Automated License Plate Reader Systems

353.1 PURPOSE AND SCOPE

This policy governs the use of Automated License Plate Reader (ALPR) technology by members.

353.2 POLICY

The policy of the Battle Creek Police Department (BCPD) is to utilize Automated License Plate Reader (ALPR) technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public. The intended use of ALPR technology is to assist officers with objective actionable leads needed to solve investigations and protect the community. All data and images gathered by the ALPR shall only be for the official use of this department.

353.3 DEFINITIONS

Active ALPR Data: Active ALPR Data is information which is provided to a law enforcement official in real-time. Active ALPR Data includes alerts or notifications that a license plate number contained on an Alert List has been detected in the vicinity of an ALPR Unit.

Shared ALPR Data: Shared ALPR Data is information that is collected from an outside agency that is law enforcement sensitive. Shared data is stored and accessed through the vendor’s data sharing platform with other law enforcement agencies. Shared information is not owned by the department and can only be used for law enforcement investigations.

Crime: As used herein, the term "crime" shall mean an act or the commission of an act that is forbidden or the omission of a duty that is commanded by a public law and that makes the offender liable to punishment by that law. The term "crime" includes acts of terrorism.

Historical ALPR Data: Historical ALPR Data consists of the dates, times, images, and locations of individually identifiable motor vehicles that are stored for future use and includes any ALPR Data not considered Active LPR Data.

Hot List: A temporary list of vehicles within the ALPR program that have been entered by an authorized BCPD member as part of an active investigation.

ALPR Alert List Entry: An ALPR Alert List Entry or “Hot List” is entering a known license plate with a criminal predicate into the ALPR System.

ALPR Data: ALPR Data consists of all ALPR images and/or alerts that are active or historical in nature and stored within the ALPR System.

ALPR System: An ALPR System consists of the ALPR Units, communications network components, data server hardware and software including any Optical Character Recognition (OCR) software and algorithms, all operating in an organized and coordinated manner.

ALPR Units: ALPR Units consist of the imaging hardware which captures the image of the license plates, regardless of the types of cameras used or the deployment of the unit.

353 Automated License Plate Reader Systems

353.4 ALPR DATA COLLECTION

Owners of motorized vehicles driven on public thoroughfares are required by law to annually register their vehicles with their state bureau or department of motor vehicles, and to attach license plates that are publicly and legibly displayed. Vehicle license plates generally consist of a series of alpha numeric characters that reference the license plate to the specific vehicle registered. Each piece of ALPR Data collected by BCPD may include:

a. Digital image of the vehicle
b. Vehicle license plate numbers and letters
c. The Global Positioning System (GPS) coordinates or other location information of the observation
d. The date and time of the observation, and
e. Other information contained in the ALPR image that aids in the identification of vehicles including, but not limited to, color, make, model, truck cap, etc.

The data captured by the ALPR Unit itself is entirely anonymous and is not considered personal identifying information. Officers can only identify the registered owner of a vehicle by querying a separate, secure state government database of vehicle license plate records, which is restricted, controlled, and audited. The federal Driver's Privacy Protection Act (DPPA) restricts access and prohibits the release of personal information from state motor vehicle records to ensure the privacy of citizens. 18 USC § 2721-2725.

353.4.1 ALPR DATA MAY BE COLLECTED FOR:

a. Supporting crime analysis techniques.
b. Alerting law enforcement officials of the proximity of a vehicle displaying a license plate number that is included on an Alert or Hot List.
c. Locating vehicles that have a known relationship to an individual who is reasonably suspected of having committed a crime.
d. Assisting Law Enforcement in locating missing or endangered persons.

353.4.2 ALPR DATA COLLECTION TECHNIQUES

ALPR Units may be deployed in any of the following manners:

a. In a Fixed Deployment, by being permanently mounted in a fixed location.
b. In a Portable Deployment, by being semi-permanently placed, whether overtly or covertly.
c. In a Mobile Deployment, by being mounted to a mobile vehicle, whether overtly or covertly, or by a handheld device.

353 Automated License Plate Reader Systems

353.5 USE AND DISSEMINATION OF ALPR DATA

Members may access Active ALPR data to be alerted in real time to the location of vehicles on an active hot or alert list. Entries on the hot list contain license plate information that is identifying a vehicle reported as:

a. Stolen or displaying a stolen license plate.
b. Associated with child abductions or missing and endangered persons.
c. Involved in an official law enforcement investigation when there is reasonable, articulable suspicion linking the individual to a crime that has already been committed.

Active ALPR alert entries shall not be the sole reason for an investigatory stop. Officers shall independently verify the ALPR alert entries though LEIN/NCIC databases or other means unless the officer has firsthand knowledge of the alert data.

a. Members with ALPR System access may access Historical ALPR Data to:
    1. Identify and analyze the movement of vehicles reasonably related to individuals when there is reasonable, articulable suspicion linking the individual to a crime that has already been committed.
    2. Identify and analyze the movement of vehicles displaying license plate numbers contained in a Hot List.

b. Field Operations and Enforcement Actions

    1. All users of the ALPR system will *un-select* the following: Supervised Release, Protection Order, Violent Person, Immigration Violator, Sex Offender under the NCIC notification reasons and will not take any enforcement action if the ALPR system alerts solely for these reasons.
    2. Custom Hot Lists that alert the entire organization or portions of the organization shall be authorized by a Detective, SIU Investigator or Command Officer.
    3. When notified of an NCIC “hit” from the ALPR system, operators will verify the ALPR response through the Law Enforcement Information Network (LEIN) before taking enforcement action. Action shall not be based solely on the ALPR alert.
    4. Occasionally, there may be errors in the ALPR system’s read of a license plate. Therefore, an alert alone is not a basis for police action.
        i. Members shall notify their supervisor of false positives.
        ii. The agency administrator of the ALPR system shall track false positives.
    5. Prior to initiation of a stop of a vehicle or other intervention based on an alert, operators will undertake the following:

i. Verification of a status on a hot list. An operator must confirm that the vehicle is still stolen, wanted, or otherwise of interest before proceeding (absent exigent circumstances). Without confirmation, a vehicle cannot be stopped based solely on an ALPR alert and there must be a legal justification for the stop, such as a traffic violation, reasonable suspicion, or probable cause.

ii. Visual verification of license plate number. Operators will visually verify that the license plate of interest matches identically with the image of the license plate number captured (read) by the ALPR, including both the alphanumeric characters of the license plate, state of issue, and vehicle descriptors before proceeding.

6. After the stop of a vehicle or other intervention based on the alert:

    i. The operator will notify their supervisor or authorized Alert List administrator of the positive hit and request that the plate be removed from the Active Alert List prior to the end of their shift, unless the interest in the vehicle still exists.

7. The member that entered the data on the hot list shall be responsible for removing the data when it is no longer needed.

c. Disseminating ALPR Data

1. Active and Historical ALPR Data may be disseminated to law enforcement officials from other jurisdictions upon request or through shared data on the vendor platform. The requesting agency must provide the reason for the request, and it can only be used for official law enforcement investigations. This request shall be documented in an appropriate report.

2. Non-Dissemination of Historical ALPR Data to the Public.

   ALPR Data shall only be used for law enforcement purposes. ALPR Data will not be released to the public unless required by statute, court order or when approved by Divisional Commander to warn the community of a vehicle associated with an individual that poses an immediate threat of harm to the community or an individual.

353.6 RETENTION OF ALPR DATA

ALPR Data connected to a criminal investigation shall be retained as part of the investigation record and shall be subject to department retention and disposal schedules.

ALPR Data used to convict an individual, including but not limited to Query Responses, shall be retained as part of the BCPD case file as an external document and shall be subject to department retention and disposal schedules for that specific case and conviction.

353 Automated License Plate Reader Systems

ALPR Data that is not connected to an investigation or conviction shall be subject to vendor retention and disposal schedules. Any data mining analysis shall require approval of a BCPD command officer of Sergeant or above and a reasonable articulable suspicion that a crime has occurred.

353.6 ALPR TRAINING

Use of the department's ALPR System shall be limited to members who have completed training in accordance with this section and provided documentation of successfully completing that training.

353.7 ISSUING AUTHORITY



Shannon Bagley

Chief of Police

Effective Date

January 14, 2025

BERRIEN COUNTY SHERIFF – POLICIES & PROCEDURES

CHAPTER	5	SECTION	43
PAGE	1 of 2	EFFECTIVE DATE	July 18, 2022
SUBJECT	Flock Safety System		
AUTHORITY	CHARLES E. HEIT, SHERIFF		

1. Purpose:

A. To provide guidelines on the proper use of the crime prevention license plate recognition (LPR) system, commonly known as the Flock Safety Camera (FSC) System.

B. To provide governmental accountability by ensuring that the FSC system use respects constitutional and privacy rights.

C. To deter criminal behavior and assist in criminal investigations and prosecutions.

2. Definitions:

A. Alert – a visual and or auditory notice that is triggered when the FSC system receives a potential "hit" on a license plate or vehicle indicator.
B. Fixed FSC system – FSC cameras that are permanently affixed to a structure.
C. Hit – A read matched to a plate within public view that has been registered on the agency's hot list of vehicles plates related to stolen vehicles, wanted vehicles, or other factors supporting investigation or which has been manually registered by a user for further investigation.
D. Hot List – License plate information of stolen cars, stolen registration plates, vehicles owned by persons of interest, vehicles associated with AMBER Alerts and vehicles associated with missing persons 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 the national AMBER Alerts and Department of Homeland Security watch lists. These list serve as an officer safety function as well as for investigative purposes.
E. FSC – Flock Safety Camera System
F. Read – Digital images of license plates, vehicles, and associated metadata that are captured by the FSC system.

3. Procedures:

A. FSC systems, FSC data and associated media are the property of the Berrien County Sheriff's Office and are to be used for official law enforcement purposes.
B. LEIN certified departmental members, who have been trained in the FSC system, may use the FSC system.
C. Except when done pursuant to a court order such as a search warrant, the FSC may be used only to record license plates of vehicles that are exposed to public view (e.g., vehicles on a public road or street, or that are on private property but whose license plates are visible from a public road, street, or a place to which members of the public have access, such as a parking lot.
D. Fixed FSC system is a passive system. Live data is not viewed.

E. All FSC system searches shall include a reason for the search to include the case number, and incident description.
F. Investigators entering searches for investigative purposes shall include the reason to locate, and the investigators requesting the search.
G. Users will unselect the following: supervised release, protection order, violent person, immigration violator, sex offender and will not take enforcement action based solely for these reasons.
H. When notified of a NCIC "hit" from the FSC system, deputies shall verify the FSC response through the Law Enforcement Information Network before taking enforcement action. Action shall not be based solely on the FSC alert.
I. If a vehicle needs to be removed from the hot list, the deputy will notify an investigative user of the FSC system.

4. Prohibited Practices

A. Using the FSC system or associated scan file or hot lists solely because of a person's or groups race, gender, religion, political affiliation, nationality, ethnicity, sexual orientation, disability, or other classification protected by law.
B. Using the FSC system or associated scan files or hot lists for personal purpose.

5. Administration:

A. The Berrien County Sheriff's Office Administration shall be responsible to designate an employee(s) with administrative oversight for the FSC system deployment and operations who is responsible for the following:
   - Establishing access protocols.
   - Provide FSC system training.
   - Communicating with FSC system representatives.

6. Data Sharing:

A. Outside law enforcement agencies that are part of the FSC network may be allowed search access for legitimate law enforcement purposes. Berrien County Sheriff's Office Administration approval is required.
B. Outside law enforcement agencies that are NOT part of the FSC network are required to complete a mutual aid agreement through the FSC with the Berrien County Sheriff's Office.
C. Personnel from the BCSO, who are authorized to utilize the FCS may conduct searches for an outside agency, as it pertains to a criminal investigation and meets the accepted criteria for a search to be conducted. The BCSO personnel conducting the search shall document the search by completing an incident report, which reflects the reasons and results of the search

C E Heit

Charles E. Heit
Sheriff

Birmingham Police Department

Chief of Police
Scott A. Grewe

SUBJECT	DIRECTIVE	NUMBER OF PAGES
Automated License Plate Reader (ALPR)	**471**	**7**
This Directive Supersedes All Previously Issued Correspondence Relative To This Topic*		

		Effective Date	Revised Date
		1/22/2024	6/5/2024

I. PURPOSE

The purpose of this policy is to provide guidance for the capture, storage, and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology.

II. POLICY

The policy of the Birmingham Police Department is to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public. This technology shall be utilized to proactively detect, alert, and respond to wanted vehicles/persons and used to investigate criminal activity. Data is retained by the vendor for no more than 30 days.

All data and images gathered by the ALPR are for the official use of this department. Because such data may contain confidential information, it is not open to the public review.

III. DEFINITIONS

Automated License Plate Reader (ALPR) – A device that uses cameras and computer technology to capture and digitalize images from vehicles including their license plates.

ALPR Operator – Trained Department members who may utilize ALPR system/equipment. ALPR operators may be assigned to any sworn or dispatch position within the Department, and the ALPR Administrator may order the deployment of the ALPR systems for use in various efforts.

ALPR Administrator – The Investigative Captain, serves as the ALPR Administrator for the Department.

Hot List – A list of license plates associated with vehicles of interest compiled from one or more databases including, but not limited to, NCIC, SOS, LEIN, Local BOLO's, etc.

Vehicles of Interest – Including, but not limited to vehicles which are reported as stolen; display stolen license plates or tags; vehicles linked to missing and/or wanted

persons and vehicles flagged by the Department of Motor Vehicles Administration or law enforcement agencies.

Detection – Data obtained by an ALPR of an image (such as a license plate) within public view that was read by the device, including potential images (such as the plate and description of vehicle on which it was displayed), and information regarding the location of the ALPR system at the time of the ALPR's read.

Hit – Alert from the ALPR system that a scanned license plate number may be in the National Crime Information Center (NCIC) or other law enforcement database for a specific reason including, but not limited to, being related to a stolen car, wanted person, missing person, domestic violence protection order or terrorist-related activity.

IV. PROCEDURES

A. Administration

The ALPR technology, also known as License Plate Recognition (LPR), allows for the automated detection of license plates along with the vehicle make, model, color, and unique identifiers through the Birmingham Police Department's ALPR's system and the vendor's vehicle identification technology. The technology is used by the Birmingham Police Department to convert data associated with vehicle license plates and vehicle descriptions for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates and missing or wanted persons. It may also be used to gather information related to active warrants, homeland security, electronic surveillance, suspect interdiction, and stolen property recovery. All installation and maintenance of the ALPR equipment, as well as, ALPR data retention and access, shall be managed by the Investigative Captain. The Investigative Captain will assign members under his/her command to administer the day-to-day operation of the ALPR equipment and data.

B. ALPR Administrator

The Investigative Captain shall be responsible for compliance with the requirements of Civil Codes.

a. Only properly trained sworn officers or select non-sworn staff are allowed access to the ALPR system or to collect ALPR information.
b. Ensuring that training requirements are completed for authorized users. This will be documented on the department training sign in sheet.
c. ALPR system monitoring to ensure the security of the information and compliance with applicable privacy laws.
d. The Investigative Captain oversees the ALPR operation is maintained.

C. Operations

Use of an APLR is restricted to the purposes outline below. Department

members shall not use or allow others to use the equipment or database records for any unauthorized purpose(s).

a. An ALPR shall only be used for official law enforcement business.

b. An ALPR may be used in conjunction with patrol operations or criminal investigation.

c. Partial license plates and unique vehicle descriptions reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.

d. No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.

e. When an alert is received, the officer shall verify an ALPR response through the Law Enforcement Information Network (LEIN) before taking enforcement action based solely on an ALPR alert. Once an alert is received, the operator shall confirm that the observed license plate from the system matches the license plate of the observed vehicle. Members will not take any police action that restricts the freedom of an individual based solely on an ALPR alert unless it has been validated. Because the ALPR alert may relate to a vehicle and may not relate to the person operating the vehicle, officers are reminded that they need to have reasonable suspicion and/or probable cause to make an enforcement stop of any vehicle. (For example, if a vehicle is entered into the system because of its association with a wanted individual, Officers should attempt to visually match the driver to the description of the wanted subject prior to making the stop or should have another legal basis for making the stop.)

f. Hot Lists. Designation of hot lists to be utilized by the ALPR system shall be made by the on duty supervisor or his/her designee. Hot lists shall be obtained or compiled from sources as may be consistent with the purpose of the ALPR system set forth in this policy. Occasionally, there may be errors in the LPR system's read of a license plate. Therefore, an alert alone shall not be the basis for police action (other than following the vehicle of interest). Prior to initiation of a stop of a vehicle or other intervention based on an alert, Department members shall undertake the following:

    a. **Verification of status on a Hot List**. An officer must receive confirmation, from a Birmingham Police Department member or other department computer device, that the license plate is 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. Department members alerted to the fact that an observed motor vehicle's license plate is entered as a Hot List (hit) in a specific BOLO (be on the lookout) list are required to make a reasonable effort to confirm that a wanted person is actually in the vehicle and/or that a reasonable bases exists before a Department member would have a lawful basis to stop the vehicle.

c. Department members will clear all stops from the hot list alerts by indicating the positive ALPR Hit, i.e., with an arrest or other enforcement action. If it is not obvious in the text of the call as to the correlation of the ALPR Hit and the arrest, then the department member shall update with the original person inputting the vehicle in the Hot List (hit).

d. All entries and updates of the specific Hot Lists within the ALPR system will be documented by requesting department members within the appropriate general offense report. As such, specific Hot Lists shall be approved by the ALPR Administrator (or his/her designee) before initial entry within the ALPR system.
The updating of such a list within the ALPR system shall therefore be accomplished pursuant to the approval of the department member's immediate supervisor. The hits from these data sources should be viewed as informational; created solely to bring the officers attention to the specific vehicles that have been associated with criminal activity.

All Hot Plates and suspect information entered into the ALPR system will contain the following information as a minimum:

1. Entering Department member's name and related case number
2. Short synopsis describing the nature of the originating call

D. Training

1. All authorized members shall receive department-approved training for the use and access of the ALPR system.
2. No member of this department shall operate the ALPR equipment or access ALPR data without first completing department-approved training and signing for this policy.

E. Login/Log-Out Procedure

To ensure proper operation and to facilitate oversight of the ALPR system, all users will be required to have individual credentials for access and use of the system and data, which has the ability to be fully audited.

F. Permitted/Impermissible Uses

The ALPR system, and all data collected is the property of the Birmingham Police Department. Department personnel may only access and use the ALPR system for

official and legitimate law enforcement purposes consistent with this policy. The following uses of the ALPR system are specifically prohibited:

a. Invasion of Privacy: Except when done pursuant to a court order such as a search warrant, is a violation of this policy to utilize the ALPR to record license plates except those of vehicle that are exposed to public view (e.g., vehicles on a public road or street, or that are on private property but whose license plate(s) are visible form a public road, street, or place to which members of the public have access, such as the parking lot of a shop or other business establishment).
b. Harassment or Intimidation: It is a violation of this policy to use the ALPR system to harass and/or intimidate any individual or group.
c. Use Based on a Protected Characteristic: It is a violation of this policy to use the ALPR system or associated scan files 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.
d. Personal Use: It is a violation of this policy to use the ALPR system or associated scan files or hot lists for any personal purpose.
e. First Amendment Rights: It is a violation of this policy to use the ALPR system or associated scan files or hot lists for the purpose, or known effect of, infringing upon First Amendment Rights.

Anyone who engages in an impermissible use of the ALPR system or associated scan files, or hot lists may be subject to:

a. Criminal Prosecution
b. Civil Liability, and or
c. Administrative sanctions, up to and including termination, pursuant to and consistent with the relevant collective bargaining agreement and department policies.

G. Data Collection and Retention

The Chief of Police or his/her designee(s) is responsible for ensuring systems and processes are in place for the proper collection and retention of ALPR data.

ALPR vendor, Flock Safety will store the data and ensure proper maintenance and security of the data stored in their data towers. Flock Safety will purge their data at the end of the thirty (30) days of storage.

Any data retrieved from the ALPR system, such as investigative search results for a criminal case, shall be stored in the Birmingham Police Department's CFS or Case Report. Large amounts of data can be stored in Watchguard.

Restrictions on use of ALPR data: Information gathered or collected, and records retained by the Flock Safety cameras will not be sold, accessed, or used for any purpose other than legitimate law enforcement or public safety purposes.

H. Accountability and Safeguards

All data will be closely safeguarded and protected by both procedural and technological means. The Birmingham Police Department will observe the following safeguards regarding access to and use of stored data:

a. All ALPR data downloaded to the mobile workstation shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date, and time.

b. Persons 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 is related to a specific criminal investigation or department-related civil or administrative action.

c. Such ALPR data may be released to other authorized and verified law enforcement officials and agencies for legitimate law enforcement purposes.

d. Every ALPR Detection Browsing Inquiry must be documented by either the associated Birmingham Police Department incident number, and noted in respective CFS or Case Report.

I. ALPR Data Detection Browsing Audits

It is the responsibility of the Chief of Police or his/her designee(s) to ensure that an audit is conducted of the ALPR Detection Browsing Inquiries once each calendar year. The department will audit a sampling of the ALPR system utilization from the prior 12- month period to verify proper use in accordance with the above authorized uses. The audit shall randomly select at least 5 Detection Browsing Inquiries conducted by department employees during the preceding 12 month period and determine if each inquiry meets the requirements established in this policy.

The audit shall be documented on a departmental memorandum to the Chief of Police. The memorandum shall include any data errors found so that such errors can be corrected. After review by the Chief of Police, the memorandum and any associated documentation shall be filled and retained by the Birmingham Police Department.

J. 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.

a. The request is reviewed by the Investigative Captain designee and approved before the request is fulfilled.
b. The approved request is retained on file by completing a call for service (Assist of Law Enforcement Agency) listing the above information.
c. Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be declined unless otherwise authorized by the Freedom of Information Act. Such as

data retained by the agency within an incident report. However, such data is subject to redactions allowed by law.

V. REVISION RESPONSIBILITY

Revision responsibility shall rest with the Chief of Police.

CHESTERFIELD TOWNSHIP DEPARTMENT OF PUBLIC SAFETY PROCEDURE MANUAL

Order # 3-143	Subject: Automated License Plate Reader (ALPR) Policy		Effective Date: 11/23/2021
Issued By: Director B. Bassett	MACP Standard:	Revised/Reviewed Date: 07/18/2024	

PURPOSE: The purpose of this policy is to provide guidance for the capture, storage, and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology.

SCOPE: This policy applies to all sworn members of the Chesterfield Township Police Department.

POLICY: The policy of the Chesterfield Township Police Department is to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public.

All data and images gathered by the ALPR are for the official use of this department. Because such data may contain confidential information, it is not open to public review.

DEFINITIONS:

Automated License Plate Reader (ALPR) - A device that uses cameras and computer technology to compare digital images to lists of known information of interest.

ALPR Operator - Trained Department members who may utilize ALPR system/equipment. ALPR operators may be assigned to any position within the Department, and the ALPR Administrator may order the deployment of the ALPR systems for use in various efforts.

ALPR Administrator - The Chief's designee(s), serves as the ALPR Administrator for the Department.

Hot List - A list of license plates associated with vehicles of interest compiled from one or more databases including, but not limited to, NCIC, SOS, LEIN, Local BOLO's, etc.

Vehicles of Interest - Including, but not limited to vehicles which are reported as stolen; display stolen license plates or tags; vehicles linked to missing and/or wanted persons and vehicles flagged by the Department of Motor Vehicle Administration or law enforcement agencies.

Detection - Data obtained by an ALPR of an image (such as a license plate) within public view that was read by the device, including potential images (such as the plate and description

of vehicle on which it was displayed), and information regarding the location of the ALPR system at the time of the ALPR's read.

Hit - Alert from the ALPR system that a scanned license plate number may be in the National Crime Information Center (NCIC) or other law enforcement database for a specific reason including, but not limited to, being related to a stolen car, wanted person, missing person, domestic violation protective order or terrorist-related activity.

