POLICY & PROCEDURE

STURGEON BAY POLICE DEPARTMENT

SUBJECT: **AUTOMATED LICENSE PLATE READER (ALPR)**

SCOPE: All Sworn Personnel
DISTRIBUTION: Policy & Procedure Manual

REFERENCE: State v. Newer, 2006AP2388-CR

NUMBER: 6.42

ISSUED: 03/30/2026
EFFECTIVE: 03/30/2026
☐ RESCINDS
☐ AMENDS
WILEAG 6TH EDITION
STANDARDS: N/A

INDEX AS: ALPR
Automated License Plate Reader

PURPOSE: The purpose of this Policy & Procedure is to provide members of the Sturgeon Bay Police Department with guidelines on the proper capture, use, and retention of digital data obtained through the use of Automated License Plate Readers (ALPR) that is consistent with respect for individuals' privacy and civil liberties.

This Policy & Procedure consists of the following numbered sections:

I. INTRODUCTION

II. DEFINITIONS

III. POLICY

IV. PROCEDURE

I. INTRODUCTION

A. An Automated License Plate Reader (ALPR) system is a computer–based system that utilizes special cameras attached to police squad cars or deployed at fixed locations to capture license plate information on public roadways and public property.

The ALPR system passively captures an infrared image of the license plates of moving or parked vehicles and converts them to a text file using Optical Character Recognition ("OCR") technology.

The text is compared to various hot lists generated by various law enforcement agencies, including the National Crime Information Center ("NCIC"), Crime Information Bureau (CIB), Wisconsin Department of Transportation (WisDot), and the local agency, and generates an alert when there is a hit.

The ALPR system also transmits and stores the 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 to a shared server.

The stored ALPR data can be queried by license plate number, time frame, and location and will return the reads (images of license plates and vehicles, date, time, and geographic coordinates) matching the search criteria. (Access and authorization to run queries is restricted.) Stored ALPR data is not associated with and will not identify any person who is operating a vehicle. It only identifies a license plate number.

The ALPR system shall be restricted to legitimate law enforcement uses for the purpose of furthering legitimate law enforcement goals and enhancing public safety. Such uses and goals include but are not limited to:

Providing information to officers that will assist in on-going criminal investigations, crime prevention, crime detection, the apprehension of wanted persons, identification of individuals who pose a potential public safety risk to the community, ensuring the safety of vulnerable individuals through the recovery of missing and endangered persons, and improving the quality of life in the community through the identification and removal of stolen, and unregistered motor vehicles, the collection of overdue fines from parking violators, and enforcement of certain regulations. In summary the ALPR system will aid officers in ensuring the safety of the community.

II. POLICY

A. It shall be the policy of the Sturgeon Bay Police Department that all members abide by the guidelines set forth herein when using ALPR's to capture, use, and retain data captured from ALPR's, thereby increasing the efficiency and effectiveness of its public safety efforts in a manner that safeguard the privacy concerns of law-abiding citizens.

III. DEFINITIONS

A. ALERT means visual and/or auditory notice that is triggered when the ALPR system receives a potential "hit" on a license plate.

B. ALPR means Automated License Plate Reader

C. FOUO means For Official Use Only.

D. HIT means a read matched to a plate that has previously been registered on a “hot list” of vehicle plates related to stolen vehicles, wanted vehicles, or other factors supporting investigation.

E. HOT LIST means 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 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 ALPR system. These lists serve an officer safety function as well as an investigatory purpose.

F. OCR means Optical Character Recognition

G. READ means a digital image 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 ALPR system.

H. STORED ALPR DATA or SCANNED FILE means data obtained by an ALPR of license plates that were read by the device, including potential images of the plate and vehicle on which it was displayed, and information regarding the location of the police squad car or fixed location at the time of the ALPR read.

IV. PROCEDURE

A. Management

1. The Captain is designated as the ALPR Administrator and is responsible for the functionality of all equipment, user access control including on which machines the ALPR software is installed, authorized users, passwords, user rights, and maintenance of hot lists, manually entered license plate numbers, ALPR Stored Data Access Log, and Secondary Dissemination Log.

