

**SAUK CENTRE POLICE DEPARTMENT**  
**Law Enforcement**  
**Policies and Procedures**

Subject: Automated License Plate Readers	Policy Number: 236
Issue Date: 05-05-2025	Revision Date:
Approval Authority - Title and Signature: Joe Jensen, Chief of Police	

**POLICY**

It is the policy of the Sauk Centre Police Department to utilize and operate automated license plate reader technology (ALPR). ALPR technology, also known as License Plate Recognition (LPR), provides automated detection of license plates.

**PROCEDURE**

ALPRs are used by law enforcement to convert data associated with vehicle license plates for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates, and missing persons. ALPRs may also be used to gather information related to active warrants, homeland security, electronic surveillance, suspect interdiction, and stolen property recovery.

**A. Definitions:**

1. Automated License Plate Reader (ALPR): A device that uses infrared cameras and/or in squad camera systems to scan license plate data of moving and stationary vehicles. This data is then compared to a downloaded “hot list” to identify license plates associated with certain unlawful acts.
2. Hot List: A downloadable list of stolen vehicles and license plates, suspended or revoked licenses and registrations as well as any other unlawful activity information. This information is provided by the Minnesota Department of Public Safety’s Driver and Vehicle Services (DVS) Division, National Crime Information Center (NCIC), and the Bureau of Criminal Apprehension (BCA).
3. Alert/Hit: An alert or hit is generated when the Automated License Plate Reader identifies license plates that have the possibility of matching information on the hot list.

**B. Administration of ALPR data:**

The Chief of Police or his/her designee will assign personnel under his/her command to administer the day-to-day operation of the ALPR equipment and data.

**C. ALPR Operation:**

Use of an ALPR is restricted to the purposes outlined below. Department personnel shall not use, or allow others to use, the equipment or database records for any unauthorized purpose.

1. No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.
2. An ALPR shall only be used for official and legitimate law enforcement business.

3. An ALPR may be used in conjunction with any patrol operation or official department investigation. Reasonable suspicion or probable cause is not necessary before using an ALPR.
4. ALPRs 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.
5. An agency's case number or incident number shall be associated with a search of the ALPR data. In the case of an emergency, the complaint or incident type can be the factual basis for the access.
6. ALPRs will be primarily used to identify possible stolen plates and vehicles, suspended or revoked license holders, and vehicle registrations; however, license plate information may be entered manually in situations where exigency exists. A supervisor will have the ability to manually enter an alert if exigency exists or a search warrant is obtained. The reason for the exigency must be entered.
7. An alert, in and of itself, does not constitute probable cause or reasonable suspicion to initiate a traffic stop. All alerts must be confirmed by the officer and reasonable suspicion or probable cause must be established before conducting a traffic stop.
8. While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped cars to canvass areas around homicides, shootings, and other major incidents.
9. If practical, the officer should verify an ALPR response through the Minnesota Justice Information Services (MNJIS) and National Law Enforcement Telecommunications System (NLETS) databases before taking enforcement action that is based solely upon an ALPR alert.
10. No ALPR operator may access MNJIS or NLETS data unless otherwise authorized to do so. ALPR operators must obtain clearance through the Bureau of Criminal Apprehension (BCA) prior to operating ALPR equipment or accessing ALPR data.

**D. Limitations of the ALPR:**

1. Because the ALPR is not connected to a “real-time” database, but rather a downloadable file, the data on the ALPR may be outdated. As such, it is imperative for officers to independently confirm all alerts before acting on an ALPR return.
2. The ALPR may generate a false-positive alert in certain instances, such as if another state’s license plate number matches the numbers of a Minnesota license plate on the hot list.

**E. Procedures:**

1. Receiving an alert
  - a. When the ALPR detects a hot list entry, an audible alert and visual notification will be generated.