PROCEDURE:

I. ADMINISTRATION

The ALPR technology, also known as License Plate Recognition (LPR), allows for the automated detection of license plates along with the vehicle make, model, color and unique identifiers through the Chesterfield Township Police Department's ALPR's system and the vendor's vehicle identification technology. The technology is used by the Chesterfield Township Police Department to convert data associated with vehicle license plates and vehicle descriptions for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates and missing persons. It may also be used to gather information related to active warrants, homeland security, electronic surveillance, suspect interdiction and stolen property recovery. All installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by Chief of Police Designee(s). The Chief of Police Designee(s) will assign members under his/her command to administer the day-to-day operation of the ALPR equipment and data.

II. ALPR ADMINISTRATOR

The Director of Public Safety/Chief of Police or Designee(s) shall be responsible for compliance with the requirements of Civil Codes.

A. Only properly trained sworn officers, crime analysts, and police assistants are allowed access to the ALPR system or to collect ALPR information.

B. Ensuring that training requirements are completed for authorized users.

C. ALPR system monitoring to ensure the security of the information and compliance with applicable privacy laws.

D. The title and name of the current designee in overseeing the ALPR operation is maintained. Continually working with the Custodian of Records on the retention and destruction of ALPR data.

E. Ensuring this policy and related procedures are conspicuously posted on the department's website.

III. OPERATIONS

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

A. An ALPR shall only be used for official law enforcement business.

B. An ALPR may be used in conjunction with any routine patrol operation or criminal investigation; reasonable suspicion or probable cause is not required before using an ALPR.

C. Partial license plates and unique vehicle descriptions reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.

D. No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.

E. The officer shall verify an ALPR response through the Law Enforcement Information Network (LEIN) before taking enforcement action that is based solely on an ALPR alert. Once an alert is received, the operator shall confirm that the observed license plate from the system matches the license plate of the observed vehicle. Before any law enforcement action is taken because of an ALPR alert, the alert will be verified through a LEIN inquiry via MDT or through Dispatch. Members will not take any police action that restricts the freedom of any individual based solely on an ALPR alert unless it has been validated. Because the ALPR alert may relate to a vehicle and may not relate to the person operating the vehicle, officers are reminded that they need to have reasonable suspicion and/or probable cause to make an enforcement stop of any vehicle. (For example, if a vehicle is entered into the system because of its association with a wanted individual, Officers should attempt to visually match the driver to the description of the wanted subject prior to making the stop or should have another legal basis for making the stop.)

F. Hot Lists. Designation of hot lists to be utilized by the ALPR system shall be made by the ALPR Administrator or his/her designee. Hot lists shall be obtained or compiled from sources as may be consistent with the purposes of the ALPR system set forth in this Policy. Hot lists utilized by the Department's LPR system may be updated by agency sources more frequently than the Department may be uploading them and thus the Department's LPR system will not have access to real time data. Occasionally, there may be errors in the LPR system's read of a license plate. Therefore, an alert alone shall not be a basis for police action (other than following the vehicle of interest). Prior to initiation of a stop of a vehicle or other intervention based on an alert, Department members shall undertake the following:

a. Verification of status on a Hot List. An officer must receive confirmation, from a Chesterfield Township Police Department Communications Dispatcher 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. Department members alerted to the fact that an observed motor vehicle's license plate is entered as a Hot Plate (hit) in a specific BOLO (be on the lookout) 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 a Department member would have a lawful basis to stop the vehicle.

c. Department members will clear all stops from hot list alerts by indicating the positive ALPR Hit, i.e., with an arrest or other enforcement action. If it is not obvious in the text of the call as to the correlation of the ALPR Hit and the arrest, then the Department member shall update with the Communications Dispatcher and original person and/or a crime analyst inputting the vehicle in the hot list (hit).

d. All entries and updates of specific Hot Lists within the ALPR system will be documented by the requesting Department member within the appropriate general offense report. As such, specific Hot Lists shall be approved by the ALPR Administrator (or his/her designee) before initial entry within the ALPR system. The updating of such a list within the ALPR system shall thereafter be accomplished pursuant to the approval of the Department member's immediate supervisor. The hits from these data sources should be viewed as informational; created solely to bring the officers attention to specific vehicles that have been associated with criminal activity.

All Hot Plates and suspect information entered into the ALPR system will contain the following information as a minimum:

1. Entering Department member's name Related case number.

2. Short synopsis describing the nature of the originating call

G. Training

The Training Sergeant should ensure that members receive department-approved training for those authorized to use or access the ALPR system. No member of this Department shall operate ALPR equipment or access ALPR data without first completing Department-approved training.

H. Login/Log-Out Procedure

To ensure proper operation and facilitate oversight of the ALPR 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.

I. Permitted/Impermissible Uses.

The ALPR system, and all data collected, is the property of the Chesterfield Township Police Department. Department personnel may only access and use the ALPR system for official and legitimate law enforcement purposes consistent with this Policy. The following uses of the ALPR system are specifically prohibited:

a. Invasion of Privacy: Except when done pursuant to a court order such as a search warrant, is a violation of this Policy to utilize the ALPR to record license plates except those of vehicles that are exposed to public view (e.g., vehicles 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).

b. Harassment or Intimidation: It is a violation of this Policy to use the ALPR system to harass and/or intimidate any individual or group.

c. Use Based on a Protected Characteristic. It is a violation of this policy to use the LPR system or associated scan files 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.

d. Personal Use: It is a violation of this Policy to use the ALPR system or associated scan files or hot lists for any personal purpose.

e. First Amendment Rights. It is a violation of this policy to use the LPR system or associated scan files or hot lists for the purpose or known effect of infringing upon First Amendment rights.

Anyone who engages in an impermissible use of the ALPR system or associated scan files or hot lists may be subject to:

a. criminal prosecution,

b. civil liability, and/or

c. administrative sanctions, up to and including termination, pursuant to and consistent with the relevant collective bargaining agreements and Department policies.

J. DATA COLLECTION AND RETENTION

The Director of Public Safety/Chief of Police or Designee(s) is responsible for ensuring systems and processes are in place for the proper collection and retention of ALPR data. Data will be transferred to the designated storage in accordance with department procedures.

All ALPR data downloaded to the server should be stored for no longer than one year, and in accordance with the established records retention schedule. Thereafter, ALPR data should be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a discovery request or other lawful action to produce records. In those circumstances the applicable data should be downloaded from the server onto portable media and booked into evidence.

ALPR vendor, Flock Safety will store the data (data hosting) and ensure proper maintenance and security of data stored in their data towers. Flock Safety will purge their data at the end of the 30 days of storage. However, this will not preclude CHTP from maintaining any relevant vehicle data obtained from the system after that period pursuant to the established Chesterfield Township Police Department's retention schedule mentioned above or outlined elsewhere.

Restrictions on use of ALPR Data**:** Information gathered or collected, and records retained by Flock Safety cameras or any other CHTP ALPR system will not be sold, accessed, or used for any purpose other than legitimate law enforcement or public safety purposes.

K. ACCOUNTABILITY AND SAFEGUARDS

All data will be closely safeguarded and protected by both procedural and technological means. The Chesterfield Township Police Department will observe the following safeguards regarding access to and use of stored data):

a. All non-law enforcement requests for access to stored ALPR data shall be processed in accordance with applicable law.

b. All ALPR data downloaded to the mobile workstation shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date, and time.

c. Persons 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 relate to a specific criminal investigation or department-related civil or administrative action.

d. Such ALPR data may be released to other authorized and verified law enforcement officials and agencies for legitimate law enforcement purposes.

e. Every ALPR Detection Browsing Inquiry must be documented by either the associated Chesterfield Township Police Departments case number or incident number, and/or a reason for the inquiry.

ALPR DATA DETECTION BROWSING AUDITS

It is the responsibility of the The Director of Public Safety/Chief of Police or Designee(s) to ensure that an audit is conducted of ALPR detection browsing inquiries at least once during each calendar year. The Department will audit a sampling of the ALPR system utilization from the prior 12-month period to verify proper use in accordance with the above authorized uses. The audit shall randomly select at least 10 detection browsing inquiries conducted by department employees during the preceding six-month period and determine if each inquiry meets the requirements established in policy section.

The audit shall be documented in the form of an internal department memorandum to The Director of Public Safety/Chief of Police or Designee(s). The memorandum shall include any data errors found so that such errors can be corrected. After review by the The Director of Public Safety/Chief of Police or Designee(s), the memorandum and any associated documentation shall be filed and retained by CHTP.

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.

a. The agency makes a request for the ALPR data that includes:

1. The name of the agency.

2. The name of the person requesting.

3. The intended purpose of obtaining the information.

b. The request is reviewed by The Director of Public Safety/Chief of Police or Designee(s) or the authorized designee and approved before the request is fulfilled.

c. The approved request is retained on file. Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Records Release Policy.

Clawson Police Department Policy and Procedure		Order No: 400-15
Subject: Automated License Plate Readers		
Date Issued: **May 6th, 2024**	**Distribution:** **All Personnel**	**New** ☒ **Amended** ☐ **Revised** ☐ **Reviewed** ☐
Issued By: **Kellie Bauss, Chief of Police**	**Replaces:** **MACP Standards:**	

I. Purpose
II. Policy
III. Definitions
IV. Procedure

I. PURPOSE

The purpose of this policy is to provide guidance for the capture, storage, and use of digital data obtained using Automated License Plate Readers (ALPR) Technology.

Automated License Plate Reader (ALPR) technology, also known as Automated License Plate Recognition, provides automated detection of license plates. ALPRs are used by the Clawson Police Department to link 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 investigations, active warrants, homeland security advisories and bulletins, electronic surveillance, suspect interdiction, and stolen property recovery. It is the intent of the Department to ensure that the access and use of ALPR data is consistent with respect for individuals' privacy and civil liberties.

II. POLICY

It is the policy of the Clawson Police Department to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public. It is department policy that all installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed as determined by the Chief of Police or their designee. The Chief of police will assign a supervisor to administer the day-to-day operation of the ALPR equipment and data. It is department policy to utilize ALPR systems only for legitimate law enforcement and public safety purposes.

III. DEFINITIONS

A. Automated License Plate Reader (ALPR): A device that uses cameras and computer technology to compare digital images to lists of known information of interest.

B. ALPR Operator: Trained Department members who may utilize the ALPR system.

C. ALPR Administrator: The Chief of Police or his/her designee(s) serves as the ALPR Administrator for the department.

D. Alert: An audible or visual signal activated upon the recognition of a license plate by the ALPR system.

E. Detection: Data obtained by an ALPR of an image, such as a license plate, within public view that was read by a device (vehicle description on which it displayed and plate) and information regarding the location of the ALPR system.

F. Hot List: Data files extracted from the law enforcement databases including, but not limited to: NCIC, SOS, LEIN, and local police department entries for official law enforcement purposes. These data extracts are updated numerous times per day in an effort to provide current data.

G. Hit: Alert from the ALPR system that a scanned license plate number may be in a law enforcement database for a specific reason, but not limited to, relation to a stolen vehicle, wanted person or vehicle, missing person, domestic violation protective order or terrorist-related activity.

H. Vehicles of Interest: Including, but not limited to, vehicles which are reported as stolen, display stolen license plates or tags, vehicles linked to missing and/or wanted persons, and vehicles flagged by the Secretary of State Administration or a law enforcement agency.

IV. PROCEDURE

A. Administration

1. Automated License Plate Recognition allows for automated detection of license plates along with vehicle make, model, color, and unique identifiers through the vendor's vehicle identification technology.

2. The technology is used by the Clawson Police Department to convert data associated with vehicle license plates and descriptions for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates, and/or missing persons. It may also gather information

related to active warrants, suspect interdiction, and stolen property recovery.

3. All installation and maintenance of ALPR equipment, as well as data retention and access, shall be managed by the Chief of Police and/or their designee. The Chief of Police or their designee will assign members under their command to administer the daily operations of the ALPR equipment and data.

B. ALPR Administrator

1. The Chief of Police or their designee shall be responsible for compliance with the requirements of Civil Codes and Laws. The Chief has designated the Criminal Investigations Section Sergeant as the Department's ALPR Administrator. The ALPR Administrator is responsible for the following:

a. Ensure only trained sworn officers and communications personnel are allowed access to the ALPR system or to collect ALPR information.

b. Ensure that training requirements are completed for authorized users.

c. ALPR system monitoring to ensure the security of the information and compliance with applicable privacy laws.

C. Operations

1. Use of an ALPR is restricted to the purposes outlined below. Department members shall not use, or allow to use, the equipment or database records for any unauthorized purpose(s).

a. An ALPR shall only be used for official law enforcement business.

b. An ALPR shall only be used in conjunction with any patrol operation or criminal investigation; reasonable suspicion or probable cause are not required before using the ALPR.

c. Partial license plates and unique vehicle descriptions reported during a major crime should be entered into the ALPR system in an attempt to identify suspect vehicles.

d. No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.

D. Hot Lists

1. An alert alone shall not be the basis for police action. Prior to initiation of a stop of the vehicle or other intervention based on an alert, department employees shall undertake the following:

e. Once an alert is received, the operator shall confirm that the observed license plate from the system matches the actual license plate of the observed vehicle.

f. Before any law enforcement action is taken because of an ALPR alert, the alert shall be verified through a LEIN inquiry by MDC or through Communications (unless exigent circumstances exist).

g. Officers shall not take any police action that restricts the freedom of any individual based solely on an ALPR alert unless it has been validated.

h. ALPR alerts may relate to a vehicle and not the person operating the vehicle, officers are reminded that they need to have reasonable suspicion and/or probable cause to make an enforcement stop of any vehicle.

For example, if a vehicle is entered into the system because of an association with a wanted individual, officers should attempt to visually match the driver's description of the wanted subject prior to making the stop or should have another legal basis for the stop.

2. Requests for Hot List entries and updates shall be forwarded to the following entities to enter into the ALPR system:

a. Communications

(1.) Communications will be responsible for entering ALPR Hot List information for items that require immediate action.

(2.) Entries by Communications shall be considered temporary with an expiration of 48 hours.

(3.) All entries must be approved by a supervisor.

b. Criminal Investigations

(1.) The Detective Bureau will be responsible for entering ALPR Hot List information related to incidents requiring entry of more than 48 hours.

(2.) The Detective Bureau will be responsible for removing entries that are determined to no longer be viable.

3. All Plates and Suspect Information entered into the ALPR system Hot List shall contain the following information:

a. Department Employee's name, related case number, and a short synopsis describing the nature of the originating call

E. Monitoring

1. Communications Supervisors and Communications Police Service Aides will have the Flock Safety website signed on at their workstation. It will be monitored and broadcast in accordance with Troy Police Department General Order #124.

F. Training

1. It is the responsibility of the Training Sergeant to ensure that all authorized employees receive department-approved training to use or access the ALPR system. No employee shall operate the ALPR equipment or access the data without the approved training.

G. Login/Logout Procedure

1. To facilitate oversight of the ALPR system, all users are required to have individual credentials for access and use of the system and/or data. All investigative inquiries are logged by user and available for auditing and review by the Clawson Police Department.

H. Impermissible Uses

1. The ALPR system, and all data collected, are the property of the Clawson Police Department. Department personnel may only access and use the ALPR system for official and legitimate law enforcement purposes consistent with this policy.

2. The following uses of the ALPR system are specifically prohibited:

a. **Invasion of Privacy**: Except when done pursuant to a court order such as a search warrant, it is a violation of this policy to utilize the ALPR to record license plates except those of vehicles that are visible to public view.

b. **Harassment or Intimidation**: It is a violation of this policy to use the ALPR system to harass and/or intimidate any individual or group.

c. **Personal Use**: It is a violation of this policy to use the ALPR system or associated files or hot lists for any personal use. All personnel are specifically prohibited from making a copy, such as but not limited to, using personal cellular phones, in any format of any video, audio or still photograph generated from the ALPR application or associated files or hotlists for personal use.

d. **First Amendment Rights**: It is a violation of this policy to use the ALPR system or associated files or hot lists for the purpose or known effect of infringing upon First Amendment rights.

I. Data Collection and Retention

1. The Chief of Police and/or their designee is responsible for enacting the procedure for proper collection and retention of ALPR data. Data will be transferred to the designated storage in accordance with departmental procedures for report writing, investigations, and evidence procedures.

2. All ALPR data downloaded to the server shall be stored in accordance with the established records retention schedule

a. ALPR data shall be purged unless it has become, or it is reasonable to become, evidence in a criminal or civil action or is subject to a discovery request or other lawful action to produce records. In those circumstances, the applicable data shall be uploaded and documented to the related Clear Case Report.

b. The ALPR's vendor will store the data and ensure proper maintenance and security of the data stored in their data towers. Recordings not relevant to an active investigation, a formal complaint against this agency, or an officer of this agency must be kept on the date it was created plus thirty days.

c. Recordings that contain evidence of incidents are retained until the case is solved, closed and litigation ends. [MCL 780.316]

J. Accountability

1. All data shall be closely safeguarded and protected by both procedural and technological means. The Cawson Police Department shall observe the following safeguards regarding access to and use of stored data:

a. All ALPR data downloaded to the mobile workstation shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date, and time.

b. Employees approved to access the ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action.

c. Such ALPR data may be released to other authorized and verified law enforcement officials and agencies for legitimate law enforcement purposes.

d. Every ALPR Detection Browsing Inquiry must be documented by the associated incident report number or a detailed reason for the inquiry.

K. ALPR Browsing Detection Audits

1. It is the responsibility of the Chief of Police or their designee to conduct an annual audit of the ALPR detection browsing inquiries, including an audit sampling of the ALPR system utilization from the previous 12 months to verify proper use in accordance with the authorized uses of the system. The audit shall randomly select a substantial sampling of the inquiries and determine if each inquiry meets the requirements established by policy.

L. Releasing ALPR Data

1. All non-law enforcement requests for access to stored ALPR data shall be processed in accordance with applicable law and FOIA procedures. The ALPR data may be shared with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law.

2. The procedure for such a request is as follows:

a. The agency making the request for the ALPR data includes the agency name, name of the requesting employee, the incident report related to the request and a synopsis of incident.

b. The request is reviewed by the approved designee, the Detective Sergeant.

c. The approved request shall be documented and retained on the City of Clawson's FOIA tracking system.

d. All non-law enforcement or non-prosecutorial agencies will be processed by the FOIA retention schedule and Michigan Law.

Coldwater Police Department
Standard Operating Procedures

SUBJECT **Automated License Plate Readers**			Order Number **604.1**
EFFECTIVE DATE January 26, 2024	DISTRIBUTION ☐ Patrol ☐ Records ☒ All	☒ NEW ☐ AMENDED ☐ REVISED ☐ REVIEWED	
ISSUED BY: Joseph Scheid, Director of Public Safety		☐ REPLACES: MLEAC STANDARDS: N/A	

I. PURPOSE

To establish guidelines for the use of Automated License Plate Readers (ALPR) by the Coldwater Police Department.

II. DEFINITIONS

A. Automated License Plate Reader – a camera system installed in public areas to collect license plate and vehicle information of passing traffic.

B. Hot List – a list of wanted vehicles and/or plates that will trigger a hit when the vehicle is captured on the ALPR system.

C. Official Use – any use related to an official department objective, such as an investigation, etc.

D. Personal Use – any use related to a personal objective, not related to a department objective.

E. Restricted Government Database – includes Michigan's Law Enforcement Information Network (LEIN), Michigan Secretary of State databases, the federal National Crime Information Center (NCIC), etc.

III. POLICY

It is the policy of the Coldwater Police Department to use ALPRs to provide objective leads for use in criminal investigations. ALPRs collect and store data, including images, related to license plates and vehicles. ALPRs shall only be installed in public areas, such as along the side of a street or highway. All data and images generated by the system are the property of the Coldwater Police Department, and is for the official use of this department. ALPR data may be shared with other law enforcement and/or prosecutorial agencies for official use, however ALPR data is exempt from public records requests.

IV. OPERATIONS

A. The ALPR system will automatically capture information regarding vehicles and license plates that pass by the ALPR. License plates are automatically run through law enforcement databases to identify stolen vehicles, wanted vehicles, stolen license plates, missing persons, felony warrants, etc.

B. Employees may enter a vehicle and / or plate information into the ALPR system as a “Custom Hot List.” The system will generate a hit if the vehicle is captured by the ALPR. Alerts from the Custom Hot List will only be received by CPD and Branch Central Dispatch personnel.

1. Vehicles and / or plates should not be entered into the hot list for minor violations such as civil infractions, license plate violations, insurance violations, driver’s license violations, misdemeanor warrants, civil process, or driving complaints called in to 9-1-1 by the public.

2. Employees shall complete a hot list entry / removal form to document the entry of a vehicle and / or license plate into the ALPR Hot List, or the removal from the list.

a. A supervisor must sign the form to approve the entry before submitting the information to the ALPR system. The supervisor will then enter the vehicle or plate into the custom hot list.

b. The Hot List entry / removal form will be kept on file in Records as long as the entry remains active in the Hot List.

c. Once the vehicle in the custom hot list has been stopped and / or apprehended, the officer making the stop shall alert a supervisor to have the vehicle removed from the custom hot list.

d. The supervisor removing the vehicle from the custom hot list shall sign the removal form and turn it in to records.

e. Records shall scan the hot list entry / removal form and attach it to the complaint in RMS.

C. Employees may search the ALPR database for investigative leads for any law enforcement purpose.

1. It should be routine practice to check the ALPR database for investigative leads for any of the following crimes with an unknown suspect committed in the vicinity of the ALPR unit: homicide, robbery, sexual assault, breaking and entering, UDAA, and hit and run traffic crashes involving serious injury or death.

2. Partial license plates or unique vehicle characteristics may also be searched in the ALPR database.

D. Hits generated by the ALPR system will be routed through Branch Central Dispatch, who will dispatch an officer to respond to the tip.

E. Hits will be limited to stolen plates, stolen vehicles, wanted persons, missing persons and missing children.

F. While responding to an ALPR generated hit, officers must validate information from an ALPR hit prior to making a traffic stop.

1. Officers must verify the hit via LEIN / NCIC to ensure the information is accurate.

2. Officers must verify the license plate and state on the suspect vehicle matches the hit.

3. Hits may relate to the vehicle, not necessarily the person driving the vehicle. For wanted persons, officers must corroborate the physical description contained on the warrant entry with the operator and occupants of the vehicle to establish reasonable cause to make a traffic stop, or have another legal basis for the stop.

G. Damage to the ALPR system shall be reported to the Deputy Chief via e-mail by the end of the officer's shift.

V. DATA RETENTION

A. ALPR data shall be purged from the system in accordance with Michigan Records Retention Schedule 11, unless it is associated with an investigation.

1. Schedule 11, section 11.061, requires ALPR data to be retained for the date of creation plus 1 year.

2. The ALPR system shall be configured to automatically purge all data 366 days from the time it was captured unless it has been flagged as evidence.

B. Employees must download data that is related to a case and forward it to the property manager as evidence to be stored on the evidence server.

1. Data that is evidence may be purged in accordance with the evidence disposition rules found in SOP 403.1 Evidence and Property Documentation, or 366 days from the date of creation, whichever is later.

C. Employees should download a pdf report from the ALPR system when this data is used to help identify and apprehend a suspect. Print one copy of the file and send it to the PA's Office with a warrant request. E-mail the pdf file to the Property Manager to be uploaded to the complaint in RMS.

VI. ACCESS TO ALPR DATA

A. Access to the ALPR system is restricted to those who have completed training and have been issued username and password credentials.

B. Access to the ALPR system is restricted to official use only. Personal use of the ALPR system or data is prohibited.

1. Employees searching the ALPR data are required to sign on using their own name and enter a complaint number into the "reason" field in the search form to access ALPR data.

C. ALPR data may be shared with prosecuting officials as needed.

D. ALPR data may be shared with other law enforcement agencies for official use only.

E. Employees searching the ALPR data on behalf of another agency shall obtain an Assist Other Agency (AOA) non-criminal complaint number from dispatch.

1. The employee drawing the AOA shall document the requesting official's name, department, complaint number and reason for the search in the report narrative.

2. When accessing ALPR data for another agency, the employee should enter our AOA number in the flock system “Reason” field.

F. ALPR images may not be released to the media or social media without prior approval of the Director or Deputy Chief of Police.