   The ALPR administrator shall periodically, at least annually, compile statistics of ALPR uses and provide an update to the Chief of Police.

2. The ALPR Administrator, along with contracted ALPR providers will be responsible for maintenance of the servers, data storage and security, system software, automatic system upload of scanned data files to the shared servers, and causing the regular updating of the WisDot ALPR Hot Lists. The ALPR Administrator will at least annually provide ALPR system status and usage information to the Chief.

3. The ALPR Administrator is responsible for procurement, installation and maintenance of cameras, hardware, loading software on to local machines, and system access and security.

4. ALPR data is confidential, for official use only (FOUO), and can be shared only for legitimate law enforcement purposes, or when required by a subpoena or court order, or unless such disclosure is required by the Rules of Court governing discovery in criminal matters. Dissemination to a non-law enforcement agency shall be approved by the Chief of Police. The Department is responsible for making reproductions of stored scanned files and for placing a copy in the local evidence system. When ALPR data is shared outside of the Department, it should be documented in a Department Secondary Dissemination Log.

5. ALPR data files will be retained for no longer than 36 months (unless a longer period is required by court order or the law), after which the data shall be purged from the data storage device or system.

B. Authorized User Access

1. The use of the ALPR system, equipment, or data is restricted to authorized Department members for official and legitimate law enforcement purposes. Unofficial, improper, or otherwise unauthorized use of the ALPR system or equipment, or the unauthorized access, use, release and/or dissemination ALPR data will be considered a significant infraction of Department policy and subject to disciplinary action and/or criminal prosecution.

2. If a civilian person(s) will be authorized, a background investigation, including CIB and FBI record checks by fingerprint identification, must be conducted before that person(s) is authorized by the Chief to use or access the ALPR system, equipment, or data.

3. Only authorized Department members who have been trained in its use and this policy may operate the ALPR system or access stored ALPR data.

4. Authorized Department members shall use their designated user identification and password when using the system.

C. Access to Stored ALPR Data

1. Access to stored ALPR data shall be limited to Department members designated by the Chief. These members will be issued a unique individual log-in ID and passwords by the ALPR Administrator.

2. Members needing to query stored ALPR data, but who are not authorized, may request that an authorized member make the query. For example, a dispatcher(s) may be authorized to access stored data.

3. Authorized members may access stored ALPR data upon a reasonable belief that the data may be related to or useful as part of a specific official action or investigation. Members accessing stored ALPR data will document each access in the ALPR Stored Data Access Log, including the date, time, purpose, reference number, and requesting employee name, comparable to what is done for criminal history checks. Similarly, dissemination of stored ALPR data outside the Department shall be documented in the ALPR Secondary Dissemination Log. ALPR data is for official law enforcement use only and any other dissemination shall be approved by the Chief.

D. ALPR Usage

1. At the start of each shift, users must log in using their designated user ID and password, enter their name or employee number in the location field, and ensure that the ALPR system has been updated with the most current hot lists available. Users should log out of the system at the end of their shift.

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

3. ALPR's should only be utilized to record license plates that are exposed to public view (visible from public streets or from private property held open to the public), absent a court order.

4. ALPR's or ALPR data shall not be used to harass or intimidate any individual or group. It is a violation of this policy to use the ALPR system or data because of a person's or group's protected characteristic, for personal use, or for the purpose or known effect of infringing upon First Amendment rights.

5. Employees should notify their supervisor of successful uses of the ALPR system.

6. 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 ALPR data, shall refer the matter to his or her supervisor as soon as possible.

E. Steps Preliminary to Police Action

Upon receiving a hit or alert, prior to initiation of a stop, the officer should:

1. Verify that the vehicle plate number matches the plate number run by the ALPR system.

2. Verify the current status of the plate through dispatch or query.

a) If the alert is valid, the officer should take appropriate action based on the type of alert. Officers are reminded that in some cases, the driver or

occupant of the vehicle may not be the person with whom the license plate is associated. Officers should develop a reasonable belief that the operator or occupant is the person of interest (compare observed physical appearance with the physical description provided). If the officer remains unaware of any facts that would suggest that the owner is not driving, there is a reasonable assumption that the owner of a vehicle is the driver (State v. Newer).

