445.17 License Plate Recognition (LPR) System

The Technology Unit will administer and oversee the License Plate Recognition (LPR) program and is responsible for training department members to operate the LPR system, maintaining records, identifying approved LPR details and their results, maintaining the LPR data query log, documenting training, and ensuring appropriate documentation of significant incidents and arrests that are related to LPR usage.

Deployment of LPR equipment is intended to provide access to stolen and wanted files and for the furtherance of criminal investigations. Use is restricted to these purposes. The proactive entry of any data, except as stipulated in this directive, or the access to LPR records, must be approved by the Technology Unit Commander, and must have a specific criminal investigative or patrol purpose. No officer may use, or authorize the use of, the equipment or database records for any other reason.

Training:

Officers are prohibited from using the LPR system until they have been properly trained in its use by Technology Unit personnel and have been instructed as to operational protocols.

LPR Operations:

SPPD may deploy both mobile and fixed-position Automated License Plate Reader (ALPR/LPR) systems at strategically selected locations within the City of Saint Paul consistent with Minn. Stat. § 13.824.

LPR systems may be installed at major ingress/egress corridors, high-crime areas supported by crime analysis, locations identified through intelligence-led policing strategies, and areas supporting critical infrastructure protection.

Deployment of LPR systems requires approval of the Chief of Police or designee. Locations shall be documented and maintained by the Technology Unit.

LPR systems shall be used solely for legitimate law enforcement purposes including detection of stolen vehicles or license plates, locating vehicles associated with missing persons, vehicles tied to active warrants, and active criminal investigations.

LPR systems shall not be used for general surveillance, monitoring First Amendment protected activity, or tracking individuals absent a warrant supported by probable cause or exigent circumstances.

Data collected by LPR systems is subject to all classification, access, retention, audit, and destruction requirements set forth in Minn. Stat. § 13.824.

Operations of LPR equipment is intended to provide access to stolen and wanted files and for the furtherance of criminal investigations.

Alerts:

The officer will receive an alert if the system reads a license plate and it matches the on-board data record. The information received from license plates which trigger an LPR alert is dated information, typically 1 to 12 hours old.

Verification:

An alert from the LPR system is not probable cause to arrest, but is an indication that a stolen property report, missing person's report, or warrant may have been filed. Officers must verify all alerts received from the LPR system. The officer, when receiving a LPR alert, must confirm that the record is accurate and up to date. Verification is essential prior to taking any action based solely upon the reception of an alert from the LPR on-board system.

Amber Alert:

When an Amber Alert is activated and information is broadcast which includes a license plate number, the LPR operator will manually place the vehicle plate number into the vehicle database and proceed to patrol areas which are likely to increase the chance of encountering the vehicle. Upon receipt of updated information (plate number changes, etc.) the LPR operator must immediately update the database entry.

Reporting:

The LPR database maintains logs of each vehicle's data for 60 days. RMS reports must be written when stolen vehicles or stolen plates are recovered, or for any arrest activity. See General Order 363.10 Auto Theft Preliminary Field Investigations and 416.00 Report Writing.

Data collection, classification & use restrictions:

Data collected by a LPR may only be matched with data in the Minnesota license plate data file, provided that a law enforcement agency may use additional sources of data for matching if the additional data relates to an active criminal investigation. A central state repository of automated license plate reader data is prohibited unless explicitly authorized by law.

Data collected by a LPR must be limited to the following: (1) license plate numbers; (2) date, time, and location data on vehicles; and (3) pictures of license plates, vehicles, and areas surrounding the vehicles. Collection of any data not authorized by this paragraph is prohibited.

All data collected by a LPR is private data on individuals or nonpublic data unless the data is public under Section 13.82, subdivision 2, 3, or 6, or is active criminal investigative data under Section 13.82, subdivision 7.

The LPR must not be used to monitor or track an individual who is the subject of an active criminal investigation unless authorized by a warrant, issued upon probable cause, or exigent circumstances justify the use without obtaining a warrant.

Authorization to access data:

LPR data is stored for a short timeframe on the LPR hard drive. Access to review and query stored data shall be limited to designated Technology Unit personnel or other trained personnel who have received documented authorization from a Technology Unit LPR administrator to access LPR data for authorized purposes. The Technology Unit will conduct an annual review of the access list. Only users whose work assignment reasonably requires access will be granted authorization to access LPR data. Any change in a user's access based on a change in work assignment will be administered through the City of St Paul Office of Technology (OTC).

