SUN PRAIRIE POLICE DEPARTMENT
POLICY AND PROCEDURE

Field Operations Policy
LICENSE PLATE RECOGNITION

POLICY F-18

UPDATED: **April 15, 2025**	REFER TO:
REVIEWED: May 6, 2025	HISTORY: REPLACES F-18 (12/17/2010); UPDATED 08/11/2014, UPDATED 10/31/2016, UPDATED NEW FORMAT 05/06/2025

CONTENTS

1.1 POLICY

The Sun Prairie Police Department (SNPD) utilizes both fixed and mobile Automated License Plate Reader (ALPR) systems to enhance public safety, aid in criminal investigations, and improve law enforcement efficiency. ALPR systems capture infrared images of vehicle license plates, convert them to digital text using Optical Character Recognition (OCR) technology, and match them against databases of license plates of interest. ALPR systems can alert officers when a match is detected, aiding in identifying stolen vehicles, wanted persons, and other subjects of interest.

This policy governs the use, management, and retention of ALPR data by SNPD personnel, ensuring compliance with privacy laws and safeguarding civil liberties.

1.2 OBJECTIVE

To provide department members with guidelines on the proper use of fixed and mobile ALPR systems in their official duties.

1.3 DEFINITIONS

ALPR (Automated License Plate Reader):
A system consisting of cameras and technology that captures images of vehicle license plates, converts them to digital text using OCR, and compares them to databases of vehicles of interest.

OCR (Optical Character Recognition):
Technology that identifies printed characters using photoelectric devices and computer software.

Read:
A digital image of a license plate and associated metadata (e.g., date, time, and geographic coordinates) are captured by the ALPR system.

Alert:
A visual and/or auditory notice triggered when an ALPR system detects a match between a scanned license plate and a plate of interest in the system's database.

Hit:
A read that matches a license plate on a list of plates related to stolen vehicles, wanted individuals, or other investigatory purposes.

Hot List:
A list of license plate numbers of interest to law enforcement agencies, including, but not limited to, 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 and the National Crime Information Center (NCIC), as well as national AMBER Alerts and Department of Homeland Security watch lists. The Department of Transportation can provide lists of expired registration plates, 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.

Stored ALPR Data:
Data, including license plate images, vehicle images, and metadata, obtained by the ALPR system and stored for future querying.

1.4 PROCEDURE

1.4.1 MANAGEMENT AND OVERSIGHT

1.4.1.1 System Oversight:

The Chief of Police shall assign a System Administrator who is responsible for overseeing the ALPR program, including the installation, maintenance, and operation of both fixed and mobile ALPR units. This individual will also manage system security, data retention, and system audits.

1.4.1.2 Quarterly Reports:

The System Administrator will compile quarterly reports on ALPR system usage, including the number of reads, alerts, successful deployments, and any policy violations. The report will also include a summary of audits completed during the quarter.

1.4.1.3 Data Retention:

Data retention for ALPR reads shall be as follows:

(1) Mobile ALPR units: Data will be retained for 12 months unless flagged for an active investigation.

(2) Fixed ALPR units: Data will be retained for 30 days unless needed for investigative purposes.

1.4.2 AUTHORIZED USER ACCESS

1.4.2.1 Authorized Personnel:

Only authorized department personnel who have received training in the use of ALPR systems may access or operate the system. Unauthorized access or use of ALPR data is strictly prohibited.

1.4.2.2 Login Requirements:

Authorized users must log into the ALPR system using their designated credentials. All access will be automatically logged by the system, including the date, time, user identity, and purpose of access.

1.4.2.3 Data Access Logs:

The system will automatically record all queries and access to stored ALPR data, including the user, the purpose of the query, and the data retrieved. These logs will be used for auditing purposes to ensure compliance with departmental policy.

1.4.2.4 Data Confidentiality:

ALPR data is confidential and restricted to legitimate law enforcement purposes. Data may only be shared with other law enforcement agencies, or released to external parties, in accordance with applicable state statutes, court orders, or subpoenas.

1.4.2.5 Background Investigations:

Personnel authorized to access or use ALPR systems must undergo background investigations, including CIB and FBI record checks by fingerprint identification, before being granted access to ALPR data or systems.

1.4.3 ALPR USAGE

1.4.3.1 System Operation:

Officers using vehicles equipped with mobile ALPR units must ensure that the system is operational at the beginning of their shift.