VII. TRAINING

A. An employee must complete the approved training on the ALPR system before they may use it.

B. New officers shall receive approved training on the ALPR during their FTO period.

C. Completed training shall be documented on a department training form and submitted to Records.

VIII. DATA PROTECTION

A. The ALPR system will be installed and maintained by a third-party vendor, Flock Safety.

B. The Coldwater Police Department is the owner of all data generated by the CPD ALPR system.

C. Flock Safety shall collect and store ALPR data using a secure network. Data shall be encrypted at rest.

D. Computer protocols will be utilized to comply with data retention and purging in accordance with this policy.

IX. QUARTERLY AUDIT

A. The Lieutenant, or designee, shall conduct an audit of the LPR system usage on a quarterly basis.

B. The audit shall include:

1. Only authorized CPD employees who have completed training have access to the department’s ALPR system.

2. The system is being used only for official business, and each search includes a case number.

3. Any hot list entries are made for official business, and each hot list entry includes a case number and reason for the stop.

C. The Lieutenant, or designee, shall report the results of the quarterly audit in writing to the Deputy Chief of Police.

X. USER ROLES

A. Access to the Flock system will be determined by user roles.

B. Administrator – An Administrator has full access to the system, to include the ability to add or remove user accounts and edit agency wide settings.

C. Supervisor – A supervisor has access to search and lookup and may receive hotlist alerts. A Supervisor may also add or remove vehicles on the department's custom hot list.

D. Patrol – Patrol level access (applies to patrol and records staff) allows access to search and lookup and to receive custom hotlist alerts.

E. Central Dispatch and MDT – Users with this level of access may only receive hot list alerts, they may not access search or lookup.

XI. CUSTOM HOT LIST

A. The department will maintain only one custom hot list, which will send alerts to all users and Central Dispatch.

B. A supervisor may enter a vehicle into the custom hot list, or remove a vehicle from the custom hot list.

1. Any officer may request a vehicle be added to the Custom Hotlist by completing the Hotlist Entry / Removal form and submitting it to a supervisor.

2. The supervisor will review the form to determine if placing the vehicle on the custom hotlist is appropriate under the circumstances. The hot list is only to be used for vehicles that need to be stopped, or to alert officers of a potential crime in progress.

a. An example would be a vehicle associated with crime such as a catalytic convertor theft. The alert would trigger officers to check our local car dealerships and repair shops to attempt to catch the suspect in the act.

b. Another example would be a vehicle associated with a commercial B&E. The alert would trigger officers to check similar establishments locally to attempt to catch the suspect in the act.

c. A custom hotlist entry should not be used to simply track a suspect. The search and lookup tools are more appropriate options.

3. After entry into the hotlist, the supervisor shall forward the form to Records, where it will be filed until the vehicle is located and removed from the hotlist.

4. When the vehicle has been stopped, the supervisor will update the Entry / Removal form and will remove the vehicle from the Custom Hot List in the Flock system.

5. The supervisor will forward the completed form to records to be scanned and attached to the case in RMS.

XII. DOCUMENTING RESULTS

A. An officer making a traffic stop or arrest based off of an ALPR alert, search, or lookup shall use the “Outcomes” tab document the incident. The outcomes tab is the small icon shaped like a hand at the bottom of the alert or search result.

B. An officer shall document a stop or arrest based on an ALPR alert, search, or lookup in the narrative of this incident or supplemental report.

XIII. DEVICES

A. The Flock system may be accessed in the following ways: Windows App, internet website, smartphone app, e-mail and text message.

1. City owned computers will have the Windows App, City owned cell phones will have the Flock App and text messaging turned on. All users will have the ability to receive alerts via their city e-mail account.

2. Employees are discouraged from using their personal devices to receive alert text messages, to use the Flock app, or to access the Flock website. Use of personal devices for this work purpose may open your phone up to FOIA and Discovery orders. That means ALL of the personal data on your phone, to include text messages, call logs, location data, browser history, apps, etc. would be subject to scrutiny by the courts, defense attorneys, or the general public.

B. Employees will have access to the flock system at work through city owned hardware, and through radio dispatch by Central Dispatch. There is no reason to access the system through a personally owned device.

Dallas Fusion Center - Real Time Crime Center

Standard Operating Procedure

900 – Flock Safety Cameras Policy

901 - Flock Safety Cameras

Purpose

- Flock cameras are a fixed pole-mounted license plate reader camera system. This system captures the rear image of a vehicle and the vehicle's license plate number. The system searches the national wanted database for stolen vehicle information or national alerts. Flock technology lets you search by vehicle make, color, type, license plate, state of the license plate, missing plate, covered plate, paper plate, and unique vehicle details. National alerts include the AMBER alert for taken children, the SILVER alert for missing senior citizens, and the BLUE alert for threats to law enforcement.

902 - Procedures

- Set Flock alerts on the website: https://hotlist.flocksafety.com/patrol

    a. keep the website open on your browser for the duration of the shift.

- Audible Flock Alert

    a. Confirm the hit validity – make sure the picture matches the stolen vehicle information.

    b. Run the plate in Mobile CAD or CRIMES to confirm the vehicle is stolen.

- Give Flock hit notification to Patrol

    a. Set the radio on the channel of the hit

    b. Call on the radio: "Fusion on [Channel] – is the radio clear?

        i. If the radio is clear, give the dispatcher the type of Flock hit, location, direction of travel, vehicle description, license plate number, and possible additional details (tinted windows, sticker on the tailgate, damage on the vehicle, items in the truck bed.)

    c. CAD message – if radio traffic doesn't allow callout on the channel,

        i. Message to the entire channel (example: CH2 -NORTHEAST PATROL (Sector)).
        ii. Add the above details to the message field and send.

iii. if the vehicle was stolen in a robbery, notify the channel immediately on the radio and repeat the location and vehicle details if necessary.

- Monitor Incident Response
    a. if a call is generated and elements are added, send Ros an email with the picture of the Flock hit. Send the information to any new elements that are added, including AIR1. Inform the Ros over the radio you have sent a picture if traffic is clear.
    b. monitor radio traffic and the call sheet for updates and additional information.
- Logging the Flock hit
    a. Log Flock hit in the Fusion Flock Hit Tracker, located in TEAMS folder "Fusion Logs"
    b. Add
        i. Date and callout time (not the time of the hit)
        ii. Division
        iii. License Plate and State
        iv. Vehicle color, make, and model
        v. Incident number if a call sheet was created
        vi. Offense type
        vii. Your badge/employee number
        viii. OCA (can be found in the Stolen vehicle bolo in CAD when the plate is searched)
        ix. Add recovery and arrest if applicable with a letter Y
- **DO NOT ADD ANYTHING IF NO RECOVERY OR NO ARREST IS MADE**.
- At the end of your shift, make sure no information is missing from columns b1-9
    a. Update Flock hit Tracker with case number if applicable and not recovery and/or arrest
- Log Flock activation in Fusion Activity Log

FRASER DEPARTMENT OF PUBLIC SAFETY
Automated License Plate Readers

NO. 5.28

TO: All Members of the Department

FROM: Director Samantha Kretzschmar

DATE OF ISSUE: June 28, 2024

RESCINDS/AMENDS: NEW POLICY

POLICY

It is the policy of the Fraser Department of Public Safety to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public. The data and images gathered provide information and investigative resources to employees. The use and access of such systems and information shall be for law enforcement purposes only and in compliance with all applicable training, policies, procedures, rules, regulations and laws.

I. DEFINITIONS

A. ***Automated License Plate Reader (ALPR):*** System equipment consisting of cameras, computers and computer software used to automatically recognize and interpret the characters on motor vehicle license plates. Digital images captured by the cameras are converted into data, which is passed through the ALPR system.

B. ***Hot List:*** A list of license plates associated with vehicles of interest compiled from one or more databases including, but not limited to: National Crime Information Center (NCIC), Michigan Secretary of State, local BOLOs, etc.

C. ***Vehicles of Interest:*** Vehicles including, but not limited to, vehicles which are reported as stolen, display stolen plates or tags, are linked to missing and/or wanted persons, and vehicles flagged by the Secretary of State or other law enforcement agencies.

D. ***Hit***: An alert from the ALPR system that a scanned license plate number may be in the NCIC or other law enforcement database for a specific reason such as, but not limited to: stolen car, wanted and/or missing person, terrorist related activity, and AMBER alerts.

E. ***ALPR Administrator***: The Director's designee(s) serves as the ALPR

Administrator for the department.

II. PROCEDURES

A. Training:

1. No member of the Fraser Department of Public Safety shall access ALPR data without first completing department approved training.

2. ALPR administration shall be responsible for planning and implementing all department approved training concerning the ALPR.

B. Automated License Plate Reader Confidentiality:

1. Use of the ALPR system, software, associated databases, and data is restricted exclusively to the department's law enforcement functions. Information obtained from the ALPR, software, associated databases, and data shall not be used for personal reasons or for reasons inconsistent with the department's law enforcement functions under any circumstances.

2. Misuse or abuse of the ALPR system, software, associated databases, or data may be subject to criminal prosecution, civil liability, and/or administrative sanctions, up to and including termination, pursuant to and consistent with the relevant collective bargaining agreements and department policies.

3. Information obtained from the ALPR system, software, associated databases, and data shall not be disseminated to the public except as authorized by law.

4. Information obtained from the ALPR system, software, associated databases, and data may be disseminated to other law enforcement agencies or officers when it is to be used for law enforcement related functions, providing all of the following criteria are met:

    a. The law enforcement agency makes an official written request for the ALPR data through LEIN or via department email.
    b. The agency's identity, the person requesting the data, and the intended purpose must be documented in such a manner as to demonstrate compliance with this policy and retained on file with the vendor's software.
    c. A supervisor must approve the request.

C. Automated License Plate Reader Use:

1. The ALPR system, software, associated databases, and data may be used in conjunction with any routine patrol operation or criminal investigation. Reasonable suspicion or probable cause is not required before using an ALPR.

2. Officers shall be aware the ALPR system will not have access to real time data. Hot lists, NCIC, LEIN, etc. are updated on a regular basis, but not continually, therefore there may be a delay in entries and removals.

3. Upon receiving an alert, officers should verify the plate and the state of issuance match the hot list alert in the ALPR system.

4. Upon locating the vehicle officers shall visually verify that the license plate on the vehicle matches that of the image captured by the ALPR and the LEIN/NCIC check before proceeding with any investigative or enforcement action.

5. **Officers are reminded that they must have a legal articulable set of facts to take action; alert from an ALPR alone shall not be the basis for police action.**

D. Restrictions of Automated License Plate Reader Use:

1. The ALPR system shall only be used for official and legitimate law enforcement purposes. Only sworn police personnel shall have access to the ALPR system.

2. Invasion of Privacy: Except when done pursuant to a court order such as a search warrant, it is a violation of this policy to utilize the ALPR to record license plates on private property. The exception is license plates on private property that are exposed to public view.

3. Harassment or Intimidation: It is a violation of this policy to use the ALPR system to harass and/or intimidate any individual or group.

4. Personal Use: It is a violation of this policy to use the ALPR system for any personal purpose.

V. RESPONSIBILITY

A. Automated License Plate Reader Administration:

1. The Director of Public Safety or designee is responsible for administrative oversight of the ALPR system operations and shall be responsible for the following:
   a) Ensuring access, collection, secure storage, and retention of ALPR data and associated media files are within policy guidelines.
   b) Ensuring ALPR reads and alerts or hits that are acted upon in the field or associated with arrests, investigations, and/or prosecutions are documented in the vendor's database.
   c) Ensuring that ALPR system audits are conducted on an annual basis. System audits shall be designed to ensure the integrity of data captured, stored, and/or retained and shall include a review of password security and system usage.
   d) Ensuring that each employee who uses or has access to the ALPR system has completed department approved training and is certified to have access to the Law Enforcement Information Network (LEIN).

2. ALPR system repairs (hardware or software) shall be made by the current ALPR system vendor or a vendor approved by the Director.

B. Data Retention and Accountability:

1. All ALPR data will be stored on the current Vendor's server for a period of thirty (30) days. After thirty days the data shall be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a lawful action or order to produce records. In such circumstances, the applicable data shall be transferred to another digital media and stored according to current procedures.
2. All saved data shall be closely safeguarded and protected by both procedural and technological means. The Department will observe the following safeguards regarding access to and use of stored data:

   a. All requests for access to historical ALPR data shall be logged in the ALPR system and the reason for the access must be recorded. The appropriate Fraser Department of Public Safety case or incident number shall be documented in the request.

b. All ALPR data downloaded to a mobile workstation shall be accessible only through a login/password protected system capable of documenting all access of information by name, date, and time.

C. Administrative Audits:

1. It is the responsibility of the Director of Public Safety to ensure that an audit is conducted of ALPR detection browsing inquiries at least once during each calendar year. The Fraser Department of Public Safety will audit a sampling of the ALPR system utilization from the prior twelve (12) month period to verify proper use in accordance with this policy. The audit shall randomly select at least ten (10) detection browsing inquiries conducted by Fraser Department of Public Safety employees during the time period selected to determine if each meets the requirements of this General Order.

2. The audit shall be performed and documented by the ALPR Administrator in the form of a Memorandum to the Director of Public Safety. The memorandum shall include any data errors found so that such errors can be corrected. After review by the Director, the memorandum and any associated documentation shall be filed in accordance with current Michigan State Police record retention policy.

ISSUED AND APPROVED



Samantha Kretzschmar
Director Public Safety

GRAND TRAVERSE COUNTY SHERIFF'S OFFICE
POLICY AND PROCEDURE

SUBJECT: **AUTOMATED LICENSE PLATE READERS (ALPR) / FLOCK SAFETY CAMERA SYSTEM (FSC)**

EFFECTIVE DATE: July 5, 2023

PREVIOUS ISSUES:

I. POLICY AND PURPOSE

It is the policy and purpose of the Grand Traverse County Sheriff's Office to utilize Vehicle Identification/Automated License Place Reader technology, specifically the Flock Safety Camera System (FSC), while recognizing the established privacy rights of the public. The data and images gathered provide information and investigative resources to employees. The use and access of such information shall be for law enforcement purposes only and in compliance with all applicable training, policies, procedures, rules, regulations, and laws.

II. ADMINISTRATION

Administration of the FSC System shall be the responsibility of the Investigative Services Division Captain. The administrator may assign select individuals to have administrative access for the purposes of account management, such as adding cameras, integrations, etc.

III. DEFINITIONS

A. ALPR: Automated License Plate Recognition

B. FSC: Flock Safety Camera System

C. Hot List: A list of license plates or identifiers associated with vehicles of interest compiled from databases including, but not limited to: National Crime Information Center (NCIC), Amber Alerts, Law Enforcement Agencies, etc.

D. Vehicles of Interest: Vehicles including, but not limited to, vehicles which are reported as stolen, display stolen plates, are linked to missing/endangered and/or wanted persons, or are linked to criminal or public safety investigations of this agency or other Law Enforcement agencies.

E. Hit: An alert from the FSC that a scanned license plate number or identifier matches an entry from a Hot List.

F. ALPR Administrator: The Investigative Services Division Captain.

IV. PROCEDURES

A. Training:

1. No member of the Grand Traverse County Sheriff's Office shall access FSC data without first completing departmental approved training. The FSC administrator(s) shall be responsible for planning and implementing all approved training concerning the FSC system.

2. The FSC Administrator shall be responsible for planning and implementing all approved training.

B. FSC/Automated License Plate Reader Confidentiality:

1. Use of the FSC system, software, associated databases, and data is restricted exclusively to Grand Traverse County Sheriff's Office law enforcement functions. Information obtained from the ALPR, software, associated databases, and data shall not be used for personal reasons or for reasons inconsistent with law enforcement functions.

2. Misuse or abuse of the FSC system, software, associated databases, or data may be subject to administrative sanctions, up to and including termination, pursuant to and consistent with the relevant collective bargaining agreements and department policies.

3. Information obtained from the ALPR system, software, associated databases, and data shall not be disseminated to the public except as authorized by law.

4. Information obtained from the ALPR system, software, associated databases, and data may be disseminated to other law enforcement agencies or officers when it is to be used for law enforcement related functions.

C. Automated License Plate Reader Use:

1. The ALPR system, software, associated databases, and data may be used in conjunction with any legitimate investigation.

2. Officers should be aware the ALPR system will not have access to real time data. Hot lists, NCIC, LEIN, etc. are updated on a regular basis, but not continually, therefore there may be a delay in entries and removals.

3. Upon receiving an alert, officers should verify the plate and the state of issuance match the hot list alert in the ALPR system.

4. Officers should then conduct a check of the plate in question in LEIN/NCIC to verify the entry.

5. Upon locating the vehicle, officers shall visually verify that the license plate on the vehicle matches that of the image captured by the ALPR and the LEIN/NCIC check before proceeding with any investigative or enforcement action.

6. Officers approved by the ALPR Administrator to access and enter Hot List information will be responsible for the entry, monitoring and removal of the Hot List information.

D. Restrictions of Automated License Plate Reader Use:

1. The ALPR system shall only be used for official and legitimate law enforcement purposes. The administrator shall determine what level of access those permitted use of the system will have.

2. Harassment or Intimidation: It is a violation of this policy to use the ALPR system to harass and/or intimidate any individual or group.

3. Personal Use: It is a violation of this policy to use the ALPR system for any personal purpose.

V. RESPONSIBILITY

A. Automated License Plate Reader Administration:

1. The ALPR administrator is responsible for administrative oversight of the ALPR system operations and shall be responsible for the following:

   a. Ensuring access, collection, secure storage, and retention of ALPR data and associated media files are within policy guidelines.
   b. Ensuring that ALPR system audits are conducted on a semi-annual basis. System audits shall be designed to ensure the integrity of data captured, stored, and/or retained and shall include a review of password security and system usage.
   c. Ensuring that each employee who uses or has access to the ALPR system has completed department approved training and is certified to have access to the Law Enforcement Information Network (LEIN).

2. ALPR system repairs (hardware or software) shall be made by the current ALPR system vendor.

B. Data Retention and Accountability:

1. All ALPR data will be stored on the current vendor's server for a period of thirty (30) days. After thirty days the data shall be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a lawful action or order to produce records. In such circumstances, the applicable data shall be transferred to another digital media and stored according to current procedures.

2. All saved data shall be closely safeguarded and protected by both procedural and technological means. The department will observe the following safeguards regarding access to and use of stored data:

   a. All requests for access to historical ALPR data shall be logged in the ALPR system and the reason for the access must be recorded. The appropriate Grand Traverse County Sheriff's Office case or incident number shall be documented in the request.

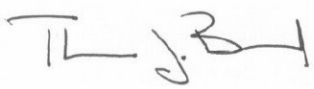
b. All ALPR data downloaded to a mobile workstation shall be accessible only through a login/password protected system capable of documenting all access of information by name, date, and time.

C. Administrative Audits:

1. It is the responsibility of the Investigative Services Division Captain to ensure that an audit is conducted of ALPR detection browsing inquires at least twice during each calendar year. The administrator will audit a sampling of the ALPR system utilization to verify proper use in accordance with this Policy. The audit shall randomly select detection browsing inquiries conducted by employees during the time period selected to determine if each meets the requirements of this Policy.

2. The ALPR Administrator will be responsible for the preparation, review and sharing of reports at the request of any entities (i.e., Townships, etc.) that have established agreements related to the Flock Safety Camera System.

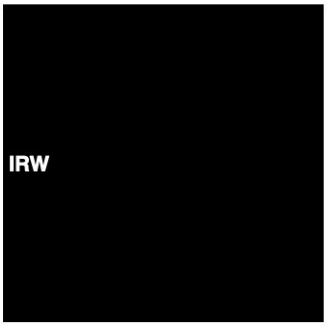
3. The audit shall be performed and documented by the ALPR Administrator in the form of a memorandum to the Sheriff. The memorandum shall include any data errors found so that such errors can be corrected. After review by the Sheriff, the memorandum and any associated documentation shall be filed in accordance with the record retention policy.



_____

Thomas J. Bensley, Sheriff

Part of this project is measuring the use. The attached link and QR code must be used if the ALPR system is utilized to solve a crime, make an arrest, or locate a missing person.



Microsoft Forms (outlook.com)

	GROSSE ILE POLICE DEPARTMENT POLICY AND PROCEDURE	**Distribution** ALL PERSONNEL	**General Order Number** **10.12**
		Original Issue Date 1/30/2024	**Reissue/Effective Date** 1/30/2024
Order Title: COMMUNITY SAFETY AND CRIME PREVENTION CAMERA SYSTEM		**Accreditation Standard:** 1.6.1	**Section** 10
		Rescinds: N/A	
Section Title: SUPPORT AND TECHNICAL SERVICES		**Douglas I. Carmack, Chief of Police**	

This General Order is for departmental use only and does not apply in any criminal or civil proceeding. This General Order should not be construed as creation of a higher legal standard of safety or care in an evidentiary sense with respect to third party claims. Violations of this General Order will only form the basis for departmental administrative sanctions. Violations of law will form the basis for civil and criminal sanctions in a recognized judicial setting

I. PURPOSE

To establish guidelines on the proper use of the crime prevention license-plate-recognition system (LPR), also known as the Flock Safety Camera System (FSC), to ensure the protection of the Constitutional and privacy rights of the public while allowing the Grosse Ile Police Department to enhance public safety, deter criminal behavior and assist in criminal investigations and prosecutions utilizing FSC system.

II. DEFINITIONS

Alert: A visual and/or auditory notice that is triggered when the FSC system receives a potential "hit" on a license plate

Fixed FSC system: FSC cameras that are permanently affixed to a structure, such as a pole, traffic barrier, or a bridge.

Hit: A read matched to a plate within public view that has been registered on the agency's "Hot Lists" 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.

Hot Lists: License plate or vehicle information of stolen cars, vehicles owned or known to be operated by wanted persons or persons of interest, and vehicles associated with criminal activity or safety alerts, such as Amber or Silver alerts.

Hot List Form: A custom document intended for requesting entry/removal of vehicles from the FSC system as well as tracking and maintaining the Department's Hot List / Saved Search files.

(See Appendix A or https://powerdms.com/link/GROSSEILE/document/?id=1276664)

III. POLICY

A. Flock Safety Camera Function

1. Fixed FSC system is a passive license-plate-recognition system; live data is not viewed.
2. Fixed FSC systems monitors all license plates that come in view of the FSC cameras.

3. The Fixed FSC system provides the ability to search historical data. A log of such requests will be maintained and monitored by the LPR Coordinator.
4. Fixed FSC systems provides the ability to notify the system administrator and/or other police personnel of a "hit" from the LPR system "Hot List."

B. Authorized Uses and Users

1. FSC systems, FSC data and associated media are the property of the Grosse Ile Police Department and are to be used only in conducting the agency's official business.
2. Only trained, LEIN certified, law enforcement staff or dispatchers may access or search FSC systems, FSC data, and associated media.
3. The use of FSC system's associated equipment and databases are restricted to public safety-related missions of this agency and are authorized for officer/public safety purposes only.
4. Except when done pursuant to a court order, such as a search warrant, the FSC may be used only to record license plates of vehicles that are exposed to public view (e.g., vehicles 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).
5. Each FSC user must have and utilize a unique log-in for the FSC system.

C. FSC Data Sharing and Dissemination

1. FSC data should be considered for official use only and can only be shared for legitimate law-enforcement purposes.
2. Outside law-enforcement agencies that are part of the FSC network may be allowed search access for legitimate law enforcement purposes. Command approval for each agency is required.
3. Trained GIPD personnel may conduct searches of the FSC database for outside law-enforcement agencies. GIPD member conducting the search will enter the last name of the GIPD member authorizing the search, the requestor's and requesting agency's name, the agency's case number, and incident type in the reason for search field (e.g., Smith, Trenton PD Jones, 22-XXXX, Robbery). Only matching returns will be shared with the agency.
4. Outside law-enforcement agencies requesting to receive alerts of hits from the FSC system must have a mutual aid agreement, letter of understanding, or other agreement in place with GIPD. If the agency does not, or if the supervisor hearing the request is unsure, the requesting agency must submit the request via LEIN message to the GIPD, indicating the reason for the request. If the on-duty shift supervisor deems the reason provided to be for legitimate law-enforcement purposes, he/she may approve the request for immediate entry or may submit a request for entry to the LPR Coordinator. All entries, or requests for entry, shall be documented on the Hot List Entry form and forwarded to the LPR Coordinator (Detective Bureau).