LPR data query log: The Property Crimes investigator or other authorized users conducting a query must make a log entry into the Technology Unit's LPR data query log, to include case number or reasons for the search. Each query must be based on a reasonable suspicion that the data is pertinent to an active criminal investigation and must include a record of the factual basis for the access and any associated case number, complaint, or incident that is the basis for the access. Data may only be accessed for a legitimate, specified and documented law enforcement purpose. Once LPR stored data has been identified as having evidentiary value, it must be copied to an investigative file according to department evidence policy.

A public audit log must be maintained, and include, but not limited to specific times of day the reader actively collected data, and the number of vehicles on which data are collected per category.

Penalties (Minnesota State Statute § 13.09)

(a) Any person who willfully violates the standards for unauthorized access to data or whose conduct constitutes the knowing unauthorized acquisition of nonpublic data, as defined in Section 13.055, subdivision 1, is guilty of a misdemeanor.

(b) Willful violation of Minnesota Statutes chapter 13, including any action subject to a criminal penalty under paragraph (a), by any public employee constitutes just cause for suspension without pay or dismissal of the public employee. See also General Orders 235.00 Data Practices and 236.00 Computer Security.

If there is a breach in security of LPR data maintained by the department, notifications will be made to those affected by the breach and an investigation started by the Technology Unit Administrators and the City of St Paul Office of Technology (OTC) staff as provided under Minn. Stat. § 13.055.

A government entity that collects, creates, receives, maintains, or disseminates private or confidential data on individuals must disclose any breach of the security of the data following discovery or notification of the breach. We will investigate crimes that occur in our jurisdiction and within our authority.

Sharing among law enforcement agencies:

Automated license plate reader data that is not related to an active criminal investigation may only be shared with, or disseminated to, another law enforcement agency upon meeting the standards for requesting access to data as provided in Minnesota State Statute § 13.824 Subd. 7.

If data collected by an automated license plate reader is shared with another law enforcement agency under this subdivision, the agency that receives the data must comply with all data classification, destruction, and security requirements of this section. When sharing with another law enforcement agency, a confidentiality notice must be transmitted with the disclosed data.

Automated license plate reader data that is not related to an active criminal investigation may not be shared with, disseminated to, sold to, or traded with any other individual or entity unless explicitly authorized by Minnesota Statutes § 13.824 or other law.

Notification to Bureau of Criminal Apprehension:

Within ten days of the installation or the integration of a LPR technology into another surveillance device, the BCA must be notified of that installation.

Destruction of Data:

Notwithstanding Minn. Stat. § 138.17 (Government Records; Administration) and except as otherwise noted below, data collected by a LPR that is not related to an active criminal investigation must be destroyed no later than 60 days from the date of collection. The Technology Unit commander will ensure compliance with statutory destruction requirements.

Upon written request from an individual who is the subject of a pending criminal charge or complaint, along with the case number and a statement that the data may be used as exculpatory evidence, data otherwise subject to destruction under the above paragraph must be preserved by the Saint Paul Police Department until the criminal charge or complaint is resolved or dismissed.

Upon written request from a program participant as defined under chapter 5B, LPR data related to the program participant must be destroyed at the time of collection or upon receipt of the request, whichever occurs later, unless the data is active criminal investigative data. The existence of a request submitted under this paragraph is private data on individuals.

Data that is inactive criminal investigative data is subject to destruction according to the retention schedule for the data established under Minn. Stat. § 138.17 (Government Records; Administration).

Biennial audit:

The law enforcement agency must maintain records showing the date and time automated license plate reader data was collected and the applicable classification of the data. The law enforcement agency shall arrange for an independent, biennial audit of the records to determine whether data currently in the records is classified, how the data is used, whether it is destroyed as required under this section, and to verify compliance with authorization to access data. The results of the audit are public.

A report summarizing the results of each audit must be provided to the commissioner of administration, to the chair and ranking minority members of the committees of the house of representatives and the senate with jurisdiction over data practices and public safety issues, and to the Legislative Commission on Data Practices and Personal Data Privacy no later than 30 days following completion of the audit.

The commander of the Technology Unit will ensure the LPR data files are collected, maintained, dispersed, audited, and destroyed in accordance with Minn. Stat. § 13.824 (Automated License Plate Readers) Automated License Plate Readers.

Effective June 12, 2026