- b. An alert on its own shall not be used as reasonable suspicion or probable cause for a traffic stop or enforcement contact. Contact with the vehicle and/or occupants may only be made after the alert is confirmed by matching the vehicle information with the hot list description and verifying information through appropriate means such as the Communications Center, DVS, CJIS, originating agency, etc.
- c. If an officer issues a citation or makes an arrest based on an ALPR alert, the officer shall upload the alert into Evidence.com under the appropriate case number and save it as evidence. The officer shall complete data entry in the system in which the alert was generated.

#### **F. ALPR Data Collection and Retention**

ALPR data received from another agency shall be maintained securely and released in the same manner as ALPR data collected by this department (Minn. Stat. § 13.824).

ALPR data not related to an active criminal investigation must be destroyed no later than 60 days from the date of collection with the following exceptions (Minn. Stat. § 13.824):

1. Exculpatory evidence – Data must be retained until a criminal matter is resolved if a written request is made from a person who is the subject of a criminal investigation asserting that ALPR data may be used as exculpatory evidence.
2. Address Confidentiality Program – Data related to a participant of the Address Confidentiality Program must be destroyed upon the written request of the participant. ALPR data already collected at the time of the request shall be destroyed and future related ALPR data must be destroyed at the time of collection. Destruction can be deferred if it relates to an active criminal investigation.

All other ALPR data should be retained in accordance with the established records retention schedule.

#### **G. Log of Use**

A public log of ALPR use will be maintained that includes (Minn. Stat. § 13.824):

1. Specific times of day that the ALPR collected data.
2. The aggregate number of vehicles or license plates on which data are collected for each period of active use and a list of all state and federal public databases with which the data were compared.
3. For each period of active use, the number of vehicles or license plates related to:
  - a. A vehicle or license plate that has been stolen.
  - b. A warrant for the arrest of the owner of the vehicle.
  - c. An owner with a suspended or revoked driver's license or similar category.
  - d. Active investigative data.
4. For an ALPR at a stationary or fixed location, the location at which the ALPR actively collected data and is installed and used.

A publicly accessible list of the current and previous locations, including dates at those locations, of any fixed ALPR or other surveillance devices with ALPR capability shall be maintained. The list may be kept from the public if the data is security information as provided in Minn. Stat. § 13.37, Subd. 2.

#### **H. Accountability**

All saved data will be closely safeguarded and protected by both procedural and technological means. The Sauk Centre Police Department will observe the following safeguards regarding access to and use of stored data (Minn. Stat. § 13.824; Minn. Stat. § 13.05):

1. All ALPR data downloaded 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. Members approved to access ALPR 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 office-related civil or administrative action.
3. Biennial audits and reports shall be completed pursuant to Minn. Stat. § 13.824, Subd. 6.
4. Breaches of personal data are addressed as set forth in the Protected Information Policy (Minn. Stat. § 13.055).
5. All queries and responses, and all actions in which data are entered, updated, accessed, shared or disseminated, must be recorded in a data audit trail.
6. Any member who violates Minn. Stat. § 13.09 through the unauthorized acquisition or use of ALPR data will face discipline and possible criminal prosecution (Minn. Stat. § 626.8472).

#### **I. Releasing ALPR Data**

The ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law, using the following procedures (Minn. Stat. § 13.824):

1. The agency makes a written request for the ALPR data that includes:
  - a. The name of the agency.
  - b. The name of the person requesting.
  - c. The intended purpose of obtaining the information.
  - d. A record of the factual basis for the access and any associated case number, complaint or incident that is the basis for the access.
  - e. A statement that the request is authorized by the head of the requesting law enforcement agency or his/her designee.
2. The request is reviewed by a supervisor and must be approved before the request is fulfilled.
  - a. A release must be based on a reasonable suspicion that the data is pertinent to an active criminal investigation.

3. The approved request is retained on file.
  - a. The approving supervisor will start an assist agency case/incident number and document in comments, the agency that is requesting data, the requesting agency's case number, and the requesting officer.
  - b. The approving sergeant will save the written request under the assist agency case number.

Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Records Maintenance and Release Policy.