D. Retention and Release of FSC Related Photos and Data

1. FSC related data is stored for a maximum of 30 days.
2. FSC data that is potential evidence must be transferred to and retained in the department's digital evidence storage system by the Detective Bureau. Transferred / Stored data will be retained in accordance with State law and Policy 10.08.
3. Freedom of Information Act requests for the release of data or photos related to the FSC are governed by applicable law and Policy 10.09. Requests that relate to travel history of individual

vehicles shall be considered an unwarranted invasion of individual privacy and denied under the Freedom of Information Act. However, if the requestor expresses a public interest exemption to the restriction, the Chief of Police, or designee, shall evaluate the request on a case-by-case basis and may authorize the release of information.

IV. PROCEDURE

A. Field Operations and Enforcement Actions

1. All searches of the FSC system shall include last name of the person conducting or requesting the search, the case /CAD number and type of incident (e.g., Smith, 22-XXXX Robbery). Searches related to broadcasts by other agencies that do not have a Grosse Ile case/CAD number, such as suspected drivers or vehicles wanted by other jurisdictions, will include the person conducting or authorizing the search, the word "Broadcast," and the reason (e.g., Smith, Broadcast – TRPD Shooting Suspect Vehicle).
2. One member of the Detective Bureau shall be designated as the LPR Coordinator, with a second detective acting as the Alternate LPR Coordinator.
3. FSC users will not take enforcement action based solely on the following LEIN/NCIC notifications: Supervised Release, Protection Order, Violent Person Advisory, Immigration Violator, or Sex Offender.
4. Custom Hot Lists that alert the entire organization or portions of the organization must be authorized by a detective or command officer unless circumstances dictate a need for immediate entry.
5. The Hot List Form must be completed to initiate entry into the FSC system. When there is a need for immediate entry, for crimes in progress or just occurred, the shift supervisor may authorize the Hot List entry, however the Hot List Form must still be completed by the shift supervisor and forwarded to the Detective Bureau.
6. The Detective Bureau LPR Coordinator / Alternate LPR Coordinator will be responsible for entry, removal, and maintaining of the custom Hot List information.
7. When notified of a NCIC "hit" from the FSC system, officers shall verify the FSC response through the Law Enforcement Information Network (LEIN) before taking enforcement action (note: the FSC system automatically updates every 45-minutes).
8. Occasionally, there may be errors in the FSC system's read of a license plate. Therefore, prior to initiation of a stop of a vehicle or other intervention based on an alert, officers shall undertake the following;
    a. 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 FSC; including both the alphanumeric characters of the license plate, state of issue, and vehicle descriptors before proceeding.
    b. Verification of a status on a Hot List: An officer must confirm that the vehicle is still stolen, wanted, or otherwise of interest before proceeding (absent exigent circumstances). Without confirmation, a vehicle cannot be stopped solely on a FSC alert.
    c. Wanted Individuals: Because the FSC alert relates to a vehicle and/or license plate and may not relate to the person operating the vehicle, officers need reasonable suspicion and/or probable cause to make an enforcement stop of any vehicle (for example, if a vehicle is entered into the system because of its association with a wanted suspect, officers shall attempt to visually match the occupant to the description of the wanted subject associated to the vehicle or BOL prior to making a stop or should have another legal basis for making the stop).

9. After the stop of a vehicle or other intervention based on the alert:
    a. The officer will notify the shift supervisor of the positive hit and request that the plate be removed from the Hot List, unless the interest in the vehicle still exists.
    b. If the vehicle is to be removed from the Hot List, the shift supervisor shall ensure the vehicle is removed and the custom Hot List Form is completed and forwarded to the Detective Bureau.

B. The following uses of the FSC system are prohibited:

1. Use the FSC 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.
2. Use the FSC system or associated scan files or Hot Lists for any personal purpose.
3. The FSC system will not have an audio recording feature, nor shall modifications be made to the system to allow audio recording.
4. The FSC shall not be utilized by off-duty personnel.

C. Administration

1. The Deputy Chief, or his/her designee, shall have administrative oversight for the FSC system deployment and operations. This individual is responsible for the following;
    a. Ensuring that all laws and protocols established in this policy for the use of the FSC system are adhered to.
    b. An audit of the Hotlist / Saved Search files at least once per calendar year to ensure adherence to entry and removal criteria and procedures.
    c. That all users have individual credentials for access and use of the systems and/or data.
    d. Modifying protocols for the entry, collection, storage, and retention of FSC data and associated media files based on evolving system capabilities, legal updates and discovered issues or best practices.
2. The Detective Bureau LPR Coordinator / Alternate Coordinator is responsible for the functionality of the equipment and shall check the equipment on a regular basis to ensure both functionality and camera alignment. Any equipment that falls outside of expected functionality shall be reported immediately to Flock Safety.
3. FSC system repairs, hardware, or software, shall be made by technicians through Flock Safety.

Appendix A

FLOCK SAFETY CAMERA HOT LIST ENTRY FORM

- ☐ Request Entry onto Hot List
- ☐ Request Entry as Saved Search
- ☐ Request Removal from Hot List / Saved Search
- ☐ Immediate Entry Notification (Date / Time Entered: _____)
- ☐ Removal Notification (Date / Time Removed: _____)

For Hotlist Entry:

Complaint Number: _____ Incident Type: _____

Reason to add to Hot List: _____

_____

_____

_____

- ☐ Investigative Purposes ONLY (provide specifics above)
- ☐ Probable Cause for stop/arrest or warrant information_____

_____

_____

- ☐ Notify - Name: _____ Contact # _____

Plate: _____ State: _____

Hot List Entry Expiration (total hours or date): _____

For Saved Search:

Vehicle Type: _____

License Plate Type: Regular Plate _____ or Temporary Plate _____

Vehicle Make: _____

Vehicle Color: _____

Start Time_____ End Time _____

Requested by / Authorized by (Must be Detective / Shift Supervisor / Command staff to authorize):

_____ **Date:** _____

FOR OFFICE STAFF:

Entered date: _____ Removed date: _____

Reason for removal: _____

HOLLAND DEPARTMENT OF PUBLIC SAFETY
POLICE SERVICES
POLICY & PROCEDURES

Section F | **Community Safety and Crime Prevention Camera System** | **No. 6**

1. Purpose

a. Provide guidelines on the proper use of the Crime Prevention license plate recognition (LPR) system, also commonly known as the Flock Safety Camera (FSC) System.

b. Provide governmental accountability by ensuring the FSC system use respects constitutional and privacy rights.

c. Deter criminal behavior and assist in criminal investigations and prosecutions.

d. Allow for appropriate cooperation with businesses, institutions, condominium associations, homeowner associations, neighborhood associations, and other entities or groups seeking safety and security for specifically identified property.

e. Enhance the department's productivity and effectiveness, while enhancing community and officer safety with the use of the FSC systems.

2. Definitions

a. Alert – A visual and/or auditory notice that is triggered when the FSC system receives a potential "hit" on a license plate

b. Fixed FSC system – FSC cameras that are permanently affixed to a structure, such as a pole, traffic barrier, or a bridge.

c. Hit – A read matched to a plate within public view that has been registered on the agency's "hot lists" 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.

d. Hot Lists – License plate information 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. Departments of motor vehicles can provide lists of expired registration tags, and law enforcement agencies can interface their own locally compiled custom hot lists to the FSC system.
These lists serve as an officer safety function as well as for investigative purposes. In addition to agency supported hot lists, designated 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 FSC system.

e. FSC – Flock Safety Camera System

f. Read – Digital images of license plates, vehicles, and associated metadata (e.g., date, time, and geographic coordinates associated with the vehicle image capture) that are captured by the FSC system.

3. Procedure

a. The City of Holland FSC system will not have an audio recording feature, nor shall modifications be made to the system to allow audio recording.

b. Authorized Uses and Users
- FSC systems, FSC data and associated media are the property of the Holland Department of Public Safety and are to be used only in conducting the agency's official business.
- Only trained LEIN certified law enforcement staff or dispatchers may access or search FSC systems, FSC data, and associated media.
- The use of FSC systems associated equipment and databases are restricted to public safety-related missions of this agency, and are authorized for officer public safety purposes only.
- Except when done pursuant to a court order such as a search warrant, the FSC may be used only to record license plates of vehicles that are exposed to public view (e.g., vehicles 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).

c. The following uses of the FSC system are prohibited:
- Use the FSC 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.
- Use the FSC system or associated scan files or hot lists for any personal purpose.

d. Administration
- The Chief of Public Safety (or that individual's designee) shall designate an employee(s) with administrative oversight (The Administrator) for FSC system deployment and operations who is responsible for the following;
  - Establishing protocols for access. To ensure proper operation and facilitate oversight of the FSC 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.
  - Establishing protocols for the entry, collection, storage, and retention of FSC data and associated media files.
  - Authorizing any requests for FSC systems use of data access according to the policies and guidelines of this agency.
- 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 Flock Safety.
- FSC system repairs, hardware, or software, shall be made by technicians through Flock Safety.

e. Fixed Flock Safety Camera Systems (FSC) Usage
   - Fixed FSC system is a passive system, live data is not viewed.
   - Fixed FSC systems monitors all license plates that come in the FSC camera's view.
   - The Fixed FSC system provides the ability to search historical data. A log of such requests will be maintained by the system administrator.
   - All searches of the FSC system shall include a reason for the search, to include the case /CAD number and type of incident (e.g., 22-XXXX Robbery). Searches related to broadcasts by dispatch that do not have a case/CAD number, such as suspected drivers or vehicles wanted by other jurisdictions, will include "Broadcast" and the reason (e.g., Broadcast – GRPD Shooting Suspect Vehicle).
   - Fixed FSC systems may have the ability to notify the system administrator and/or other police personnel of a "hit" from the LPR system "hot list."

f. Field Operations and Enforcement Actions
   - All users of the FSC system will *unselect* the following: Supervised Release, Protection Order, Violent Person, Immigration Violator, Sex Offender under the NCIC notification reasons and will not take any enforcement action if the FSC system alerts solely for these reasons.
   - Custom hotlists that alert the entire organization or portions of the organization must be authorized by a detective, sergeant, or command officer.
   - The custom hotlist form (attached) must be completed to initiate entry into the FSC system. When there is a need for immediate entry by the OCCDA dispatch supervisor for serious crimes in progress or just occurred, the hotlist form must still be completed and forwarded to the Investigative Division Assistant.
   - The Investigative Division Assistant will be responsible for entry, removal, and auditing of the custom hotlist information.
   - When notified of a NCIC "hit" from the FSC system, officers shall verify the FSC response through the Law Enforcement Information Network (LEIN) before taking enforcement action. Action shall not be based solely on the FSC alert.
   - Occasionally, there may be errors in the FSC system's read of a license plate. Therefore, an alert alone is not a basis for police action.
   - Prior to initiation of a stop of a vehicle or other intervention based on an alert, officers shall undertake the following;
     - Verification of a status on a hot list. An officer must confirm that the vehicle is still stolen, wanted, or otherwise of interest before proceeding (absent exigent circumstances). Without confirmation, a vehicle cannot be stopped solely on a FSC alert and there must be a legal justification for the stop, such as a traffic violation, reasonable suspicion or probable cause.
     - 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 FSC, including both the alphanumeric characters of the license plate, state of issue, and vehicle descriptors before proceeding.
     - Because the FSC alert relates to a vehicle plate and may not relate to the person operating the vehicle, officers need reasonable suspicion and/or probable cause to make an enforcement stop of any vehicle (for example, if a vehicle is entered into the system because of its association with a wanted individual, officers shall attempt to visually match the occupant to the description of the wanted subject associated to the vehicle plate or BOL prior to making a stop or should have another legal basis for making the stop).
   - After the stop of a vehicle or other intervention based on the alert:

- The officer will notify the dispatch supervisor of the positive hit and request that the plate be removed from the hot list, unless the interest in the vehicle still exists.
- The officer will also notify the Investigative Division Assistant of the removal via department e-mail or voicemail.

g. FSC Data Sharing and Dissemination

FSC data should be considered for official use only and can only be shared for legitimate law enforcement purposes.

- Outside law enforcement agencies that are part of the FSC network may be allowed search access for legitimate law enforcement purposes. Command approval for each agency is required.
- Trained HDPS personnel may conduct searches of the FSC database for outside law enforcement agencies. HDPS Personnel will enter the requesting agency's name, the agency's case number, and incident type in the reason for search field (i.e. OCSD 22-XXXX Robbery). Only matching returns will be shared with the agency.
- Outside law enforcement agencies requesting to receive alerts of hits from the FSC system must have a mutual aid agreement, letter of understanding, or other agreement in place with HDPS, and must have an HDPS approved policy related to the FSC system. Command approval is required.
- All custom hot list data entries into the FSC system for hits and alerts for outside law enforcement agencies will be completed by HDPS designated administrators.

h. Retention of FSC related photos and data

- FSC related data is stored for a maximum of 30 days.
- FSC data that is potential evidence must be transferred to and retained in the department's digital evidence storage system.

i. Business and Home Owner Association Partnerships

- Business Entities and Home Owner Associations
  - May purchase and install FSC technology
  - May provide inquiry/view access to the Holland Department of Public Safety
- Any publicly/privately owned Crime Prevention FSC Camera System that stores data on City of Holland databases must be done according to the specifications, policies, and guidelines of this agency.
- Any publicly/privately owned Crime Prevention FSC Camera System will not have access to search or view FSC data stored on the City of Holland databases.



Matt J. Messer
Chief of Public Safety Services

FLOCK SAFETY CAMERA HOT LIST ENTRY FORM

- Enter onto Hot List
- Enter as Saved Search
- OCCDA entered – date: _____

For Hotlist Entry:

Complaint Number: _____ Incident Type: _____

Reason to add to Hot List: _____

_____

_____

_____

- Investigative Purposes ONLY (provide specifics above)
- Probable Cause for stop/arrest or warrant information_____

_____

_____

- Notify - Name: _____ Contact # _____

Plate: _____ State: _____

Hot List Entry Expiration (total hours or date): _____

For Saved Search:

Vehicle Type: _____

License Plate Type: Regular Plate _____ or Temporary Plate _____

Vehicle Make: _____

Vehicle Color: _____

Start Time_____ End Time _____

Name of person making the request to enter (Must be Detective/Sergeant / Command):

_____ **Date:** _____

FOR OFFICE STAFF:

Entered date: _____ Removed date: _____

Reason for removal: _____

Township of Kalamazoo Police Department Order No. 04-03

Subject: Automatic License Plate Readers (ALPRs)

Distribution: All Employees

New: ☒ Replaces: Effective: April 30, 2024

Amended: ☐

Revised: ☐ Notes:

Reviewed Date:

Authorized by: Bryan N. Ergang, Chief of Police

GENERAL ORDER

I. PURPOSE

This policy governs the use of Automated License Plate Reader (ALPR) technology by members of the Township of Kalamazoo Police Department (TKPD).

II. POLICY

It is the policy of this law enforcement agency to utilize Automated License Plate Reader (ALPR) technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public. The intended use of ALPR technology is to assist officers with objectively actionable leads needed to solve investigations and protect the community. All data and images gathered by the ALPR are for the official use of sworn law enforcement only.

III. DEFINITIONS

A. ALPR System – The ALPR Units, communications network components, data server hardware and software including any Optical Character Recognition (OCR) software and algorithms, all operating in an organized and coordinated manner.

B. ALPR Units – The imaging hardware which captures the image of the license plates, regardless of the types of cameras used or the deployment of the unit.

C. ALPR Data – All ALPR images and/or alerts that are active or historical in nature and stored within the ALPR System.

D. Active ALPR Data – Information which is provided to a law enforcement official in real-time. Active ALPR Data includes alerts or notifications that a license plate number contained on an Alert List has been detected in the vicinity of an ALPR Unit.

E. Historical ALPR Data – The dates, times, and locations of individually identifiable motor vehicles that are stored for future use and includes any ALPR Data not considered Active ALPR Data.

F. Crime – As used herein, the term "crime" shall mean an act or the commission of an act that is forbidden by a public law or the omission of a duty that is commanded by a public law and makes the offender liable to punishment by that law. The term "crime" also includes acts of terrorism.

G. Alert List – List containing license plate numbers of stolen cars, vehicles owned by persons of interest, vehicles reasonably suspected of being involved in a crime, and/or vehicles associated with AMBER Alerts that are regularly circulated among law enforcement agencies. Alert 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. Departments of motor vehicles can provide lists of expired registration tags and law enforcement agencies can interface their own, locally compiled lists to the ALPR System. These lists serve an officer safety function as well as an investigatory purpose. In addition to agency supported Alert Lists, users may also manually add license plate numbers to lists in order to be alerted if and when a vehicle license plate of interest is “read” by the ALPR system.

H. Authorized Administrator – A sworn command officer of this department who has been authorized by the Chief of Police or designee who is

responsible for system administration to include setting up groups of Authorized Users as well as maintaining and/or removing data from lists, providing training to agency Authorized Users, and coordination with the system vendor for hardware and software setup and maintenance. The Support Services Lieutenant should be included as an Authorized Administrator.

I. Authorized User – A sworn employee of this department who has been authorized by the Chief of Police or designee to operate an ALPR or to access and use ALPR stored data, and who has successfully completed training provided by an agency Authorized Administrator.

IV. ALPR DATA COLLECTION

Owners of motorized vehicles driven on public thoroughfares are required by law to register their vehicle(s) with their state bureau or department of motor vehicles, and to attach license plates which are publicly and legibly displayed. Vehicle license plates generally consist of a series of alpha numeric characters that reference the license plate to the specific vehicle registered. Each piece of ALPR Data collected by TKPD may include:

A. Digital image of the vehicle

B. Vehicle license plate numbers and letters

C. The Global Positioning System (GPS) coordinates or other location information of the observation

D. The date and time of the observation, and

E. Other information contained in the ALPR image aids in the identification of vehicles including, but not limited to, color, make, body style, decals, etc.

The data captured by the ALPR Unit itself is entirely anonymous and is not considered personal identifying information. Authorized Users can only identify the registered owner of a vehicle by querying a separate, secure state government database of vehicle license plate records, which is restricted, controlled, and audited. The Driver's Privacy Protection Act (DPPA) restricts access and prohibits the release of personal information from state motor vehicle records to ensure the privacy of citizens, 18 USC
§ 2721-2725.

V. ALPR DATA MAY BE COLLECTED FOR:

A. Supporting crime analysis techniques.

B. Alerting law enforcement officials of the proximity of a vehicle displaying a license plate number included on an Alert List.

C. Locating vehicles with a known relationship to an individual who is reasonably suspected of having committed a crime.

D. Assisting Law Enforcement in locating missing or endangered persons.

VI. ALPR DATA COLLECTION TECHNIQUES

ALPR Units may be deployed in any of the following manners:

A. In a fixed deployment, by being permanently mounted in a fixed location.

B. In a portable deployment, by being semi-permanently placed, whether overtly or covertly.

C. In a mobile deployment, by being mounted to a mobile vehicle, whether overtly or covertly, or by a handheld device.

VII. USE AND DISSEMINATION OF ALPR DATA

A. Authorized Users may access Active ALPR Data to be alerted in real time to the location of vehicles on an active alert list. Entries on the alert list contain license plate information identifying a vehicle reported as:

1. Stolen or displaying a stolen license plate.

2. Associated with child abductions or missing and endangered persons.

3. Involved in an official law enforcement investigation when there is articulable suspicion linking the individual to a crime that has already been committed.

Generally, active ALPR alert entries should not be the sole reason for an investigatory stop. Officers should independently verify the ALPR alert entries though LEIN/NCIC databases or other means unless the officer has firsthand knowledge of the alert data.

B. Authorized Users of an ALPR System may access Historical ALPR Data to:

1. Identify and analyze the time-based locations of vehicles

reasonably related to individuals when there is articulable suspicion linking the individual to a crime that has already been committed.

2. Identify and analyze the time-based locations of vehicles displaying alphanumeric license plates contained in an Alert List.

C. Field Operations and Enforcement Actions

1. Authorized Users of the ALPR system will unselect the following: Supervised Release, Protection Order, Violent Person, Immigration Violator, Sex Offender, Protective Interest, and CPIC (Canadian Police Information Center) Data Records under the National Crime Information Center (NCIC) notification reasons and will not take any enforcement action if the ALPR system alerts solely for these reasons.

2. Custom alert lists that alert the entire organization or portions of the organization must be authorized by a detective or command officer.

3. When notified of a NCIC “hit” from the ALPR system, Authorized Users shall verify the ALPR response through the Law Enforcement Information Network (LEIN) before taking enforcement action. Action shall not be based solely on the ALPR alert.

4. An alert alone is not a basis for enforcement action.

5. Prior to initiation of a stop of a vehicle or other intervention based on an alert, personnel shall undertake the following:

   a. An authorized user must confirm the vehicle is still stolen, wanted, or otherwise of interest before proceeding (absent exigent circumstances). Without confirmation, a vehicle cannot be stopped solely on an ALPR alert and there must be a legal justification for the stop, such as a traffic violation, reasonable suspicion, or probable cause.

   b. Authorized Users will verify the license plate of interest matches identically with the image of the license plate number captured (read) by the ALPR, including:

      - the alphanumeric characters of the license plate
      - issuing state
      - vehicle descriptors before proceeding

6. After the stop of a vehicle or other intervention based on the alert, the Authorized User(s) will notify their supervisor or Authorized Administrator of the positive hit and request the plate be removed

from the list, unless the interest in the vehicle still exists.

D. Disseminating ALPR Data

1. Active and Historical ALPR Data may be disseminated to law enforcement officials from other jurisdictions upon request or through shared data on the vendor platform. The requesting agency must provide the reason for the request, and it can only be used for official law enforcement investigations.

2. ALPR Data shall only be used for law enforcement purposes. ALPR Data will not be released to the public unless required by statute, court order or when approved by a Division Commander or higher rank to warn the community of a vehicle associated with an individual who poses an immediate threat of harm to the community or an individual.

VIII. RETENTION OF ALPR DATA

A. ALPR Data connected to a criminal investigation shall be retained as part of the investigation record and shall be subject to department retention and disposal schedules.

B. ALPR Data used to convict an individual, including but not limited to Query Responses, shall be retained as part of the TKPD case file as an external document and shall be subject to department retention and disposal schedules for that specific case and conviction.

C. ALPR Data not connected to an investigation or conviction shall be subject to 3rd party vendor retention and disposal schedules and are not to exceed 30 days.

IX. ALPR TRAINING

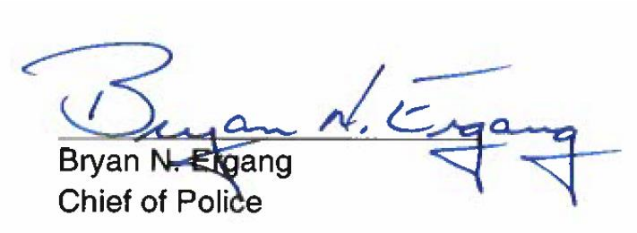
Use of the department's ALPR System shall be limited to personnel who have completed training in accordance with this section and provided documentation of successfully completed training.

A. ALPR training will be conducted by an Authorized Administrator.

B. Training for Authorized Administrators of the system will initially be provided by the vendor.

X. ALPR MAINTENANCE

ALPR operational status can be monitored through the system by an Authorized Administrator. ALPR Maintenance for hardware and software will be performed by the vendor of the ALPR system. Software updates are regularly pushed out to the system by the vendor. If hardware requires repair or replacement, the Support Services Lieutenant will coordinate with the vendor.



Bryan N. Elgang
Chief of Police

FC: 514
DC: A

DEPARTMENT OF POLICE

KENTWOOD, MICHIGAN

SUBJECT: LICENSE PLATE RECOGNITION SYSTEMS

Effective: January 24, 2024

1.0 PURPOSE

The purpose of this directive is to establish requirements and procedures for the use of crime prevention license plate recognition (LPR) system(s), and storage of electronic data used in conjunction with this equipment. Expected outcomes include:

a) Ensure LPR system use respects individuals' constitutional and statutory rights, including for example, privacy, freedom of speech and association, freedom of religion, and equal protection.
b) Provide governmental accountability.
c) Deter criminal behavior and, when appropriate, assist in criminal investigations and prosecutions.
d) Allow for appropriate cooperation with businesses, institutions, condominium associations, homeowner associations, neighborhood associations, and other entities or groups seeking safety and security for specifically identified property.
e) Enhance the Department's productivity and effectiveness and enhance community and officer safety with deployment and use of LPR systems.