Trained and authorized officers operating LPR equipped squads should have the system in operation to maximize the opportunity to scan vehicles, compare them to the hot lists, and collect ALPR data.

1.4.3.2 Alert Verification:

Upon receiving an alert, officers must visually verify that the license plate matches the plate read by the ALPR system. Officers must also verify the current status of the vehicle through dispatch or a law enforcement database (e.g., NCIC, TIME) before taking any enforcement action.

1.4.3.3 Documentation of Actions:

Any law enforcement actions taken based on an ALPR alert must be documented in a report of citation, including the reason for the stop, the verification process, and any enforcement actions taken.

Standardized Statement: A standardized statement should be included in reports or citations, such as:

“The vehicle was identified via the Automated License Plate Reader (ALPR) system. The license plate was visually verified, and the status was confirmed through NCIC/TIME before enforcement action was taken.”

1.4.3.4 Reporting Successful Uses:

Officers are required to report all successful uses of the ALPR system (e.g., identification of stolen vehicles or wanted persons) to the System Administrator by using the ALPR classification in RMS, ensuring accountability and tracking system effectiveness.

1.4.4 ACCESS TO STORED ALPR DATA

1.4.4.1 Querying ALPR Data:

Authorized personnel may query stored ALPR data only when there is a reasonable belief that the data relates to an active investigation or legitimate law enforcement purpose.

1.4.4.2 Data Sharing:

Mobile ALPR Data: Data from mobile ALPR systems is shared through the Multi-jurisdictional Public Safety Information System (MPSIS) with authorized agencies.
Fixed ALPR Data: Data from fixed ALPR systems is shared through the Flock System, the current fixed ALPR provider, with designated law enforcement agencies.

1.4.4.3 Dissemination to Non-Law Enforcement Agencies:

ALPR data shall only be released to law enforcement agencies for legitimate law enforcement purposes. Any request for data from non-law enforcement entities must go through the department's open records process. Any other release or dissemination of ALPR data to non-law enforcement agencies, private individuals, or external organizations is strictly prohibited unless required by court order, subpoena, or the chief or their designee.

1.4.5 MAINTENANCE AND AUDITING

The System Administrator shall conduct audits of ALPR system usage and data access at least quarterly. Audits will ensure compliance with departmental policy.

(1) All searches of ALPR data have a reason that includes either a unique identifying number, such as a case number, or specific information showing the purpose of the request.
(2) Will verify the data search reason.
(3) Verify retention plan.

1.4.6 SYSTEM UPDATES AND TECHNOLOGY CHANGES

The Sun Prairie Police Department will regularly review its ALPR systems to ensure they remain up to date with technological developments and legal standards. The System Administrator will be responsible for:

(1) Implementing any necessary software or hardware updates.
(2) Ensuring that any updates comply with current legal and regulatory standards.
(3) Regularly evaluating the system for any required modifications to ensure optimal performance and continued compliance with privacy laws.

1.4.7 PRIVACY SAFEGUARDS

The Sun Prairie Police Department is committed to safeguarding the privacy and civil liberties of the community while utilizing ALPR technology. To ensure privacy protection, the following measures are implemented:

1.4.7.1 Minimization of Data Retention:

ALPR data retention periods are minimized to 30 days for fixed units and 12 months for mobile units, with any extensions only applied for legitimate investigative purposes.

1.4.7.2 Restricted Access:

Only authorized personnel with a clear law enforcement purpose may access stored ALPR data. All access is automatically logged and subject to regular audits.

Any employee becoming aware of a possible violation of this policy, including but not limited to the unauthorized access, use, release and/or dissemination of LPR data, shall refer the matter to his or her supervisor.

1.4.7.3 Limited Data Usage:

ALPR systems are only used for legitimate law enforcement activities, including locating stolen vehicles, identifying wanted persons, and supporting criminal investigations. The system must not be used to track individuals or vehicles without reasonable suspicion of a crime.

1.4.7.4 Non-Discriminatory Use:

ALPR technology must not be used to monitor individuals or groups based on protected characteristics such as race, religion, gender, or political affiliation. All uses of the ALPR system must comply with federal, state, and local anti-discrimination laws.

1.4.7.5 Public Transparency:

The department will provide annual reports summarizing the use of ALPR systems, including audits, to maintain public transparency and trust. These reports will be made available to the public in accordance with department policies on public records requests.