establishment).

#### E. PROHIBITED USES

1. Except when done pursuant to a court order, recording license plates that are not exposed to public view.
2. Use of the LPR system to harass and/or intimidate any individual or group.
3. Use of the LPR system or associated scan file or hot lists solely because of a person’s or group’s race, gender, religion, political affiliation, nationality, ethnicity, sexual orientation, disability, or other classification protected by law.
4. Use of the LPR system or associated scan files or hot lists for any personal purpose.

5. Use of the LPR system or associated scan files or hot lists for the purpose of identifying any individual or group engaged in the exercise of First Amendment rights unless used only for the protection of those persons.

#### F. LICENSE PLATE RECOGNITION (LPR) SYSTEMS USAGE

1. LPR system is a passive system; live data is not viewed.
2. LPR systems shall monitor all license plates that come in the LPR camera's view. Information for legitimate public safety purposes will be accessed by trained sworn and civilian employees of this department as appropriate.
3. LPR system searches of historical data shall only be conducted by trained sworn and civilian employees of this department and can only be done for legitimate public safety related purposes.
4. All searches of the LPR system shall include a reason for the search to include the case/CAD number and type of incident (e.g., 24-XXXXXX Robbery). Searches related to broadcasts by dispatch that do not have a case/CAD number, such as suspected OWI drivers or vehicles wanted by other jurisdictions will include "Broadcast" and the reason (e.g., Broadcast – WYPD Robbery Suspect Vehicle).
5. LPR systems may have the ability to notify the system administrator and/or other police personnel of a "hit" from the LPR system "hot list."

#### G. OPERATIONS and ENFORCEMENT ACTIONS

1. All users of the LPR system will unselect "Immigration Violator" under the NCIC notification reasons and will not take any enforcement action if the LPR system alerts solely on an immigration violation.
2. Hot lists that alert the entire organization may only be created by a supervisor or the department's designated crime analyst(s). Individual officers may create their own hot lists that only alert that officer of vehicles that are of interest in a criminal investigation.
3. When notified of a "hit" from the LPR system, officers shall verify the LPR response through the Law Enforcement Information Network (LEIN) and the National Crime Information Center (NCIC) before taking enforcement action that is based solely on an LPR alert.

4. Once an alert is received, the operator shall confirm that the observed license plate from the LPR system matches the license plate of the observed vehicle.
5. Because the LPR alert relates to a vehicle plate and may not related to the person operating the vehicle, officers need reasonable suspicion and/or probable cause to make an enforcement stop of any vehicle (e.g., if a vehicle is entered into the system because of its association with a wanted individual, officers shall attempt to visually match the driver to the description of the wanted subject prior to making a stop or should have another legal basis for making the stop).
6. Occasionally there may be errors in the LPR system's read of a license plate, therefore an alert alone is not a basis for police action.
7. Hot lists shall be obtained or compiled from sources as may be consistent with the purposes of the LPR system set forth in this policy.
8. Prior to initiation of a stop of a vehicle or other intervention based on an alert, officers shall undertake the following:
  - a. Verification of a status on a hot list. An officer must receive confirmation, either from dispatch, MDT, or other department computer device, that the license plate is still stolen, wanted, or otherwise of interest before proceeding (absent exigent circumstances).
  - b. Visual verification of license plate number. Officers shall visually verify that the license plate of interest matches identically with the image of the license plate number captured (read) by the LPR, including both the alphanumeric characters of the license plate, state of issue, and vehicle descriptors before proceeding. Officers alerted to the fact that an observed motor vehicle's license plate is entered as a hot plate (hit) in a specific BOLO/ATL list are required to make a reasonable effort to confirm that a wanted person is actually in the vehicle and/or that a reasonable basis exists before the officer would have a lawful basis to stop the vehicle.
9. All entries and updates of specific hot lists within the LPR system will be documented by the requesting officer within the appropriate offense report. As such, specific hot lists shall be approved by the LPR system administrator, or their designee, before initial entry within the LPR system. Updating of such a list within the LPR system shall thereafter

be accomplished pursuant to the approval of the officer's immediate supervisor. The hits from these data sources should be viewed as informational; created solely to bring the officer's attention to specific vehicles that have been associated with criminal activity.

10. All hot list plates and suspect information added into the LPR system will contain the following information as a minimum:

- a. Entering officer's name
- b. Related case number
- c. Short synopsis describing the nature of the originating call

11. Any time LPR data is used, whether from a hot list alert or from a system search, and a suspect and/or suspect vehicle is identified, the user will document the positive results in the appropriate offense report.

H. LPR DATA SHARING AND DISSEMINATION. LPR data should be considered "For Official Use Only" and can only be shared for legitimate law enforcement purposes.

1. Outside agencies without LPR capabilities can make requests to a system administrator or supervisor for specific queries of the LPR database for legitimate law enforcement purposes. Only matching returns will be shared with the agency.
  - a. The administrator or supervisor will enter the requesting agency's name, the agency's case number, and incident type in the reason for the search field.
2. Sworn law enforcement members of any multi-jurisdictional task force housed at the Grand Rapids Police Department (GRPD), whose law enforcement duties require them to assist in the investigation of crimes that occur in the City of Grand Rapids, are permitted to access the LPR database. Task force team members will:
  - a. Have individual credentials for accessing the LPR database.
  - b. Receive training on the proper use of the LPR system.
  - c. Abide by GRPD policies pertaining to the use of the LPR system.

3. Sharing of LPR data and information to third parties, non-law enforcement agencies, including private litigants is prohibited except to the degree required by law (FOIA).

#### I. RETENTION OF LPR RELATED PHOTOS AND DATA

1. LPR related data will be stored for a maximum of 30 days.
2. LPR data that is deemed evidence in a police related case will be transferred to and retained in the department's digital evidence storage system.

#### J. SPECIFIC RESPONSIBILITIES. LPR systems and associated equipment and databases are authorized for official public safety purposes and only in accordance with this policy. Any individual misusing this equipment and associated databases, or data, may be subject to:

1. Criminal prosecution
2. Civil liability, and/or
3. Administrative sanctions, up to and including termination, pursuant to and consistent with the relevant collective bargaining agreements and department policies.

#### K. ADMINISTRATION

1. The Chief of Police, or his/her designee, shall designate an employee(s) with administrative oversight (Administrator) for LPR system deployment and operations who is responsible for the following:
  - a. Establishing protocols for access. 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 has the ability to be fully audited.
  - b. Establishing protocols for the collection, storage, and retention of LPR data and associated media files.
  - c. Establishing protocols to preserve and document LPR reads and "alerts" or "hits" that are acted on in the field or associated with investigations or prosecutions.

- d. Establishing protocols to ensure the security and integrity of data captured, stored, and/or retained by the LPR system.
  - e. Maintaining records identifying approved LPR deployments and documenting their results, including appropriate documentation of significant incidents and arrests that are related to its usage.
  - f. Authorizing any request for LPR systems use or data access according to the policies and guidelines of this agency.
- 2. Designated personnel shall check equipment on a regular basis to ensure functionality and camera alignment. Any equipment that falls outside of expected functionality shall be reported immediately to the system administrator.
- 3. LPR system repairs, hardware, or software, shall be made by technicians through contact with a system administrator.