2.0 POLICY

All Department personnel must comply with this policy in the deployment and use of License Plate Recognition (LPR) systems and any reports, data, or information generated by LPR systems.

3.0 DEFINITIONS

Alert - A visual and/or auditory notice that is triggered when the LPR system receives a potential "hit" on a license plate.

Fixed LPR system - LPR cameras that are permanently affixed to a structure, such as a pole, traffic barrier, or a bridge.

FOUO - For Official Use Only

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.

Hot list - 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. 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.

LPR - License Plate Recognition/License Plate Reader

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 system.

4.0 PROCEDURE

4.1 AUDIO RECORDING RESTRICITONS

4.1.1 The Kentwood Police Department LPR system will not have an audio recording feature, nor shall modifications be made to the system to allow audio recording. Audio recording is governed by federal law and is separate and apart from the recording performed by the Crime Prevention LPR Camera System. Title 1 of the Electronic Communications Privacy Act of 1996 (16 U.S.C. Section 2510) limits the ability of law enforcement to execute wiretaps.

4.2 AUTHORIZED USES

4.2.1 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.

4.2.2 Only trained, sworn law enforcement officers authorized by an administrator may access LPR systems, LPR data and associated media and all their access must comply with this policy.

4.2.3 The use of LPR systems is restricted to public safety-related missions of this agency.

4.2.4 Except when done pursuant to a court order such as a search warrant, the LPR may be used only to record license plates of vehicles that are exposed to public view (*e.g.*, vehicles 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).

4.3 PROHIBITED USES OF LPR SYSTEM

4.3.1 Prohibited uses of the LPR system include:

a) Recording license plates that are not exposed to public view, except when done pursuant to a court order such as a search warrant.
b) Using the LPR system to harass and/or intimidate any individual or group.
c) Using 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.
d) Using the LPR system or associated scan files or hot lists for any personal purpose.
e) Using 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.

4.4 ADMINISTRATION

4.4.1 The Chief of Police, or their designee, shall designate an employee(s) with administrative oversight (The 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 establish and 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 requests for LPR systems use or data access according to the policies and guidelines of this agency.

4.4.2 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 designated LPR vendor.

4.4.3 LPR system repairs, hardware, or software, shall be made by technicians through the designated LPR vendor.

4.5 FIXED LICENSE PLATE RECOGNITION SYSTEMS (LPR) USAGE

4.5.1 Fixed LPR system is a passive system, live data is not viewed.

4.5.2 Fixed 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 law enforcement officers of the department as appropriate.

4.5.3 Fixed LPR system searches of historical data shall only be conducted by trained sworn law enforcement officers of this department and can only be done for legitimate public safety related purposes. A log of such requests will be maintained by the system administrator.

4.5.4 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.,* 22-XXXX 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 – GRPD Shooting Suspect Vehicle).

4.5.5 Fixed 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."

4.6 FIELD OPERATIONS AND ENFORCEMENT ACTIONS

4.6.1 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.

4.6.2 Hotlists that alert the entire organization may only be created by a supervisor or the department's designated crime analyst. Individual officers may create their own hotlists that only alert that officer of vehicles that are of interest in a criminal investigation.

4.6.3 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 before taking enforcement action that is based solely on an LPR alert.

4.6.4 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.

4.6.5 Because the LPR alert relates to a vehicle plate and may not relate to the person operating the vehicle, officers need reasonable suspicion and/or probable cause to make an enforcement stop of any vehicle (for example, 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).

4.6.6 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.

4.6.7 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.

4.6.8 Prior to initiation of a stop of a vehicle or other intervention based on an alert, officers shall undertake the following:

1. 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).

2. 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 (be on the lookout) 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.

4.6.9 Officers will clear all stops initiated from a hot list alert by indicating the positive LPR hit in the appropriate offense report (i.e., with an arrest or enforcement action).

a) The officer will notify a supervisor of the positive hit and request that the plate be removed from the hot list.
b) The supervisor will remove the plate from the hot list and notify all department supervisors via email, using the KPD Supervisor email group list.

4.6.10 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.

4.6.11 All hot list plates and suspect information entered 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

4.6.12 Anytime 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. The user will also document the positive result in the LPR software system. The LPR supervisor will review these entries and make additions when necessary.

4.7 LPR DATA SHARING AND DISSEMINATION

4.7.1 LPR data should be considered FOUO and can only be shared for legitimate law enforcement purposes:

4.7.2 Outside law enforcement agencies 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.

4.7.3 The detective assigned to the multi-jurisdictional auto theft task force may conduct searches and share returns with members of the task force to further enhance their mission of recovering stolen vehicles.

4.7.4 Only system administrators or supervisors will conduct searches of the LPR database for outside law enforcement agencies. The administrator or supervisor will enter the requesting agency's name, the agency's case number, and incident type in the reason for search field (i.e., GRPD 22- XXXX Robbery).

4.7.5 Information sharing among agencies should be dictated in established departmental policies.

4.7.6 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).

4.8 RETENTION OF LPR RELATED PHOTOS AND DATA

4.8.1 LPR related data will be stored for a maximum of 30 days

4.8.2 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.

4.9 BUSINESS AND HOMEOWNER ASSOCIATION PARTNERSHIPS

4.9.1 Business Entities and Homeowner Associations:

a) May purchase and install LPR technology
b) May provide inquiry/view access to the Kentwood Police Department.

4.9.2 Any publicly/privately owned Crime Prevention LPR camera system that stores data on Kentwood Police Department databases must be done according to the specifications, policies, and guidelines of this agency.

4.9.3 Any publicly/privately owned Crime Prevention LPR camera system will not have access to search or view LPR data stored on the Kentwood Police Department databases.

4.10 VIOLATION OF LPR POLICY AND PROCEDURE

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

a) Criminal prosecution
b) Civil liability, and/or
c) Administrative sanctions, up to and including termination, pursuant to and consistent with the relevant collective bargaining agreements and department policies.

4.0 CANCELLATION

None

Bryan Litwin
Chief of Police

MONROE POLICE DEPARTMENT
STANDARD OPERATING PROCEDURE

Subject: License Plate Readers (LPR)	
Number: 12.7	
Published: June 2024	Review/Amended: June 2024
Distribution: Police Personnel	Issued by: Director Chad J. Tolstedt

I. PURPOSE

The purpose of this policy is to provide guidance for the capture, storage, and use of digital data obtained through the use of license plate reader (LPR) technology.

II. POLICY

It is the policy of the Monroe Police Department to utilize LPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public.

It is department policy that all installation and maintenance of LPR equipment, as well as LPR data retention and access, shall be managed as determined by the Director of Public Safety or designee. The Director of Public Safety will assign a supervisor to administer the day-to-day operation of the LPR equipment and data.

It is department policy to use LPR systems only for legitimate law enforcement and public safety purposes. The LPR administrator shall ensure that LPRs are not deployed or used to enforce the law in any discriminatory manner that is prohibited by the United States Constitution and laws, the State of Michigan laws, or the City of Monroe Charter and Ordinances.

III. PROCEDURE

A. General

1. Use of an LPR is restricted to the purposes outlined in policy and training.

   a. Information gathered or collected, and records retained by department LPR system cameras will not be accessed or used for any purpose other than legitimate law enforcement or public safety purposes.

   b. Officers shall not use, or allow others to use, the equipment or database records for any unauthorized purpose.

2. The following uses of the LPR system are specifically prohibited:

a. Invasion of Privacy: Except when done pursuant to a court order such as a search warrant, it is a violation of this policy to utilize the LPR to record license plates except those of vehicles that are exposed to public view (e.g., vehicles 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).

b. Harassment or Intimidation: It is a violation of this policy to use the LPR system to harass and/or intimidate any individual or group.

c. Personal Use: It is a violation of this policy to use the LPR system or associated scan files or hot lists for any personal purpose.

B. Administration

1. All installation and maintenance of LPR equipment, as well as LPR data retention and access, shall be managed by the LPR administrator.

a. All LPR equipment shall be considered department owned property.

2. The Director of Public Safety or designee shall designate an LPR administrator with administrative oversight for LPR system operations and is responsible for:

a. Establishing protocols for access, collection, storage, and retention of LPR data and associated media files.

b. 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.

c. Establishing protocols for LPR system monitoring to ensure the security and integrity of data captured, stored, and/or retained by the LPR system and compliance with applicable privacy laws.

d. Establishing the training requirements for officers to operate the LPR system and coordinating with other department personnel as needed.

e. Maintaining records identifying approved LPR deployments and documenting their results, including appropriate documentation of significant incidents and arrests that are related to LPR usage.

f. Analyzing crime patterns and demographic information when an LPR is moved or when additional LPRs are added to the department's LPR system.

g. Authorizing any requests for LPR systems use or data access in consultation with the Director of Public Safety and according to department policies and guidelines.

3. Officers will report any damage to department LPR equipment, via the chain of command, to the LPR administrator who will coordinate any necessary repairs.

4. The LPR administrator will ensure that designated, trained personnel check LPR equipment on a regular basis to ensure functionality and camera alignment.

5. Repairs or modifications to LPR systems hardware or software, shall only be made by authorized sources or employees as determined by the LPR administrator.

C. License Plate Reader System Usage

1. LPR operation, all data and images gathered by the LPR, and access to LPR collected data shall be for the official use of this department.

2. Only properly trained employees are allowed access to the LPR system, to operate LPR equipment, to access LPR data, or to collect LPR information.

3. To ensure proper operation and facilitate oversight of the LPR system, all trained users are required to have individual credentials for access and use of the LPR system and/or data, which has the ability to be fully audited.

4. Officers shall not use personal devices to take or upload images to the LPR system.

D. Operations

1. LPR Alerts/Hits:

a. E911 will monitor the LPR system for alerts and dispatch officers as appropriate.

b. If practicable, officers should confirm the license plate from the alert matches the license plate of the observed vehicle prior to

initiating a stop.

c. Absent exigent circumstances, the officer shall verify the suspect and/or vehicle is still wanted if the alert was generated due to the inclusion of the suspect and/or vehicle on a state or national database.

d. The officer shall verify an LPR response through the appropriate database before taking enforcement action that is based solely on an LPR alert.

e. Because the LPR alert may relate to a vehicle and may not relate to the person operating the vehicle, officers are reminded that they need to have reasonable suspicion and/or probable cause to make a stop of any vehicle.

f. Any traffic stop resulting from an LPR alert will have “LPR alert” added to the call’s narrative.

2. Hot Lists

a. Designation of hot lists to be utilized by the LPR system shall be made by the LPR administrator or designee.

1. Specific hot lists shall be approved and entered by the LPR administrator (or designee) within the LPR system.

2. All plates, vehicles, and suspect information entered into the LPR system will also contain the following information:

a. Entering user’s name

b. Requesting officer’s name

c. Related case number

d. Short synopsis describing the nature of the originating call

b. Internal requests to add information to the LPR system shall be done by using the currently approved department form. The requests will be processed by the LPR administrator or designee and added to the system as appropriate.

c. Exigent requests and requests from outside law enforcement agencies will be sent to the shift supervisor. If the shift supervisor determines the request is for legitimate law enforcement purposes, they shall notify the LPR Administrator for entry into the LPR system.

d. The LPR administrator or designee shall audit local hot list entries weekly, by requesting justification from the requesting officer, case detective or supervisor to keep the entry on the hot list. If acceptable justification is not received within seven days of the request, the entry shall be removed.

3. Special Details

a. LPR use during nontraditional deployments (e.g., special operations or during a criminal investigation) must be approved by the shift supervisor.

E. LPR Data Detection Browsing Audits

1. Before an officer can access the LPR database to browse LPR detections, the inquiring officer must document a reason for the inquiry within the LPR system.

2. It is the responsibility of the LPR administrator or the Director of Public Safety's designee to ensure that an audit is conducted of LPR detection browsing inquiries at least once each quarter. The LPR Administrator will audit a sampling of the LPR system utilization from the prior period to verify proper use in accordance with the authorized uses.

3. The audit shall be documented in writing and forwarded to the Director of Public Safety. The audit shall include any data errors found so that such errors can be corrected. After review by the Director of Public Safety, the audit and any associated documentation shall be filed and retained by the LPR administrator.

F. Data Collection and Retention

1. All data will be closely safeguarded and protected by both procedural and technological means.

2. The LPR vendor will store and ensure proper maintenance and security of data.

3. The department will retain LPR data for a maximum of 30 days, unless a longer retention period is required by KRS or applicable records retention

schedules.

a. If data has evidentiary value, it must be stored according to policy as soon as practicable.

G. Releasing LPR Data

1. LPR data may be released to other authorized and verified law enforcement officials and agencies for legitimate law enforcement purposes.

2. All non-law enforcement requests for access to stored LPR data shall be processed in accordance with applicable law.

3. Any employee who receives a written request for LPR data will accept the request in accordance with G.O. series 2018-03 Open Records and will immediately forward the request to the Open Records Unit.

IV. DEFINITIONS

***Alert*:** A visual and/or auditory notice that is triggered when the LPR system receives a potential "hit" on a license plate.

***Hit*:** Alert from the LPR system that a scanned license plate number may be in the National Crime Information Center (NCIC) or other law enforcement database for a specific reason including, but not limited to, being related to a stolen car, wanted person, missing person, domestic violation protective order or terrorist-related activity.

Hot List: A list containing vehicles of interest with an articulable criminal nexus or valid public safety concern, including but not limited to, vehicles which are reported as stolen, display stolen license plates, vehicles linked to missing and/or wanted people, and vehicles flagged by law enforcement agencies.

License Plate Reader *(LPR)*: A device that uses cameras and computer technology to compare digital images to database lists of known information of interest.

LPR Data: Data captured by the LPR cameras of an image (such as a license plate and description of vehicle on which it was displayed) within public view that was read by the device, including GPS coordinates and date and time information of the LPR system at the time of the LPR's read.

Vehicles of Interest: Including, but not limited to vehicles which are reported as stolen; display stolen license plates or tags; vehicles linked to missing and/or wanted persons and vehicles flagged by law enforcement agencies.

Automated License Plate Reader (ALPR) Acceptable Use

612.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance for the capture, storage and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology.

612.2 POLICY

The policy of the Muskegon Police Department is to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public. It is used by the Muskegon Police Department 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. It may also be used to gather information related to active warrants, homeland security, suspect interdiction and stolen property recovery. All data and images gathered by the ALPR are for the official use of this department.

Because such data may contain confidential information, it is not open to public review. ALPR technology will not be used to contribute to the criminalization of poverty. As such, ALPR technology will not be used for traffic enforcement, or the enforcement of civil judgements and immigration laws.

612.3 OPERATIONS

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

(a) An ALPR shall only be used for official law enforcement business.

(b) An ALPR may be used in conjunction with any routine patrol operation or criminal investigation. Reasonable suspicion or probable cause is not required before using an ALPR.

(c) While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR to canvass areas around homicides, shootings and other major incidents. Partial license plates reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.

(d) No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.

(e) No ALPR operator may access confidential department, state or federal data unless authorized to do so.

(f) If practicable, the officer should verify an ALPR response through the appropriate official law enforcement database before taking enforcement action that is based solely on an ALPR alert.

612.4 DATA COLLECTION AND RETENTION

The Director of Public Safety or authorized designee is responsible for ensuring systems and processes are in place for the proper collection and retention of ALPR data.

All stored ALPR data should be retained in accordance with the established records retention schedule. Thereafter, ALPR data should be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a discovery request or other lawful action to produce records. In those circumstances, the applicable data should be downloaded onto portable media and booked into evidence.

612.5 ACCOUNTABILITY

All data will be closely safeguarded and protected by both procedural and technological means. The Muskegon Police Department will observe the following safeguards regarding access to and use of stored data:

(a) All ALPR data downloaded to the mobile workstation 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.

(b) 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 relate to a specific criminal investigation or department-related civil or administrative action.

(c) ALPR system audits should be conducted on a regular basis.

612.6 RELEASING ALPR DATA

ALPR data may be shared with other law enforcement or prosecutorial agencies upon request or through shared data on the vendor platform. The requesting agency must provide the reason for the request, and it can only be used for official law enforcement purposes. Any dissemination will be documented.

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

06/05/2025

GENERAL ORDER NO. 132

TO: All Personnel

FROM: Steve Cooper, Director of Public Safety

SUBJECT: Automated License Plate Readers

I. PURPOSE

The purpose of this policy is to provide guidance for the capture, storage and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology.

II. POLICY

The availability and use of License Plate Recognition (LPR) systems have provided many opportunities for the enhancement of productivity, effectiveness, and officer safety. It is the policy of this agency that all members abide by the guidelines set forth herein when using this technology, while maintaining compliance with applicable state and federal laws.

III. DEFINITIONS

Automated License Plate Reader (ALPR): A device that uses cameras and computer technology to compare digital images to lists of known information of interest.

ALPR Operator: Trained Department members who may utilize ALPR system/equipment. ALPR operators may be assigned to any position within the Department, and the ALPR Administrator may order the deployment of the ALPR Systems for use in various efforts.

ALPR Administrator: The Director of Public Safety or his designee(s) serves as the ALPR Administrator for the Department.

Hot List: A list of license plates associated with vehicles of interest compiled from one or more databases including, but not limited to, NCIC, SOS, LEIN, Local BOLOs, etc.

Vehicles of Interest: Including, but not limited to, vehicles which are reported as stolen; display stolen license plates or tags; vehicles linked to missing and/or wanted persons and vehicles flagged by the Secretary of State Administration or law enforcement agencies.

Detection: Data obtained by an ALPR of an image (such as a license plate) within public view that was read by the device, including potential images (such as the plate and description of vehicle on which it was displayed), and information regarding the location of the ALPR system at the time of the ALPR's read.

Hit: Alert from the ALPR system that a scanned license plate number may be in the National Crime Information Center (NCIC) or other law enforcement database for a specific reason including, but not limited to, being related to a stolen car, wanted person, missing person, domestic violation protective order or terrorist-related activity.

IV. PROCEDURE

A. ADMINISTRATION

The ALPR technology, also known as License Plate Recognition (LPR), allows for the automated detection of license plates along with the vehicle make, model, color and unique identifiers through the Oak Park Public Safety Department's ALPR's system and the vendor's (Flock Safety/AXON) vehicle identification technology. The technology is used by the Oak Park Public Safety Department to convert data associated with vehicle license plates and vehicle descriptions for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates and missing persons. It may also be used to gather information related to active warrants, homeland security, electronic surveillance, suspect interdiction and stolen property recovery. All installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Director of Public Safety and/or his /her designee. The Director of Public Safety or his

designee(s) will assign members under his/her command to administer the day-to-day operation of the ALPR equipment and data.

B. ALPR ADMINISTRATOR

The Director of Public Safety or his / her designee(s) shall be responsible for compliance with the requirements of Civil Codes/Laws. The Director has designated the Investigations Bureau Commander as the Department's ALPR Administrator. The ALPR Administrator shall:

1. ensure that only properly trained personnel are allowed access to the ALPR systems or to collect ALPR information.
2. ensure that training requirements are completed for authorized users.
3. monitor the ALPR systems to ensure the security of the information and compliance with applicable privacy laws.

C. OPERATIONS

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

1. An ALPR shall only be used for official law enforcement business.
2. An ALPR may be used in conjunction with any routine patrol operation or criminal investigation; reasonable suspicion or probable cause is not required before using an ALPR.
3. Partial license plates and unique vehicle descriptions reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.
4. No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.

5. The officer shall verify an ALPR response through the Law Enforcement Information Network (LEIN) before taking enforcement action that is based solely on an ALPR alert.

    a. Once an alert is received, the operator shall confirm that the observed license plate from the system matches the license plate of the observed vehicle.

    b. Before any law enforcement action is taken because of an ALPR alert, the alert will be verified through a LEIN inquiry via MDC or through Dispatch.

    c. Officers will not take any police action that restricts the freedom of any individual based solely on an ALPR alert unless it has been validated.

    d. ALPR alerts may relate to a vehicle and may not relate to the person operating the vehicle; officers are reminded that they need to have reasonable suspicion and/or probable cause to make an enforcement stop of any vehicle.

        -For example, if a vehicle is entered into the system because of its association with a wanted individual, Officers should attempt to visually match the driver to the description of the wanted subject prior to making the stop or should have another legal basis for making the stop.

6. Hot Lists: An alert alone shall not be a basis for police action (other than following the vehicle of interest). Prior to initiation of a stop of a vehicle or other intervention based on an alert, Department members shall undertake the following:

    a. Verification of status on a Hot List: An officer must receive confirmation through a LEIN inquiry by MDC or through Dispatch that the license plate was entered as 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 with the image of the license plate captured by the ALPR system,

including both alphanumeric characters of the license plate, state of issue, and the vehicle descriptors prior to proceeding.

i. Department employees alerted to a Hot List hit are required to make a reasonable effort to confirm that a wanted person is in the vehicle and/or that a reasonable basis exists before a reasonable stop of the vehicle.

c. All entries and updates of specific Hot Lists within the ALPR system will be documented by the employee entering or by the requesting department employee within the subsequent incident report or call for service. Hotlist entries and updates shall be approved by a supervisor before entry into the ALPR system.

i. The hits from these data sources should be viewed as informational, created solely to bring the officers' attention to specific vehicles that may be associated with criminal activity.

ii. All plates and suspect information entered into the ALPR system Hot List shall contain the following information:

- Entering Department employee's name
- Related case number
- Short synopsis describing the nature of the originating call

7. Monitoring Operations: Dispatchers shall ensure that the Flock Safety application is active in the telecommunication center and that the current on-duty dispatcher is signed into the system.

a. Dispatchers shall monitor the system for any Hot List alerts. Dispatchers should immediately, or as soon as practical, broadcast a BOLO for any of the following Hot List alerts:

i. Stolen Vehicle or License Plate

ii. Serious Warrants / Wanted Felony Vehicles

iii. Amber Alerts / Missing Children

iv. Involuntary Missing People

b. In order to confirm the Hot List alert, dispatch shall run the license plate of the vehicle through LEIN/SOS/NCIC. Dispatch should then broadcast any information gained from the law enforcement systems.

D. TRAINING

1. The Department will ensure that all authorized employees receive department approved training to use or access the ALPR system. No employee shall operate the ALPR equipment or access the data without the approved training

E. LOGIN/LOG OUT PROCEDURE

1. To facilitate oversight of the ALPR system, all users are required to have individual credentials for access and use of the systems and/or data, which have the ability to be fully audited.

F. IMPERMISSIBLE USES

1. The ALPR systems, and all data collected, are the property of the Oak Park Department of Public Safety. Department personnel may only access and use the ALPR systems for official and legitimate law enforcement purposes consistent with this policy. The following uses of the ALPR system are specifically prohibited:

a. Invasion of Privacy: Except when done pursuant to a court order such as a search warrant, it is violation of this policy to utilize the ALPR to record license plates except those of vehicles that are visible to public view.

i. Vehicles visible to public view are on a public road or highway, or in a place where members of the public have access, such as parking lots or business establishments.

b. Harassment or Intimidation: It is a violation of this policy to use the ALPR system to harass and/or intimidate any individual or group.

c. Use based on a protected characteristic: It is a violation of this policy to use the ALPR system or associated files or hot lists solely because of a person's or groups race, gender religious or political affiliation, nationality, ethnicity, sexual orientation, disability, or other classification protected by law.

d. Personal Use: It is a violation of this policy to use the ALPR system or associated files or hot lists for any personal use. All personnel are specifically prohibited from making a copy, such as but not limited to, using personal cellular phones, in any format of any video, audio or still photograph generated from the ALPR application or associated files or hotlists for personal use.

e. First Amendment Rights: It is a violation of this policy to use the ALPR system or associated files or hot lists for the purpose or known effect of infringing upon First Amendment rights.

2. Any employee who engages in or allows the impermissible use of the ALPR system or the associated files or hot lists may be subject to:

a. Criminal Prosecution

b. Civil Liability

c. Discipline, up to and including termination.