3. Police actions or stops precipitated by an ALPR alert will be documented using an incident or call number.

4. In any case, the officer may stop a vehicle where he/she has an independent reason for doing so, such as an unrelated traffic violation.

5. Nothing in this policy shall restrict or prohibit an officer from taking appropriate police action based on facts or reason obtained independently from ALPR operation.

F. Hot Lists

1. The Department shall utilize hot lists that further the goals of the ALPR system where there is a legitimate and specific law enforcement reason for identifying a vehicle or a person reasonably believed to be associated with that vehicle, such as:

Persons who are subject to an outstanding arrest warrant; missing persons; AMBER Alerts; stolen vehicles; vehicles that are reasonably believed to be involved in the commission of a crime; vehicles that are registered to or are reasonably believed to be operated by persons who do not have a valid operator's license or who are on the revoked or suspended list.

Also, vehicles with expired registrations; persons who are subject to a restraining order issued by a court, or who are subject to any other duly issued order restricting their movements; persons wanted by a law enforcement agency who are of interest in a specific investigation, whether or not such persons are themselves suspected of criminal activity; and when information has been received concerning a specific individual or individuals who pose a potential public safety risk to the community.

2. The Department will utilize the following WisDot supplied hot lists.

Hot Lists	
Articles (Stolen)	License Plate (Stolen)
Boat (Stolen)	Local Agency Hot Lists
Canadian Stolen Vehicle	Missing Person
DOT Cancelled	National Sex

	Offender
DOT Expired	Probation
DOT History	Protection Order
DOT Restricted	Sex Offender
Foreign Fugitive	USSS Protected
Gun (Stolen)	Vehicles (Stolen)
Identity Theft	Violent Gang Member
Immigration Violator	Wanted Person

3. The Department created hot lists and license plate numbers manually entered into the ALPR system shall, consistent with this policy, be for a legitimate and specific law enforcement purpose.

G. Public Records Analysis Considerations

1. Requests for records are analyzed on a case by case basis to determine whether the record is exempt from disclosure under applicable law, or the public interest served by not making the record public clearly outweighed the public interest served by disclosure. Also refer to 10.03: Open Records and 10.04: DPPA.

2. Disclosure of ALPR data that would infringe on the personal privacy of individuals.

3. Disclosure that could affect the perceived character and reputation of an individual.

4. Aggregated ALPR data in uncorroborated and there may be errors in ALPR reads of license plates.

5. Disclosure of a person's location or pattern of travel could heighten the person's vulnerability to theft or physical harm.

6. Disclosure would chill First Amendment rights by diminishing anonymity as the person travels to and from protected activities (protests, religious services, AA meetings, etc.).

7. Disclosure of aggregated data could result in unsolicited contact of individuals by commercial enterprises.

8. A record subject often has an enhanced right of access, however, in this instance this data is not associated with persons. Often a vehicle displaying a license plate is not used exclusively by one person or is registered to more than one person.

9. ALPR System statistical information, secondary dissemination logs, stored file access logs, audits, and reports to oversight bodies, Commissions, or

Committees may be subject to disclosure or partial disclosure.

H. TRAINING

1. Only persons trained in the use of the Department ALPR system, including its privacy and civil liberties protections and this policy, shall be allowed access to Department ALPR Data. All training shall be determined by the Chief and administered and recorded by the ALPR Administrator.

2. Training shall be updated as technological, legal, and other changes that affect the use of the Department ALPR system occur or at the discretion of the Chief. In no case shall a person utilize the Department ALPR system if he/she has not completed training in more than a year.

Clinton Henry
Chief of Police

This Policy & Procedure cancels and supersedes any and all previous written directives relative to the subject matter contained herein.

Initial 04/10/2023