G. DATA COLLECTION AND RETENTION

1. The Director or his/her designee(s) is responsible for ensuring systems and processes are in place for the proper collection and retention of ALPR data.

2. ALPR vendors will store the data and ensure proper maintenance and security of the stored data. Flock Safety will purge their data at the end of the thirty (30) days of storage.

3. Any data retrieved from the ALPR system, such as investigative search results for a criminal case, shall be transferred and stored in accordance with Department policies and procedure.

4. Information gathered or collected, and records retained by the Flock Safety cameras will not be sold, accessed, or used for any purpose other than legitimate law enforcement or public safety purposes.

H. ACCOUNTABILITY

1. All data shall be closely safeguarded and protected by both procedural and technological means. The Oak Park Public Safety Department shall observe the following safeguards regarding access to and use of stored data:

   a. All ALPR data downloaded to the mobile workstation shall be accessible only through a login/password-protected system capable of documenting all access information by name, date, and time.

   b. Employees approved to access the ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action.

   c. Such ALPR data may be released to other authorized and verified law enforcement officials and agencies for legitimate law enforcement purposes.

   d. Every ALPR Detection Browsing Inquiry must be documented by the associated Oak Park Public Safety Department incident report and the reason for the inquiry.

   e. Every ALPR search or hotlist alert that produces investigative leads shall be documented using the outcome-tracking software provided by the ALPR system.

I. ALPR DATA SEARCH AUDITS

1. It is the responsibility of the Director or his/her designee(s) to ensure that an audit is conducted of ALPR data search inquiries once a month. The audit shall randomly select at least 10 search inquiries conducted by department employees during the preceding one-month period and determine if each inquiry meets the requirements established in this policy.

2. A monthly report of audit results shall be forwarded to the Deputy Director.

J. RELEASING ALPR DATA

1. All non-law enforcement requests for access to stored ALPR data shall be processed in accordance with applicable law and FOIA procedures.

2. The ALPR data may be shared with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law. The procedure for such a request is as follows:

   a. Partnering law enforcement agencies may be granted access to the ALPR system by the Director of Public Safety or their designee upon meeting the following conditions:

      i. The partnering law enforcement agency must have a policy regarding ALPR system usage that contains oversight and accountability provisions consistent with this policy or have a signed memorandum of understanding with this department.

      ii. A list of approved partnering law enforcement agencies will be documented in the department's electronic files.

   b. A non-sharing law enforcement agency requesting ALPR data must include the agency name, the name of the requesting employee, the incident report related to the request, and a synopsis of the incident. Any investigative aid provided by an OPPSD member to a non-sharing law enforcement agency will

be detailed in an Assist Other Law Enforcement (ALE) incident report.

c. The request is reviewed by the Director of Public Safety or their designee.

d. The approved request shall be documented and retained in the report writing system.

e. All non-law enforcement or non-prosecutorial agencies will be processed by the FOIA retention schedule.

V. COMPLIANCE

Violations of this policy, or portions thereof, may result in disciplinary action.



Steve Cooper

Director of Public Safety

Redford Township Police Department

Policy Manual

SUBJECT	WRITTEN DIRECTIVE	NUMBER OF PAGES
Automated License Plate Reader (ALPR)	1-013	10
*This Directive Supersedes All Previously Issued Correspondence Relative To This Topic. *		

Accreditation Standards:	1.6.1	Effective Date	Revised Date
		5-7-2024	

I. PURPOSE

The purpose of this policy is to provide guidance for the capture, storage, and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology.

II. SCOPE

This policy applies to all sworn members of the Redford Township Police Department, and Dispatchers. Reserve Officers are prohibited from having ALPR accounts.

III. Policy

The policy of the Redford Township Department is to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public. All data and images gathered by the ALPR are for the official use of this department. Because such data may contain confidential information, it is not open to public review.

IV. Definitions

A. Automated License Plate Reader (ALPR) - A device that uses cameras and computer technology to compare digital images to lists of known information of interest.

B. ALPR Operator - Trained Department members who may utilize ALPR system/equipment. ALPR operators may be assigned to any position within the Department, and the ALPR Administrator may order the deployment of the ALPR systems for use in various efforts.

C. ALPR Administrator - The Chief and/or his or her designee, serves as the ALPR Administrator for the Department.

D. Hot List - A list of license plates associated with vehicles of interest compiled from one or

more databases including, but not limited to, NCIC, SOS, LEIN, Local BOLO's, etc.

E. Vehicles of Interest - Including, but not limited to vehicles which are reported as stolen; display stolen license plates or tags; vehicles linked to missing and/or wanted persons and vehicles flagged by the Department of Motor Vehicle Administration or law enforcement agencies.

F. Detection - Data obtained by an ALPR of an image (such as a license plate) within public view that was read by the device, including potential images (such as the plate and description of vehicle on which it was displayed), and information regarding the location of the ALPR system at the time of the ALPR's read.

G. Hit - Alert from the ALPR system that a scanned license plate number may be in the National Crime Information Center (NCIC) or other law enforcement database for a specific reason including, but not limited to, being related to a stolen car, wanted person, missing person, domestic violation protective order or terrorist-related activity.

V. Procedure

A. Administration

The ALPR technology, also known as License Plate Recognition (LPR), allows for the automated detection of license plates along with the vehicle make, model, color and unique identifiers through the Redford Township Police Department's ALPR's system and the vendor's vehicle identification technology. The technology is used by the Redford Township Police Department to convert data associated with vehicle license plates and vehicle descriptions for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates and missing persons. It may also be used to gather information related to active warrants, homeland security, electronic surveillance, suspect interdiction, and stolen property recovery. All installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Chief of Police and/or his or her Designee. Currently, the Detective Bureau Captain will administer the day-to-day operation

of the ALPR equipment and data and training.

B. ALPR Administrator

The Detective Bureau Captain, or Flock administrator, shall be responsible for the below requirements.

1. Only properly trained sworn officers, crime analysts, and dispatchers are allowed access to the ALPR system or to collect ALPR information.

2. Ensuring that training requirements are completed for authorized users. Officers and Dispatchers must view Flock training videos prior to using Flock.

3. ALPR system monitoring to ensure the security of the information and compliance with applicable privacy laws.

4. The Detective Bureau Captain is to ensure that the operation system is maintained and will continually work with the Custodian of Records regarding retention and destruction of ALPR data.

C. Operations

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

1. An ALPR shall only be used for official law enforcement business.

2. ALPR may be used in conjunction with any routine patrol operation or criminal investigation; reasonable suspicion or probable cause is not required.

3. Partial license plates and unique vehicle descriptions reported during major crimes

should be entered into the ALPR system in an attempt to identify suspect vehicles.

4. No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.

5. The officer shall verify an ALPR response through the Law Enforcement Information Network (LEIN) before taking enforcement action that is based solely on an ALPR alert. Once an alert is received, the operator shall confirm that the observed license plate from the system matches the license plate of the observed vehicle. Before any law enforcement action is taken because of an ALPR alert, the alert will be verified through a LEIN inquiry via MDT or through Dispatch. Members will not take any police action that restricts the freedom of any individual based solely on an ALPR alert unless it has been validated. Because the ALPR alert may relate to a vehicle and may not relate to the person operating the vehicle, officers are reminded that they need to have reasonable suspicion and/or probable cause to make an enforcement stop of any vehicle. (For example, if a vehicle is entered into the system because of its association with a wanted individual, Officers should attempt to visually match the driver to the description of the wanted subject prior to making the stop or should have another legal basis for making the stop.)

D. Hot Lists

Designation of hot lists to be utilized by the ALPR system shall be made by the ALPR Administrator or his/her designee. Hot lists shall be obtained or compiled from sources as may be consistent with the purposes of the ALPR system set forth in this Policy. Hot lists utilized by the Department's ALPR system may be updated by agency sources more frequently than the Department may be uploading them and thus the Department's ALPR system will not have access to real time data. Occasionally, there may be errors in the ALPR system's read of a license plate. Therefore, an alert alone shall not be a basis for police action (other than following the vehicle of interest). Prior to initiation of a stop of a vehicle or other intervention based on an alert, Department members shall undertake the following:

1. **Verification of status on a Hot List**. An officer must receive confirmation, from a Dispatcher or other department computer device, that the license plate is still stolen,

wanted, or otherwise of interest before proceeding (absent exigent circumstances).

2. 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 ALPR, including both the alphanumeric characters of the license plate, state of issue, and vehicle descriptors before proceeding. Department members alerted to the fact that an observed motor vehicle's license plate is entered as a Hot Plate (hit) in a specific BOLO (be on the lookout) 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 a department member would have a lawful basis to stop the vehicle.

3. Department members will clear all stops from hot list alerts by indicating the positive ALPR Hit, i.e., with an arrest or other enforcement action. If it is not obvious in the text of the call as to the correlation of the ALPR Hit and the arrest, then the Department member shall update with the Dispatcher and original person and/or a staff member inputting the vehicle in the hot list (hit).

4. All entries and updates of specific Hot Lists within the ALPR system will be documented by the requesting Department member within the appropriate general offense report. As such, specific Hot Lists shall be approved by the ALPR Administrator (or his/her designee) before initial entry within the ALPR system. The updating of such a list within the ALPR system shall thereafter be accomplished pursuant to the approval of the Department member's immediate supervisor. The hits from these data sources should be viewed as informational; created solely to bring the officers' attention to specific vehicles that have been associated with criminal activity.

5. All license plates and suspect information entered into the ALPR system shall contain the following information at a **minimum:**

a. Entering inquiring Department member's name and related case CR or CFS number.

SUBJECT	WRITTEN DIRECTIVE	NUMBER OF PAGES
Automated License Plate Reader (ALPR)	1-013	10
*This Directive Supersedes All Previously Issued Correspondence Relative To This Topic. *		

Accreditation Standards:	1.6.1	Effective Date	Revised Date
		5-7-2024	

E. Training

The Administrator shall design department-approved training for those authorized to use or access the ALPR system, including a review of this Directive.

1. Login/Log-Out Procedure

To ensure proper operation and facilitate oversight of the ALPR system, all users will be required to have individual credentials (username and password) for access and use of the systems and/or data, which has the ability to be fully audited.

2. Permitted/Impermissible Uses.

The ALPR system, and all data collected, is the property of the Redford Township Police Department. Department personnel may only access and use the ALPR system for official and legitimate law enforcement purposes consistent with this Policy. The following uses of the ALPR system are specifically prohibited:

a. Invasion of Privacy: Except when done pursuant to a court order such as a search warrant, it is a violation of this Policy to utilize the ALPR to record license plates except those of vehicles that are exposed to public view (e.g., vehicles 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).

b. Harassment or Intimidation: It is a violation of this Policy to use the ALPR system to harass and/or intimidate any individual or group.

c. Use Based on a Protected Characteristic. It is a violation of this policy to use the ALPR system or associated scan files 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.

d. Personal Use: It is a violation of this Directive to use the ALPR system or associated scan files or hot lists for any personal purpose, or to access files on behalf of another user not authorized to access the system. Prior WRITTEN permission from the Chief is required to run any colleague of the Township of Redford Police Department.

e. First Amendment Rights. It is a violation of this policy to use the ALPR system or associated scan files or hot lists for the purpose or known effect of infringing upon First Amendment rights.

f. Other Agency Data Access. Members of the Redford Township Police Department are subject to this directive when accessing other agencies' ALPR data.

3. Anyone from the Redford Township Police Department who engages in an impermissible use of the ALPR system or associated scan files, or hot lists may be subject to:

a. Criminal prosecution

b. Civil liability, and/or

c. administrative sanctions, up to and including termination, pursuant to and consistent with the relevant collective bargaining agreements and/or Department policies.

d. Denial of access to ALPR system.

F. DATA COLLECTION AND RETENTION

The Detective Bureau Captain is responsible for ensuring systems and processes are in place for the proper collection and retention of ALPR data. Data will be transferred to the designated storage in accordance with department procedures.

All ALPR data downloaded to the server should be stored for no longer than one year, and in accordance with the established records retention schedule. Thereafter, ALPR data should be

purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a discovery request or other lawful action to produce records. In those circumstances the applicable data should be downloaded from the server onto portable media and booked into evidence.

ALPR vendor, Flock Safety will store the data (data hosting) and ensure proper maintenance and security of data stored in their data towers. Flock Safety will purge their data at the end of the 30 days of storage. However, this will not preclude Redford Township Police Department from maintaining any relevant vehicle data obtained from the system after that period pursuant to the established Redford Township Police Department's retention schedule mentioned above or outlined elsewhere.

Restrictions on use of ALPR Data: Information gathered or collected, and records retained by Flock Safety cameras, or any other Redford Township Police Department ALPR system will not be sold, accessed, or used for any purpose other than legitimate law enforcement or public safety purposes.

G. ACCOUNTABILITY AND SAFEGUARDS

All data will be closely safeguarded and protected by both procedural and technological means. The Redford Township Police Department will observe the following safeguards regarding access to and use of stored data:

1. All non-law enforcement requests for access to stored ALPR data shall be processed in accordance with applicable law.

2. All ALPR data downloaded to the mobile workstation shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date, and time.

3. Persons 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 relate to a specific criminal investigation or department-related civil or administrative action.

4. Such ALPR data may be released to other authorized and verified law enforcement officials and agencies for legitimate law enforcement purposes.

5. Every ALPR Detection Browsing Inquiry must be documented by either the associated Redford Township Police Department's call for service or case number.

H. ALPR DATA DETECTION BROWSING AUDITS

It is the responsibility of the Detective Captain to ensure that an audit is conducted of ALPR detection browsing inquiries at least once during each calendar year. The Department will audit a sampling of the ALPR system utilization from the prior 12- month period to verify proper use in accordance with the above authorized uses. The audit shall randomly select at least 10 detection browsing inquiries conducted by department employees during the preceding six-month period and determine if each inquiry meets the requirements established in the policy section.

The audit shall be documented in the form of an internal department memorandum to the Chief of Police or his / her Designee(s). The memorandum shall include any data errors found so that such errors can be corrected. After review by the Chief of Police or his / her Designee(s), the memorandum and any associated documentation shall be filed and retained by the Redford Township Police Department.

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.

1. The agency makes a 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.

2. The request is reviewed by the Chief of Police or his / her Designee(s) or the authorized designee and approved before the request is fulfilled.

3. The approved request is retained on file. Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Freedom of Information Act / Records Release Policy.

SAGINAW POLICE DEPARTMENT
POLICY AND PROCEDURE ORDER

SUBJECT			ORDER NO.
LICENSE PLATE READERS			**PP-43**
EFFECTIVE DATE	DISTRIBUTION	NEW ☒ AMENDED ☐ CANCELS ☐	REVIEWED/NO CHANGE ☐
February 5, 2024	C		
ISSUED BY Robert M. Ruth			

I. PURPOSE

The purpose of this policy is to provide Saginaw Police Department (SPD) sworn and professional staff with guidelines on the procedure for deployment, utilization, maintenance, and training associated with the use of license plate recognition (LPR) systems, also commonly known as license plate reader systems. This policy promotes public safety and efficiency of law enforcement criminal investigatory activities through the use of license plate reader technologies and protocols, while ensuring the appropriate safeguards are in place to protect the privacy, civil rights, and civil liberties of individuals.

II. POLICY

The availability and use of LPR systems have provided many opportunities for the enhancement of productivity, effectiveness, and officer safety. License plate reader technology can be used to enhance public safety by assisting law enforcement to identify possible vehicles involved in an investigation. The technology should be used in a manner that protects the civil rights and civil liberties of citizens, including those rights guaranteed by the First, Fourth, and Fourteenth Amendments of the United States Constitution. It is the policy of the SPD that all members abide by the guidelines set forth herein when using LPR systems.

III. DEFINITIONS

LPR: License Plate Recognition/License Plate Reader

LPR Administrator: The Support Services Administrator will serve as the LPR Administrator who is responsible for the administrative oversight of the LPR system deployment, operations, and maintenance.

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 system.

Alert: A visual and/or auditory notice that is triggered when the LPR system receives a potential "hit" on a license plate.

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.

Hot list: 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 Secretary of State and other 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, approved personnel (all sworn supervisors, detectives, and the Support Services Administrator) may also manually add license plate numbers to hot lists to be alerted when a vehicle license plate of interest is "read" by the LPR system. The Support Services Administrator is responsible for maintenance of the local LPR system database function(s).

Fixed LPR system: LPR cameras that are permanently affixed to a structure, such as a pole, a traffic barrier, or a bridge.

Mobile Data Terminal: MDT is a mobile computer such as in-car computer or other mobile device that is authorized and capable of transmitting and receiving law enforcement information.

Mobile LPR system: LPR cameras that are affixed, either permanently (hardwired) or temporarily (e.g., magnet-mounted), to a law enforcement vehicle for mobile deployment.

Portable LPR system: LPR cameras that are transportable and can be moved and deployed in a variety of venues as needed, such as a traffic barrel or speed radar sign.

IV. PROCEDURES

A. General

1. The use of LPR systems is restricted to public safety–related missions of the SPD.

2. LPR systems and associated equipment and databases are authorized for official public safety purposes. Misuse of this equipment and associated databases, or data, may be subject to sanctions and/or disciplinary actions up to and including termination.

3. LPR systems and LPR data and associated media are the property of the SPD and intended only for use in conducting official business.

B. Administration

1. The Support Services Administrator will have administrative oversight for LPR system deployment and operations and is responsible for the following:

   a. Establishing protocols for access, collection, storage, and retention of LPR data and associated media files. Authorized users will be assigned specific security levels.

      1). Authorized read only security level users (patrol officers) are only provided view access to LPR alerts and live LPR footage.

      2). Authorized read/write security level users (sworn supervisors, detectives, and the Support Services Administrator can enter license plates and download LPR footage.

      3). Authorized users have been assigned a unique user identity and each user is required to create their own password at their first log-in. Authorized users are prohibited from sharing their password with others.

   b. 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.

      1). Successful alerts or "hits" acted upon in the field (apprehensions or recoveries) or associated with investigations or prosecutions shall be documented in the PremierOne system.

   c. Ensuring the security and integrity of data captured, stored, and/or retained by the LPR system.

   d. Maintaining records identifying approved LPR deployments and documenting their results, including appropriate documentation of significant incidents and arrests that are related to LPR usage.

   e. Authorizing any requests for LPR system access according to the policies and guidelines of the SPD.

   f. Prior to use of the LPR equipment or software, the LPR administrator will:

      1). Coordinate initial training for authorized staff - provided by the vendor.

      2). Provide on-going and/or initial training for new staff.

3). Ensuring that any changes in hardware, software, applicable laws, or training are relayed to the department.

2. The Support Services Administrator shall check equipment monthly to ensure functionality and camera alignment. Any equipment that falls outside expected functionality shall be removed from service until deficiencies have been corrected. Any SPD staff member that is aware that the LPR system is physically damaged, misaligned, not functioning, or not functioning properly is required to report that information immediately to the LPR Administrator. The LPR Administrator shall perform periodic, no less than annual, random audits or inspections of LPR system usage.

3. LPR systems repairs, hardware, or software, shall be done only by SPD authorized sources.

C. Permissible Use of License Plate Reader Technology

1. The use of LPR and associated equipment and databases by SPD personnel are authorized only for official public safety purposes; locating stolen or wanted vehicles, vehicles connected to AMBER alerts, Silver Alerts, missing persons reports, abductions reports, vehicles connected to other crimes, wanted subjects, or other suspected criminals.

2. Approved SPD personnel are only authorized to utilize license plate reader technology to:

a. Attempt to identify and/or locate a vehicle related to an investigation; or

b. Attempt to identify vehicle owner(s), driver, and/or occupant(s) when such individual(s):

1). Has committed a criminal offense; or

2). Is involved in or is planning criminal conduct or activity; or

3). Is a possible missing person, crime victim, or witness to criminal activity; or

c. Prevent, detect, and/or assess potential safety threats to members of the public and/or public officials.

d. Identify vehicles during routine patrol with suspended or revoked vehicle registrations.

e. Regulate public parking areas.

f. Monitor access to secured areas.

3. The on-duty patrol sergeant(s) must ensure that the LPR system is updated during their shift with the most current hot lists available.

4. LPR Alerts/Hits: Prior to initiation of the stop:

   a. Visually verify that the vehicle plate number matches the plate number run by the LPR system, including both alphanumeric characters of the license plate and the state of issuance.

   b. If time permits, the officer shall obtain confirmation via LEIN (NCIC) and/or Saginaw County Central Dispatch, that a hit on a stolen vehicle and/or wanted person(s) is valid.

5. In each case in which an alert or a hit is triggered, the user shall record the disposition of the alert and the hit into the PremiereOne system under the related case number. If there is not a related case number, it will be recorded in the member's daily report. All inquiries shall be documented including the reason(s) for the search, case number, and identity of the inquirer.

6. Special Details: LPR use during nontraditional deployments (e.g., special operations or during criminal investigations of a sensitive nature) must be approved by the chief and/or his/her designee.

7. Once an SPD staff member is aware that an alert is no longer valid (property has been recovered, missing person has been located etc.), he/she should immediately notify a sworn supervisor or a detective and request that the tag be removed from the system. The sworn supervisor or the detective who was notified shall immediately remove the tag from the system.

8. The use of LPR technology is restricted to approved legitimate law enforcement purposes as outlined in this policy. Prohibited Use of the LPR System includes:

   a. Use of LPR technology for personal or other non-official purposes.

   b. Use of LPR technology for investigatory purposes when the request/use for identification is based solely upon:

      1). Religious, political, or social views or activities, and/or

2). Participation in a noncriminal organization or lawful event.

D. Data and Security Access

1. SPD staff members who are granted access to LPR system devices and/or databases will be issued a username and password specific to everyone by the LPR administrator(s).

2. All operators of the LPR system will be responsible for maintaining a secure login and password. This password will not be shared with anyone else.

3. The database may be accessed for law enforcement purposes only.

4. Personnel will not release any information obtained by the LPR system to non-law enforcement personnel unless required by law and authorized by the chief or his designee. Release of data gathered by LPR system is restricted in the same manner as Criminal Justice Information Services and is unauthorized to non-law enforcement personnel.

5. Any policy violation or other misuse of the system will result in further investigation and appropriate disciplinary action, if warranted, up to and including termination.

E. LPR Data Sharing and Dissemination

1. LPR data shall be considered for official use only and shall only be shared for legitimate law enforcement purposes.

2. SPD personnel may accept database search requests from another law enforcement agency or grant access to the database to another agency, to identify vehicles and/or individuals, provided the following requirements are met:

   a. All permissible and prohibited uses of this policy are adhered to; and

   b. LPR data and search results may be disseminated to any law enforcement agency or official with a need to know such information the performance of official duties, provided the dissemination is for an authorized use as delineated in Section IV. B. and is subject to all state and federal laws on privacy, confidentiality, and dissemination.

3. Information sharing among law enforcement agencies should be dictated in accordance with established SPD policies.

4. When LPR data is disseminated outside of the agency, the reason(s) and identity of the authorized requesting person or agency shall be documented in the PremiereOne system and shall be titled as an Assist Outside Agency report and the LPR tab completed. The report shall contain information as to whom the information was released and for what purposes.

5. Release of data shall be subject to departmental policies, applicable LEIN regulations, requirements and standards including local, state, and federal regulations, including applicable statutes regarding, but not limited to evidence discovery and disclosure pursuant to the Freedom of Information Act (FOIA). FOIA requests shall be reviewed by the Support Services Administrator.

F. Retention

1. LPR data retention shall be in accordance with system capability; local, state, and federal regulations including City of Saginaw and State of Michigan retention requirements.

2. Any LPR data determined to have investigative, or prosecution value shall be exported to an authorized medium and maintained in accordance with applicable statutory time frames. If no extension of LPR data retention is required, the recordings may be destroyed in accordance with State of Michigan retention requirements and department procedures.

3. All disclosure of LPR data must be consistent with the agency's record release policy and applicable statutes regarding, but not limited to, evidence discovery and disclosure pursuant to the Freedom of Information Act. Any requests for such data should be reviewed by the Support Services Administrator.

V. REVISION RESPONSIBILITY

Responsibility for the continuous updating and revision of this order lies with the Chief of Police. Continuous shall be construed to mean when necessary or when mandated by law.

If this procedure conflicts with or supersedes any previous departmental order, procedure, or directive; to that extent the conflicting or superseded order is canceled.

BY ORDER OF:

Robert M Ruth

Robert M. Ruth
Chief of Police

	Office of St. Clair County Sheriff **DEPARTMENT ORDER**	Effective Date: 3-23-2023	Policy Number: 30.5
POLICY: **License Plate Reader Policy**			Page 1 of 3

A. Purpose: The purpose of this policy is to provide guidance for the capture, storage, and use of digital data obtained through the use of License Plate Reader (LPR) technology.

B. Policy: The policy of the St. Clair County Sheriff's Office is to utilize LPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public. All data and images gathered by the LPR are for the official use of this department. Because such data may contain confidential information, it is not open to public review.

C. Procedure:

1. The use of LPR systems is restricted to law enforcement and public safety related missions of this agency.

2. LPR systems and associated equipment and databases are authorized for official public safety purposes. Misuse of this equipment, databases, or data, may be subject the employee to disciplinary actions.

3. LPR systems, data, and associated media are the property of this agency and intended for use in conducting official business.

D. Administration

1. The Sheriff or designee shall designate "Administrator(s)" for LPR system deployment and operations that is responsible for the following:
   a) Establishing protocols for access, collection, storage, and retention of LPR data and associated media files.

b) Establishing protocols to preserve and document LPR "alerts" or "hits" that are acted on in the field or associated with investigations or prosecutions.
c) Establishing protocols to establish and ensure the security and integrity of data captured, stored, and/or retained by the LPR system.

2. Designated personnel shall check equipment on a regular basis to ensure functionality and camera alignment. Any equipment that falls outside expected functionality shall be reported immediately to Flock Safety.

3. LPR system repairs, hardware or software, shall be made by vendor technicians.

E. License Plate Reader Usage

1. Fixed LPR systems are passive systems. Live data is not viewed.

2. Fixed LPR systems shall monitor all license plates that come in contact wit the LPR camera. Information for legitimate public safety purposes will be accessed by police members as appropriate.

3. LPR systems may have the ability to notify the Administrator(s) and other personnel of a HIT from the system HOT LIST.

    a) HIT: Alert from the LPR system that a scanned license plate number may be in the National Crime Information Center (NCIC) or other law enforcement database for a specific reason including, but not limited to, being related to a stolen car, wanted person, missing person, domestic violence protective order, or terrorist-related activity.
    b) HOT LIST: A list of license plates associated with vehicles of interest compiled from one or more databases including, but not limited to, NCIC, SOS, LEIN, Local BOL's, etc.

4. If notification of a HIT is made, the process for verifying the HIT shall be the same as a LEIN or NCIC hit.

5. LPR data sharing and dissemination of LPR data should be considered law enforcement sensitive and can only be shared for legitimate law enforcement purposes:

    a) When LPR data is disseminated outside the agency it should be documented in the LPR system (i.e. case number/brief synopsis).
    b) Sharing of LPR data and information to third parties, including private litigants, is prohibited except to the degree required by law.
    c) Retention of LPR related data will be stored for a maximum of 30 days.
    d) LPR data that is deemed evidence in police related cases will be transferred to and retained in the department's digital evidence storage system.

F. Accountability

All data will be closely safeguarded and protected by both procedural and technological means. The following safeguards will be followed regarding access to and use of stored data:

a) All LPR data downloaded to the mobile workstation 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.
b) Members approved to access LPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department related civil or administrative action.

G. Releasing LPR Data

The LPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law.

Requests for LPR data by non-law enforcement or non-prosecutorial agencies will be processed like any other information request received through the Records Division.

STERLING HEIGHTS POLICE DEPARTMENT
GENERAL ORDER

GENERAL ORDER NUMBER:	6.81
SUBJECT:	**AUTOMATED LICENSE PLATE READERS (ALPR)**
DATE OF ISSUE:	12/12/2022
EFFECTIVE DATE:	12/12/2022
RESCINDS:	N/A

I. POLICY

It is the policy of the Sterling Heights Police Department to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public. The data and images gathered provide information and investigative resources to employees. The use and access of such systems and information shall be for law enforcement purposes only and in compliance with all applicable training, policies, procedures, rules, regulations, and laws.

II. PURPOSE

This purpose of this policy is to establish a minimum set of binding guidelines to govern the use of Automated License Plate Reader to include data collection, management and use of LPR data, and maintenance of LPR equipment.

III. AUTHORITY

Sterling Heights Police Department Manual of Rules, Articles I, II, and VI. Title 18 of the United States Code Chapter 123.2721 - Prohibition on release and use of certain personal information from State motor vehicle records.

IV. DEFINITIONS

A. Automated License Plate Reader (ALPR) System equipment consisting of cameras, computers, and computer software used to automatically recognize and interpret the characters on motor vehicle license plates. Digital images captured by the cameras are converted into data which is processed through the ALPR system.

B. Hot List A list of license plates associated with vehicles of interest compiled from one or more databases including, but not limited to: National Crime Information Center (NCIC), Michigan Secretary of State, local BOLOs, etc.

C. Vehicles of Interest Vehicles including, but not limited to, vehicles which are reported as stolen, display stolen plates or tags, are linked to missing and/or wanted persons, and vehicles flagged by the Secretary of State or other Law Enforcement agencies.

D. Hit An alert from the ALPR system that a scanned license plate number may be in the NCIC or other law enforcement database for a specific reason such as, but not limited to: stolen car, wanted and/or missing person, terrorist related activity, and AMBER alerts.

E. ALPR Administrator The Chief's designee(s), serves as the ALPR Administrator for the department.

V. PROCEDURES

A. Training:

1. No member of the Sterling Heights Police Department shall access ALPR data without first completing department approved training.

2. ALPR Administrator shall be responsible for planning and implementing all department approved training concerning the ALPR.

B. Automated License Plate Reader Confidentiality:

1. Use of the ALPR system, software, associated databases, and data is restricted exclusively to the Department's law enforcement functions. Information obtained from the ALPR, software, associated databases, and data shall not be used for personal reasons or for reasons inconsistent with the Department's law enforcement functions under any circumstances.

2. Misuse or abuse of the ALPR system, software, associated databases, or data may be subject to criminal prosecution, civil liability, and/or administrative sanctions, up to and including termination, pursuant to and consistent with the relevant collective bargaining agreements and Department policies.

3. Information obtained from the ALPR system, software, associated databases, and data shall not be disseminated to the public except as authorized by law.

4. Information obtained from the ALPR system, software, associated databases, and data may be disseminated to other law enforcement agencies or officers when it is to be used for law enforcement related functions, providing all of the following criteria are met:

    a. The law enforcement agency makes an official written request for the ALPR data through LEIN or via department email.
    b. The agency's identity, the person requesting the data, and the intended purpose must be documented in such a manner as to demonstrate compliance with this policy and retained on file with the vendor's software.
    c. A supervisor must approve the request.

C. Automated License Plate Reader Use:

1. The ALPR system, software, associated databases, and data may be used in conjunction with any routine patrol operation or criminal investigation. Reasonable suspicion or probable cause is not required before using an ALPR.

2. Officers shall be aware the ALPR system will not have access to real time data. Hot lists, NCIC, LEIN, etc. are updated on a regular basis, but not continually, therefore there may be a delay in entries and removals.

3. Upon receiving an alert, officers should verify the plate and the state of issuance match the hot list alert in the ALPR system.

4. Officers should then conduct a check of the plate in question in LEIN/NCIC to verify the entry.

5. Upon locating the vehicle officers shall visually verify that the license plate on the vehicle matches that of the image captured by the ALPR and the LEIN/NCIC check before proceeding with any investigative or enforcement action.

6. Officers are reminded that an alert alone shall not be the basis for police action. For example, if a vehicle is entered into the system because of its association with a wanted individual, Officers should attempt to visually match the driver to the description of the wanted subject prior to making the stop or should have another legal basis for making the stop.

D. Restrictions of Automated License Plate Reader Use:

1. The ALPR system shall only be used for official and legitimate law enforcement purposes. Only sworn police personnel and dispatchers shall have access to the ALPR system.

2. Invasion of Privacy: Except when done pursuant to a court order such as a search warrant, it is a violation of this policy to utilize the ALPR to record license plates on private property. The exception is license plates on private property that are exposed to public view.

3. Harassment or Intimidation: It is a violation of this policy to use the ALPR system to harass and/or intimidate any individual or group.

4. Personal Use: It is a violation of this policy to use the ALPR system for any personal purpose.

VI. RESPONSIBILITY

A. Automated License Plate Reader Administration:

1. The Chief of Police or designee is responsible for administrative oversight of the ALPR system operations and shall be responsible for the following:

   a. Ensuring access, collection, secure storage, and retention of ALPR data and associated media files are within policy guidelines.
   b. Ensuring ALPR reads and alerts or hits that are acted upon in the field or associated with arrests, investigations, and/or prosecutions are documented in the vendor's database.
   c. Ensuring that ALPR system audits are conducted on an annual basis. System audits shall be designed to ensure the integrity of data captured, stored, and/or retained and shall include a review of password security and system usage.

d. Ensuring that each employee who uses or has access to the ALPR system has completed department approved training and is certified to have access to the Law Enforcement Information Network (LEIN).

2. ALPR system repairs (hardware or software) shall be made by the current ALPR system vendor or a vendor approved by the Chief of Police.

B. Data Retention and Accountability:

1. All ALPR data will be stored on the current Vendor's server for a period of thirty (30) days. After thirty days the data shall be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a lawful action or order to produce records. In such circumstances, the applicable data shall be transferred to another digital media and stored according to current procedures.

2. All saved data shall be closely safeguarded and protected by both procedural and technological means. The Department will observe the following safeguards regarding access to and use of stored data:

a. All requests for access to historical ALPR data shall be logged in the ALPR system and the reason for the access must be recorded. The appropriate Sterling Heights Police Department case or incident number shall be documented in the request.
b. All ALPR data downloaded to a mobile workstation shall be accessible only through a login/password protected system capable of documenting all access of information by name, date, and time.

C. Administrative Audits:

1. It is the responsibility of the Chief of Police to ensure that an audit is conducted of ALPR detection browsing inquires at least once during each calendar year. The Sterling Heights Police Department will audit a sampling of the ALPR system utilization from the prior twelve (12) month period to verify proper use in accordance with this General Order. The audit shall randomly select at least ten (10) detection browsing inquiries conducted by Sterling Heights Police Department employees during the time period selected to determine if each meets the requirements of this General Order.

2. The audit shall be performed and documented by the ALPR Administrator in the form of a Memorandum to the Chief of Police. The memorandum shall include any data errors found so that such errors can be corrected. After review by the Chief of Police, the memorandum any associated documentation shall be filed in accordance with current Michigan State Police record retention policy.

_____

Dale Dwojakowski
Chief of Police

GENERAL ORDER

JULY 2023

AUTOMATED LICENSE PLATE READER

#72

72.0 PURPOSE AND SCOPE

This policy governs the use of Automated License Plate Reader (ALPR) technology by members.

72.1 POLICY

The policy of the Three Rivers Police Department (TRPD) is to utilize Automated License Plate Reader (ALPR) technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public. The intended use of ALPR technology is to assist officers with objective actionable leads needed to solve investigations and protect the community. All data and images gathered by the ALPR are for the official use of this department.

72.2 DEFINITIONS

Active ALPR Data: Active ALPR Data is information that is provided to a law enforcement official in real-time. Active ALPR Data includes alerts or notifications that a license plate number contained on an Alert List has been detected in the vicinity of an ALPR Unit.

Shared Data: ALPR Data is information that is collected from an outside agency that is law enforcement sensitive. Shared data is stored and accessed through the vendor's data-sharing platform with other law enforcement agencies. Shared information is not owned by the department and can only be used for law enforcement investigations.

Crime: As used herein, the term "crime" shall mean an act or the commission of an act that is forbidden or the omission of a duty that is commanded by a public law and that makes the offender liable to punishment by that law. The term "crime" includes acts of terrorism.

Historical ALPR Data: Historical ALPR Data consists of the dates, times, and locations of individually identifiable motor vehicles that are stored for future use and includes any ALPR Data not considered Active LPR Data.

ALPR Alert List Entry: An ALPR Alert List Entry or "Hot List" is entering a known license plate with a criminal predicate into the ALPR System.

ALPR Data: ALPR Data consists of all ALPR images and/or alerts that are active or historical in nature and stored within the ALPR System.

ALPR System: An ALPR System consists of the ALPR Units, communications network components, data server hardware, and software including any Optical Character Recognition (OCR) software and algorithms, all operating in an organized and coordinated manner.

ALPR Units: ALPR Units consist of imaging hardware which captures the image of the license plates, regardless of the types of cameras used or the deployment of the unit.

72.2 ALPR DATA COLLECTION

Owners of motorized vehicles driven on public thoroughfares are required by law to annually register their vehicles with their state bureau or department of motor vehicles and to attach license plates that are publicly and legibly displayed. Vehicle license plates generally consist of a series of alphanumeric characters that reference the license plate to the specific vehicle registered that captures the license plate's image, regardless of the types of cameras used or the unit's deployment numbers and letters.

c. The Global Positioning System (GPS) coordinates or other location information of the observation

d. The date and time of the observation.

e. Other information contained in the ALPR image aids in the identification of vehicles including, but not limited to, color, make, model, truck cap, etc.

The data captured by the ALPR Unit itself is entirely anonymous and is not considered personal identifying information. Officers can only identify the registered owner of a vehicle by querying a separate, secure state government database of vehicle license plate records, which is restricted, controlled, and audited. The federal Driver's Privacy Protection Act (DPPA) restricts access and prohibits the release of personal information from state motor vehicle records to ensure the privacy of citizens. 18 USC § 2721-2725.

72.3 ALPR DATA MAY BE COLLECTED FOR:

a. Supporting crime analysis techniques.

b. Alerting law enforcement officials of the proximity of a vehicle displaying a license plate number that is included on an Alert List.

c. Locating vehicles that have a known relationship to an individual who is reasonably suspected of having committed a crime.

d. Assisting Law Enforcement in locating missing or endangered persons.

72.4 ALPR DATA COLLECTION TECHNIQUES

ALPR Units may be deployed in any of the following manners:

a. In a Fixed Deployment, by being permanently mounted in a fixed location.

b. In a Mobile Deployment, by being mounted to a mobile vehicle, whether overtly or covertly, or by a handheld device.

72.5 ACCOUNTABILITY

All data will be closely safeguarded and protected by both procedural and technological means. The Three Rivers Police Department will observe the following safeguards regarding access to and use of stored data:

a. All ALPR data downloaded shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date, and time.

b. Officers 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 is related to a specific criminal investigation or department-related civil or administrative action.

c. ALPR system audits will be conducted on a regular base.

72.6 USE AND DISSEMINATION OF ALPR DATA

a. Members may access active ALPR data to be alerted in real-time to the location of vehicles on an active alert list. Entries on the alert list contain license plate information that is identifying a vehicle reported as:

1. Stolen or displaying a stolen license plate.
2. Associated with child abductions or missing and endangered persons.
3. Involved in an official law enforcement investigation when there is articulable suspicion linking the individual to a crime that has already been committed.

Generally, active ALPR alert entries should not be the sole reason for an investigatory stop. Officers should independently verify the ALPR alert entries through LEIN/NCIC databases or other means unless the officer has firsthand knowledge of the alert data.

c. Members with ALPR System may access historical ALPR Data to:

1. Identify and analyze the movement of vehicles reasonably related to individuals when there is articulable suspicion linking the individual to a crime that has already been committed.
2. Identify and analyze the movement of vehicles displaying license plate numbers contained in an Alert List.

d. Field Operations and Enforcement Actions:

1. All users of the ALPR system will *unselect* the following: Supervised Release, Protection Order, Violent Person, Immigration Violator, Sex Offender under the NCIC notification reasons and will not take any enforcement action if the ALPR system alerts solely for these reasons.

2. Custom Alert Lists that alert the entire organization or portions of the organization must be authorized by the detective or command officer.

3. When notified of a NCIC "hit" from the ALPR system, operators will verify the ALPR response through the Law Enforcement Information Network (LEIN) before taking enforcement action. An action shall not be based solely on the ALPR alert.

4. Occasionally, there may be errors in the ALPR system's reading of a license plate. Therefore, an alert alone is not a basis for police action.

5. Prior to initiation of a stop of a vehicle or other intervention based on an alert, operators will undertake the following:

   - Verification of a status on a hot list. An operator must confirm that the vehicle is still stolen, wanted, or otherwise of interest before proceeding (absent exigent circumstances). Without confirmation, a vehicle cannot be stopped solely on an ALPR alert and there must be a legal justification for the stop, such as a traffic violation, reasonable suspicion, or probable cause.

   - Visual verification of license plate number. Operators will visually verify that the license plate of interest matches identically with the image of the license plate number captured (read) by the ALPR, including both the alphanumeric characters of the license plate, state of issue and vehicle descriptors before proceeding.

6. After the stop of a vehicle or other intervention based on the alert:

   - The operator will notify their supervisor or authorized Alert List administrator of the positive hit and request that the plate be removed from the active Alert List unless the interest in the vehicle still exists.

d. Disseminating ALPR Data

1. Active and historical ALPR Data may be disseminated to law enforcement officials from other jurisdictions upon request or through shared data on the vendor platform. The requesting agency must provide the reason for the request, and it can only be used for official law enforcement investigations.

2. Non-Dissemination of historical ALPR Data to the Public.
   ALPR Data shall only be used for law enforcement purposes. ALPR Data will not be released to the public unless required by statute, court order, or when approved by the Chief of Police or designee to warn the community of a vehicle associated with an individual that poses an immediate threat of harm to the community or an individual.

72.7 RETENTION OF ALPR DATA

a. ALPR Data connected to a criminal investigation shall be retained as part of the investigation record and shall be subject to department retention and disposal schedules.

b. ALPR Data used to convict an individual, including but not limited to Query Responses, shall be retained as part of the TRPD case file as an external document and shall be subject to department retention and disposal schedules for that specific case and conviction.

c. ALPR Data that is not connected to an investigation or conviction shall be subject to 3rd party vendor retention and disposal schedules and are not to exceed 30 days.

72.8 ALPR TRAINING

Use of the department's ALPR System shall be limited to members who have completed training in accordance with this section and provided documentation of successfully completing that training.

WALKER POLICE DEPARTMENT

WALKER, MICHIGAN

SUBJECT: Flock Safety Camera System

1.0 PURPOSE

A. Provide guidelines on the proper use of the Crime Prevention license plate recognition (LPR) system, also commonly known as the Flock Safety Camera (FSC) System.

B. Provide accountability by ensuring the FSC system user respects constitutional and privacy rights.

C. Deter criminal behavior and assist in criminal investigations and prosecutions.

D. Allow for appropriate cooperation with businesses, institutions, condominium associations, homeowner associations, neighborhood associations, and other entities or groups seeking safety and security for specifically identified property.

E. Enhance the department's productivity and effectiveness, while enhancing community and officer safety with the use of the FSC systems.

2.0 POLICY

This policy applies to all law enforcement personnel and civilian personnel within the Walker Police Department who have access to the Flock Safety System. It is the policy of the Walker Police Department to ensure all employees are properly trained in the use of the FSC system.

3.0 DEFINITIONS

A. **Alert** – A visual and/or auditory notice that is triggered when the FSC system receives a potential "hit" on a license plate

B. **Fixed FSC system** – FSC cameras that are permanently affixed to a structure, such as a pole, traffic barrier, or a bridge.

C. **Hit** – A read matched to a plate within public view that has been registered on the agency's "hot lists" 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.

D. **Hot Lists** – License plate information 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. Departments of motor vehicles can provide lists of expired registration tags, and law enforcement agencies can interface their own locally compiled custom hot lists to the FSC system.

   These lists serve as an officer safety function as well as for investigative purposes. In addition to agency supported hot lists, designated 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 FSC system.

E. **FSC** – Flock Safety Camera System

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

4.0 PROCEDURES

The Walker Police Department FSC system will not have an audio recording feature, nor shall any modifications be made to the system to allow audio recording.

4.1 Authorized Uses and Users:

A. FSC systems, FSC data and associated media are the property of the Walker Police Department and are to be used only in conducting the agency’s official business.

B. Only trained LEIN certified law enforcement staff or dispatchers may access or search FSC systems, FSC data, and associated media.

C. The use of FSC systems associated equipment and databases are restricted to public safety-related missions of this agency and are authorized for officer public safety purposes only.

D. Except when done pursuant to a court order such as a search warrant, the FSC may be used only to record license plates of vehicles that are exposed to public view (e.g., vehicles 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).

4.2 The following uses of the FSC system are prohibited:

A. Use of the FSC 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.

B. Use of the FSC system or associated scan files or hot lists for any personal purpose.

4.3 Administration

A. The Detective Bureau Sergeant will have administrative oversight (The Administrator) for FSC system deployment and operations who is responsible for the following.

- Establishing protocols for access. To ensure proper operation and facilitate oversight of the FSC 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.

- Establishing protocols for the entry, collection, storage, and retention of FSC data and associated media files.

- Authorizing any requests for FSC systems use of data access according to the policies and guidelines of this agency.

B. 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 Flock Safety.

C. FSC system repairs, hardware, or software shall only be made by authorized technicians through Flock Safety.

4.4 Fixed Flock Safety Camera Systems (FSC) Usage

A. Fixed FSC system is a passive system, live data is not viewed.

B. Fixed FSC systems monitors all license plates that come in the FSC camera's view.

C. The Fixed FSC system provides the ability to search historical data. A log of such requests will be maintained by the system administrator.

D. All searches of the FSC system shall include a reason for the search, to include the case /CAD number and type of incident (e.g., 22-XXXX Robbery). Searches related to broadcasts by dispatch that do not have a case/CAD number, such as suspected drivers or vehicles wanted by other jurisdictions, will include “Broadcast” and the reason (e.g., Broadcast – GRPD Shooting Suspect Vehicle).

E. Fixed FSC systems may have the ability to notify the system administrator and/or other police personnel of a “hit” from the LPR system “hot list.”

4.5 Field Operations and Enforcement Actions

A. All users of the FSC system will unselect the following: Supervised Release, Protection Order, Violent Person, Immigration Violator, Sex Offender under the NCIC notification reasons and will not take any enforcement action if the FSC system alerts solely for these reasons.

B. Custom hotlists that alert the entire organization or portions of the organization must be authorized by a detective, sergeant, or command officer.

C. A Hotlist entry into the FSC system must be documented in the incident report. The report shall include all vehicle information, including probable cause, warrant information, or investigative purposes supporting the entry. The report shall be forwarded to the Detective Bureau.

D. The Detective Bureau Sergeant or designee will be responsible for entry, removal, and auditing of the custom hotlist information.

E. When notified of a NCIC “hit” from the FSC system, officers **shall verify** the FSC response through the Law Enforcement Information Network (LEIN) before taking enforcement action. Action shall not be based solely on the FSC alert.

F. Occasionally, there may be errors in the FSC systems read of a license plate. Therefore, an alert alone is not a basis for police action.

G. Prior to initiation of a stop of a vehicle or other intervention based on an alert, officers shall undertake the following:

- **Verification of a status on a hot list. An officer must confirm that the vehicle is still stolen, wanted, or otherwise of interest before proceeding (absent exigent circumstances). Without confirmation,**

a vehicle cannot be stopped solely on a FSC alert and there must be a legal justification for the stop, such as a traffic violation, reasonable suspicion, or probable cause.

- 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 FSC, including both the alphanumeric characters of the license plate, state of issue, and vehicle descriptors before proceeding.

- Because the FSC alert relates to a vehicle plate and may not relate to the person operating the vehicle, officers need reasonable suspicion and/or probable cause to make an enforcement stop of any vehicle (for example, if a vehicle is entered into the system because of its association with a wanted individual, officers shall attempt to visually match the occupant to the description of the wanted subject associated to the vehicle plate or BOL prior to making a stop or should have another legal basis for making the stop).

H. After the stop of a vehicle or other intervention based on the alert:

- The officer will notify the dispatch supervisor of the positive hit and request that the plate be removed from the hot list unless the interest in the vehicle still exists.

- The officer will also notify the on-call Detective of the removal via department e-mail or voicemail.

4.6 FSC Data Sharing and Dissemination

FSC data should be considered for official use only and can only be shared for legitimate law enforcement purposes.

A. Outside law enforcement agencies that are part of the FSC network may be allowed search access for legitimate law enforcement purposes. Command approval for each agency is required.
B. Trained Walker Police Department personnel may conduct searches of the FSC database for outside law enforcement agencies. Walker Police Department personnel will enter the requesting agency's name, the agency's case number, and incident type in the reason for search field (i.e., OCSD 22-XXXX Robbery). Only matching returns will be shared with the agency.

C. Outside law enforcement agencies requesting to receive alerts of hits from the FSC system must have a mutual aid agreement, letter of

understanding, or other agreement in place with the Walker Police Department and must have a Walker Police Department approved policy related to the FSC system. Command approval is required.

D. All custom hot list data entries into the FSC system for hits and alerts for outside law enforcement agencies will be completed by the Walker Police Department Detective Bureau Sergeant or designee.

4.7 Retention of FSC related photos and data

A. FSC related data is stored for a maximum of 30 days.

B. FSC data that is potential evidence must be transferred to and retained in the department's digital evidence storage system.

4.8 Business and Homeowner Association Partnerships

A. Business Entities and Homeowner Associations

1. May purchase and install FSC technology

2. May provide inquiry/view access to the Walker Police Department.

B. Any publicly/privately owned Crime Prevention FSC Camera System that stores data on City of Walker must be done according to the specifications, policies, and guidelines of this agency.

D. Any publicly/privately owned Crime Prevention FSC Camera System will not have access to search or view FSC data stored on the City of Walker databases.

Keith Mankel
Chief Of Police

WALLED LAKE POLICE
GENERAL ORDER

SUBJECT:	DATE OF ISSUE	EFFECTIVE DATE	NUMBER
Automatic License Plate Readers (ALPR)	July 31, 2024	July 31, 2024	24-04
REFERENCE:		CANCELS	EXPIRATION DATE
			Indefinite

I. Purpose

To set forth guidelines and procedures regarding the authorized use of automatic license plate readers (ALPR) known as Flock Safety Cameras (FSC).

II. Policy

ALPR technology accessed via the FSC system will be used for official law enforcement purposes. This technology can assist with law enforcement investigations, as well as the safety and security of the Walled Lake community. FSC's can either be fixed or portable in nature and will be placed at locations which will maximize the law enforcement efforts of the Walled Lake Police Department.

III. Definitions

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

B. HIT – A read matched to a plate within public view that has been registered on the agency's "hot lists" 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.

C. HOT LISTS – License plate information 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. Michigan Secretary of State (SOS) or other state Departments of Motor Vehicles (DMV) can provide lists of expired registration tags, and law enforcement agencies can interface their own locally compiled custom hot lists to the FSC system.

These lists serve as an officer safety function as well as for investigative purposes. In addition to agency supported hot lists, designated users may also manually add license plate numbers to hot lists to be alerted if a vehicle license plate of interest is read by the FSC system.

D. READ – Digital images of license plates, vehicles, and associated metadata such as date, time, and geographic coordinates associated with the vehicle image capture that are captured by the FSC system.

E. AUTHORIZED USER – Department member that has been granted permission to utilize the FSC system by the Chief of Police or his/her designee.

F. ADMINISTRATOR – Department member that has been designated by the Chief of Police or his/her designee to be the point of contact for the FSC system.

IV. Use of the FSC System

A. Authorized users will access the FSC system with their individual credentials for official business.

B. Searches are only available from the date of the search and the previous 30 days. If a search result populates information that you need to keep, you will have to export the file to PDF and save it.

C. Hits from the FSC system should be viewed as informational; created solely to bring the users attention to specific vehicles that may be associated with criminal activity.

D. If choosing to be alerted of a hit by email or text message, the alert must be directed to either your authorized City of Walled Lake email address or work cell phone number. Personal email addresses and phone numbers should not be used.

E. If notified of a hit, users will confirm that the information provided by the FSC system matches the actual vehicle of interest before acting on it. Resources such as LEIN, NCIC, SOS, and CLEMIS are possible ways, depending on the type of hit, to seek confirmation.

1. Without prior confirmation that a vehicle is still wanted, stolen, or otherwise of interest, a vehicle cannot be stopped solely on a FSC alert and there must be a legal justification for the stop (i.e., traffic violation, reasonable suspicion, probable cause).

2. Officers shall ensure visual verification that the license plate number on the vehicle, state of issue, and vehicle characteristics matches the FSC alert before proceeding.

3. FSC alerts relate to a vehicle's plate and may not relate to the person who is operating the vehicle. Officers may need to develop reasonable suspicion or probable cause before taking enforcement action, based on the totality of the circumstances.

V. Restrictions

A. Only those persons authorized by the Chief of Police, or his/her designee will have access to the FSC system.

B. For each search in the FSC system, the user will input the reason why the search is being conducted. The search reason will include the case report/call for service number (if applicable) as well as a short description of the type of incident (i.e., LFA, robbery, flee/elude, etc.).

C. All searches, including the search reason inputted by the user in the FSC system are saved by Flock. Therefore, all searches by users can be audited at any time by an administrator.

D. Use of the FSC system is restricted to authorized law enforcement purposes. Misuse, abuse, and personal use of the system is strictly prohibited.

1. The FSC system shall not be used to search for or investigate someone based solely on a person's or group's race, gender, religion, political affiliation, nationality, ethnicity, sexual orientation, disability, or other protected class.

VI. Data

A. Data ownership is covered in the terms and conditions of Flock. All data not owned by Flock is considered the property of the Walled Lake Police Department.

B. Data retained by users, as deemed necessary for investigations or otherwise, shall be in accordance with the Walled Lake Police General Order on evidence collection. Retention of said data will conform with Michigan General Schedule #11.

C. FSC system data shall not be disclosed to the public except as authorized or required by law.

VII. Accountability

A. Users and any related uses of the FSC system are subject to audit at any time.

B. Users will keep their login information confidential.

C. Unauthorized users shall not have access to the FSC system.

VIII. Training

A. New authorized users will be trained in how to operate the FSC system by an existing authorized user or Flock representative.



L. Dennis Whitt

Director of Public Safety/City Manager

White Lake Township Police Department

Chief of Police
Daniel T. Keller

General Order	SUBJECT	Number of Pages
3.5.8	Public Safety Vehicle Locating System	7
This Directive Supersedes All Previously Issued Correspondence Relative To This Topic		
MLEAC Standards: N/A	Effective Date: 06/07/2023	Revised Date: 01/24/2024

I. Purpose

The purpose of this policy is to provide guidance for the capture, storage, and use of digital data obtained through the use of the Vehicle Locating System (VLS). This policy applies to all members of the White Lake Township Police Department.

II. Policy

The policy of the White Lake Township Police Department is to utilize the Vehicle Locating System (VLS) technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public. All data and images gathered by the VLS are for the official use of this department. Because such data may contain confidential information, it is not open to public review. The VLS will be used to capture the rear of vehicles, and are not intended for facial recognition.

III. Definitions

VLS Operator - Trained Department members who may utilize VLS system/equipment. VLS operators may be assigned to any position within the Department, and the VLS Administrator may order the deployment of the VLS systems for use in various efforts.

VLS Administrator - The Administrative Lieutenant serves as the VLS Administrator for the Department.

Hot List - A list of license plates associated with vehicles of interest compiled from one or more databases including, but not limited to, NCIC, SOS, LEIN, Local BOL's, etc.

Vehicles of Interest - Including, but not limited to vehicles which are reported as stolen; display stolen license plates or tags; vehicles linked to missing and/or wanted persons and vehicles flagged by the Michigan Secretary of State or authorized law enforcement agencies.

Detection - Data obtained by an VLS of an image (such as a license plate) within public view that was read by the device, including potential images (such as the plate and description of vehicle on which it was displayed), and information regarding the location of the VLS system at the time of the VLS's read.

Hit - Alert from the VLS system that a scanned license plate number may be in the National Crime Information Center (NCIC) or other law enforcement database for a specific reason including, but not limited to, being related to a stolen car, wanted person, missing person, domestic violation protective order, or terrorist-related activity.

IV. Guidelines for Use

A. Administration

1. The Vehicle Locating System (VLS) allows for the automated detection of license plates along with the vehicle make, model, color and unique identifiers through the White Lake Township Police Department's VLS's system and the vendor's vehicle identification technology. The technology is used by the White Lake Township Police Department to convert data associated with vehicle license plates and vehicle descriptions for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates and missing persons. It may also be used to gather information related to active warrants, homeland security, electronic surveillance, suspect interdiction, and stolen property recovery. All installation and maintenance of VLS equipment, as well as VLS data retention and access, shall be managed by Chief of Police or Designee(s). The Chief of Police or Designee(s) will assign members under his/her command to administer the day-to-day operation of the VLS equipment and data.

B. VLS Administrator

The Administrative Lieutenant or Designee(s) shall be responsible for compliance with the requirements of Civil Codes.

1. Only properly trained police employees are allowed access to the VLS system or to collect VLS information.

2. Ensuring that training requirements are completed for authorized users.

3. VLS system monitoring to ensure the security of the information and compliance with applicable privacy laws.

4. The title and name of the current designee in overseeing the VLS operation is maintained. Continually working with the Custodian of Records on the retention and destruction of VLS data.

C. Operations

Use of an VLS is restricted to the purposes outlined below. Department members shall not use, or allow others to use the equipment or database records for any unauthorized purpose(s).

1. An VLS shall only be used for official law enforcement business.

2. An VLS may be used in conjunction with any routine patrol operation or criminal investigation; reasonable suspicion or probable cause is not required before using an VLS.

3. Partial license plates and unique vehicle descriptions reported during major crimes should be entered into the VLS system in an attempt to identify suspect vehicles.

4. No member of this department shall operate VLS equipment or access VLS data without first completing department-approved training.

5. The officer shall verify an VLS response through the Law Enforcement Information Network (LEIN) before taking enforcement action that is based solely on a VLS alert. Once an alert is received, the operator shall confirm that the observed license plate from the system matches the license plate of the observed vehicle. Before any law enforcement action is taken because of a VLS alert, the alert will be verified through a LEIN inquiry via MDC or through Dispatch. Members will not take any police action that restricts the freedom of any individual based solely on an VLS alert unless it has been validated. Because the VLS alert may relate to a vehicle and may not relate to the person operating the vehicle, officers are reminded that they need to have reasonable suspicion and/or probable cause to make an enforcement stop of any vehicle. (For example, if a vehicle is entered into the system because of its association with a wanted individual, Officers should attempt to visually match the driver to the description of the wanted subject prior to making the stop or should have another legal basis for making the stop.)

6. Hot Lists. Designation of hot lists to be utilized by the VLS system shall be made by the VLS Administrator or his/her designee. Hot lists shall be obtained or compiled from sources as may be consistent with the purposes of the VLS system set forth in this Order. Hot lists utilized by the Department's VLS system may be updated by agency sources more frequently than the Department may be uploading them and thus the Department's VLS system will not have access to real time data. Occasionally, there may be errors in the VLS system's read of a license plate. Therefore, an alert alone shall not be a basis for police action (other than confirming the vehicle of interest information is correct). Prior to initiation of a stop of a vehicle or other intervention based on an alert, Department members shall undertake the following:

    a. Verification of status on a Hot List. An officer must receive confirmation, from a White Lake Township Police Department Communications Dispatcher 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 VLS, including both the alphanumeric characters of the license plate, state of issue, and vehicle descriptors before proceeding. Department members alerted to the fact that an observed motor vehicle's license plate is entered as a Hot Plate (hit) in a specific BOL (be on the lookout) 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 a Department member would have a lawful basis to stop the vehicle.

    c. Department members will clear all stops from hot list alerts by indicating the positive VLS Hit, i.e., with an arrest or other enforcement action. If it is not obvious in the text of the call for service as to the correlation of the VLS Hit and the arrest, then the Department member shall update with the Communications

Dispatcher and original person and/or a crime analyst inputting the vehicle in the hot list (hit).

d. All entries and updates of specific Hot Lists within the VLS system will be documented by the requesting Department member within the appropriate general offense report. As such, specific Hot Lists shall be approved by the VLS Administrator (or his/her designee) before initial entry within the VLS system. The updating of such a list within the VLS system shall thereafter be accomplished pursuant to the approval of the Department member's division supervisor. The hits from these data sources should be viewed as informational; created solely to bring the officers attention to specific vehicles that have been associated with criminal activity or other investigations.

   All vehicle and suspect information entered into the VLS system will contain the following information as a minimum:

   1. Entering Department member's name.
   2. Related case number.
   3. Short synopsis describing the nature of the originating investigation.

V. Training

The Administrative Lieutenant should ensure that members receive department-approved training for those authorized to use or access the VLS system. No member of this Department shall operate VLS equipment or access VLS data without first completing Department-approved training.

VI. Login/Log-Out Procedure

To ensure proper operation and facilitate oversight of the VLS 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. Dispatchers may use Dispatchers group credentials for access, the Dispatch Station one Dispatcher will be responsible for oversight of the system.

VII. Permitted/Impermissible Uses

A. The VLS system, and all data collected, is the property of the White Lake Township Police Department. Department personnel may only access and use the VLS system for official and legitimate law enforcement purposes consistent with this Order. The following uses of the VLS system are specifically prohibited:

   1. Invasion of Privacy: Except when done pursuant to a court order such as a search warrant, it is a violation of this Policy to utilize the VLS to record license plates except those of vehicles that are exposed to public view (e.g., vehicles 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).

2. Harassment or Intimidation: It is a violation of this Order to use the VLS system to harass and/or intimidate any individual or group.

3. Use Based on a Protected Characteristic. It is a violation of this Order to use the VLS system or associated scan files 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. Personal Use: It is a violation of this Policy to use the VLS system or associated scan files or hot lists for any personal purpose.

5. First Amendment Rights. It is a violation of this policy to use the VLS system or associated scan files or hot lists for the purpose or known effect of infringing upon First Amendment rights.

B. Anyone who engages in an impermissible use of the VLS system or associated scan files or hot lists may be subject to:

1. Criminal prosecution,

2. Civil liability, and/or

3. Department Discipline, up to and including termination, pursuant to and consistent with the relevant collective bargaining agreements and Department General Orders.

VIII. Vehicle Locating System Alerts or "Hits"

A. Patrol Officers on duty shall have the Flock Safety system, with alerts activated, running on their vehicle's mobile data computer at all times during their working shift.

B. Dispatch shall have the Flock Safety system, with alerts activated, running on the dedicated Flock computer and viewable in Dispatch at all times during their working shift.

1. Once an alert is populated, Dispatch will view the alert and run the plate in LEIN/SOS to confirm the validity.

2. If the alert appears valid, a BOL will be sent to all on duty patrol vehicles. A CFS will be created and assigned to the area or closest available Patrol Unit.

3. If the alert is not valid, a CFS will be created and assigned to the dispatcher. The CFS shall document why the alert was found not to be valid. Example: the alert was for license plate "ABC123", and the photo on the alert shows the plate is "ABC1234", but the "4" is partially obstructed causing the system to not read it.

C. Once the vehicle identified in the alert is located, the Officer shall verify the information provided by the alert.

1. Before any law enforcement action is taken because of a VLS alert, the alert will be verified through a LEIN inquiry via MDC or through Dispatch. Members will not take any police action that restricts the freedom of any individual based solely on an VLS alert unless it has been validated.

D. Once the validity of the information has been established through LEIN or SOS, the Officer shall take necessary enforcement action. Example: Stolen Vehicle, Stolen Plate, Wanted Person.

E. If the BOL vehicle is unable to be located, or there is not an Officer available to investigate, the CFS will be documented with normal BOL procedures.

IX. Data Collection and Retention

The Chief of Police or Designee(s) is responsible for ensuring systems and processes are in place for the proper collection and retention of VLS data. Data will be transferred to the designated storage in accordance with department procedures.

All VLS data downloaded to the server should be stored for no longer than one year, and in accordance with the established records retention schedule. Thereafter, VLS data should be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a discovery request or other lawful action to produce records. In those circumstances the applicable data should be attached to CLEMIS report or downloaded from the server onto portable media and booked into evidence.

VLS vendor, Flock Safety will store the data (data hosting) and ensure proper maintenance and security of data stored in their data towers. Flock Safety will purge their data at the end of the 30 days of storage. However, this will not preclude WLTPD from maintaining any relevant vehicle data obtained from the system after that period pursuant to the established White Lake Township Police Department's retention schedule mentioned above or outlined elsewhere.

Restrictions on use of VLS Data**:** Information gathered or collected, and records retained by the vendor (Flock Safety cameras) or any other WLTPD VLS system will not be sold, accessed, or used for any purpose other than legitimate law enforcement or public safety purposes.

X. Accountability and Safeguards

All data will be closely safeguarded and protected by both procedural and technological means. The White Lake Township Police Department will observe the following safeguards regarding access to and use of stored data:

A. All non-law enforcement requests for access to stored VLS data shall be processed in accordance with applicable law.

B. All VLS data downloaded to the mobile workstation shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date, and time.

C. Persons approved to access VLS data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action.

D. Such VLS data may be released to other authorized and verified law enforcement officials and agencies for legitimate law enforcement purposes.

E. Every VLS Detection Browsing Inquiry must be documented by either the associated White Lake Township Police Departments case number or incident number, and/or a reason for the inquiry.

XI. VLS Data Detection Browsing Audits

It is the responsibility of the Administrative Lieutenant or Designee(s) to ensure that an audit is conducted of VLS detection browsing inquiries at least once during each calendar year. The Department will audit a sampling of the VLS system utilization from the prior 12-month period to verify proper use in accordance with the above authorized uses. The audit shall randomly select at least 10 detection browsing inquiries conducted by department employees during the preceding six-month period and determine if each inquiry meets the requirements established in policy section.

The audit shall be documented in the form of an internal department memorandum to The Chief of Police. The memorandum shall include any data errors found so that such errors can be corrected. After review by the Chief of Police or Designee(s), the memorandum and any associated documentation shall be filed and retained by WLTPD.

XII. Releasing VLS Data

The VLS data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law.

A. The agency makes a request for the VLS data that includes:

1. The name of the agency.

2. The name of the person requesting.

3. The intended purpose of obtaining the information.

B. The request is reviewed by a division supervisor or an authorized designee and approved before the request is fulfilled.

C. The approved request is retained on file. Requests for VLS data by non-law enforcement or non-prosecutorial agencies will be processed as provided in General Orders.

WIXOM POLICE DEPARTMENT GENERAL ORDER			
Order Subject License Plate Recognition System (LPR)			Order Number M-023
Revision Date 1-29-2024	Effective Date 1-30-2024	Review Date 1-30-2025	Expiration Date N/A
MACP Function Miscellaneous		MACP Standard(s) N/A	
Issued By P. Langmeyer, Chief of Police		Rescinds N/A	Number of Pages 5

I. PURPOSE

The License Plate Reader System (LPR) is a computer-based platform which utilizes cameras to capture license plate information. The LPR system captures an image of a license plate and converts it to a file. This file is compared to various hotlists generated by local, state, and federal law enforcement agencies, including the National Crime Information Center (NCIC). Information obtained from these sources generate an alert when there is a hit. License plate readers have enhanced law enforcement's ability to locate and recover stolen vehicles, apprehend fugitives, locate missing and/or endangered persons, and assist in criminal investigations. The Wixom Police Department will utilize license plate readers to further legitimate law enforcement goals and enhance public safety. The purpose of this policy is to provide officers with guidelines on the proper use of License Plate Recognition Systems, commonly known as license plate reader systems (LPR).

II. POLICY

It is the policy of the Wixom Police Department that LPR systems use shall be restricted to trained personnel and for legitimate law enforcement purposes only.

III. DEFINITIONS

A. LPR: License Plate Recognition/License Plate Reader

B. Vehicles of Interest - Including, but not limited to vehicles which are reported as stolen; display stolen license plates or tags; vehicles linked to missing and/or endangered persons, wanted persons, and vehicles flagged by the Michigan Secretary of State or authorized law enforcement agencies.

C. Alert: A visual and/or auditory notice that is triggered when the LPR system receives a potential "hit" on a license plate.

D. 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.

E. Hot List: Data files extracted from law enforcement databases which contain a listing of stolen license plates, stolen vehicles, wanted persons, and other vehicles or persons actively being sought by a law enforcement agency such as Amber Alert or Silver Alert vehicles or persons.

IV. STANDARDS FOR USE

A. LPR Administrator

1. The administrator oversees LPR system to ensure the security of the information and compliance with applicable privacy laws.

2. The LPR Administrator shall be responsible for:

   a. All installation and maintenance of LPR equipment, as well as LPR data retention and access.

   b. The administrator will ensure training requirements are completed for all users.

   c. No member of this department shall operate LPR equipment or access LPR data without first completing department-approved training.

3. The LPR Administrator shall be a Sergeant, assigned by the Office of the Chief.

B. Operations

1. Only properly trained police employees are allowed access to the LPR system or to collect LPR information.

2. Department members shall not use or allow others to use the equipment or database records for any unauthorized purpose(s).

3. An LPR shall only be used for official law enforcement business.

4. An LPR may be used in conjunction with any routine patrol operation or

criminal investigation; reasonable suspicion or probable cause is not required before using an LPR.

5. Partial license plates and unique vehicle descriptions reported during major crimes should be entered into the LPR system to identify suspect vehicles.

6. Officers Should be aware the LPR system does not provide real-time data. Hotlists and other information contained in the system updates regularly, but not continually, resulting in a delay in entries and removals.

7. Officers should be aware the LPR system may erroneously read a license plate. The information obtained by an LPR should be confirmed before acting.

8. Upon receiving an alert, officers shall verify the license plate and state of issuance match the alert in the LPR system, including comparison to photos provided by the LPR.

9. Officers shall conduct a LEIN/NCIC check of the plate to verify the information provided by the LPR system.

10. Upon locating a vehicle subject to an alert, officers shall visually verify the license plate on the vehicle in question matches the image of the license plate captured by the LPR, and the LEIN/NCIC check before proceeding with any investigative or enforcement action.

    a. Any alert received by an LPR shall not be the sole basis for police action.

11. Any employee conducting an LPR search shall enter a valid reason for the search in the “Search Reason” field. Search reasons should include terms like “LFA”, “UDAA”, and similar incident descriptors. When practical, incident case numbers or other more accurate descriptors should be used.

D. Login/Logout Procedure

1. 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 can be fully audited.

E. Prohibitions

1. The LPR system, and all data collected, is the property of the Wixom Police Department. Department personnel may only access and use the LPR

system for official and legitimate law enforcement purposes consistent with this General Order. The following uses of the LPR system are prohibited:

a. Invasion of Privacy: Except when done pursuant to a court order such as a search warrant, it is a violation of this policy to utilize the LPR to record license plates except those on vehicles that are in the public view (e.g., vehicles 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).

b. Harassment or Intimidation: It is a violation of this directive to use the LPR system to harass and/or intimidate any individual or group.

c. Use Based on a Protected Characteristic. It is a violation of this directive to use the LPR system or associated scan files or hot lists solely because of a person's race, gender, religion, political affiliation, nationality, ethnicity, sexual orientation, disability, or other classification protected by law.

d. Personal Use: It is a violation of this order to use the LPR system or associated scan files or Hot Lists for any personal purpose.

e. Anyone who engages in an impermissible use of the LPR system or the associated scan files or Hot Lists may be subject to Department discipline, civil action and/or criminal prosecution.

V. DATA COLLECTION AND RETENTION

A. LPR system data obtained through LPR infrastructure will be securely maintained by the system manufacturer for 30 days. LPR data shall not be maintained by the department unless the data is needed to support criminal investigations.

B. LPR system data and notifications utilized to support criminal investigations shall be saved by the department. This data will be saved in the physical case file and/or uploaded into the CLEAR case file and shall be retained pursuant to department records retention guidelines.

VI. RELEASING LPR DATA

A. The LPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law.

B. Upon sharing data with other law enforcement agencies, officers shall indicate on the query, in the search reason field, the reason for the search, the requesting officer's name and agency.