BLOOMFIELD TOWNSHIP POLICE DEPARTMENT

POLICIES AND PROCEDURES

FLOCK CAMERAS			5.14
MACP STANDARDS:		AMENDS:	
EFFECTIVE:	02/14/2024	RESCINDS:	

I. POLICY

It is the policy of the Bloomfield Township Police Department to utilize Automated License Plate Readers (ALPRs) technology to capture and store digital license plate data and images, while recognizing the established privacy rights of the public. All data and image gathered by the ALPRs are for official Department use only. Information obtained may be confidential, therefore it is not open to the public.

II. DEFINITIONS

A. Automated License Plate Readers (ALPR): A device that uses cameras and computer technology to compare digital images to a list of known information of interest. The ALPR allows for automated detection of license plates along with vehicle make, model, color, and unique identifiers through the vehicle's identification technology. The technology is used by the Bloomfield Township 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, homeland security, electronic surveillance, suspect interdiction, and stolen property recovery.

B. ALPR Administrator: The Chief of Police or his or her designee, serves as the ALPR Administrator for the Department and shall be responsible with laws and civil codes. Ensures that all training requirements are completed for authorized users. ALPR system monitoring to ensure the security of the formation and compliance. The administrator works with the Custodian of Records on the retention and destruction of ALPR data.

C. ALPR Operator: Trained department members who may utilize ALPR system/equipment.

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

E. Hit/Alarm: 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, a wanted person, missing person, domestic violation protective order or terrorist-related activity.

F. Hot List: Data files extracted from the law enforcement databases including, but not limited to: NCIC, SOS, LEIN, and local police department Be on the Lookouts (BOLO).

G. Vehicles of Interest: Included but not limited to vehicles that are reported stolen, display stolen license plates or tags, vehicles linked to missing and /or wanted persons and vehicles flagged by the Secretary of State Administration (SOS) or a law enforcement agency.

III. OPERATIONAL PROCEDURES

A. Operations

1. Use of an APLR 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). Misuse of the ALPR technology is subject to discipline.

2. Only properly trained sworn officers or select non-sworn staff are permitted to access the ALPR system or to collect ALPR data.

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

4. 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.

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

6. Authorized users shall complete department approved training prior to using the ALPR system.

7. ALPR responses shall be verified through the Law Enforcement Identification Network (LEIN) before taking enforcement action that is based solely on the ALPR alert.

a. 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.

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

c. 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 its association with a wanted individual, Officers should attempt to visually match the driver description of the wanted subject prior to making the stop or should have another legal basis for the stop.)

B. Hot Lists

1. Designations of hot lists to be utilized by the ALPR system shall be made by the ALPR Administrator or his/her designee.

2. 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 do the following:

a. Verification of status on a Hot List: Officer's must receive confirmation through a LEIN inquiry by MDC or through Dispatch that the license plate entered as stolen, wanted, or otherwise of interest before proceeding (absent exigent circumstances).

b. Visual verification of license plate number: Officer's shall visually verify that the license plate of interest matches 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 before proceeding.

c. Department members alerted to a Hot List 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 stopping the vehicle.

d. 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 call for service or incident report.

e. Hot List entries and updates shall be approved by a supervisor before entry into the ALPR system.

f. Hits from these data sources should be viewed as informational; created solely to bring the officers' attention to specific vehicles.

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

(1) Entering Department member's name and badge number
(2) Related case number
(3) Short synopsis describing the nature of the originating call

IV. MONITORING OPERATIONS

A. Dispatchers shall ensure that the FLOCK ALPR Safety application is active in the telecommunications center and signed into the system.

B. Dispatchers shall monitor the system for any Hot List alerts.

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

1. Felony wanted vehicle
2. Stolen vehicle
3. Warrants of a serious nature
4. Amber Alerts/Missing children
5. Involuntary missing people

D. 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.

V. TRAINING

A. It is the responsibility of the ALPR Administrators or designee to ensure that all authorized users shall receive department-approved training for the use and accessing the ALPR system.

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

VI. LOGIN/LOGOUT PROCEDURE

A. 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 and reviewed by the Bloomfield Township Police Department.

VII. IMPERMISSIBLE USES

A. The ALPR system, and data collected, is the property of the Bloomfield Township Police Department. Department personnel may only access and use the ALPR system for official and legitimate law enforcement purposes consistent with this policy.

B. The following uses of the ALPR system are strictly prohibited:

1. Invasion of privacy

a. 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 (e.g., vehicles visible to public view are on a public road or highway, in a place where members of the public have access, such as parking lots or business establishments)

2. Harassment or intimidation

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

3. Use based on protected characteristics

a. 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.

VIII. PERSONAL USE

A. 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 limited to, using cellular phones, in any format or any video, audio, or still photography generated from the ALPR application or associated files or Hot Lists for personal use.

IX. FIRST AMENDMENT RIGHTS

A. It is a violation of this policy to use the ALPR system or associated files or Hot Lists for the purpose of effect of infringing upon First Amendment rights.

B. It is a violation of this policy to use the ALPR system for traffic enforcement, or the enforcement of civil infractions and civil judgements.

C. Any employee who engages in or allows the impermissible use of the ALPR system or associated files, Hot Lists, or scan files may be subject to:

1. Criminal Prosecution
2. Civil Liability
3. Discipline, up to and including termination

X. DATA COLLECTION AND RETENTION

A. The Chief of Police and/or their designee is responsible for ensuring systems and processes are in place for the proper collection and retention of ALPR data.

B. ALPR vendor, FLOCK Safety will store the data to 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.

C. Any data retrieved from the ALPR system, such as investigative search results for a criminal case, shall be stored in the Bloomfield Township Police Department's digital evidence management system in accordance with the Property and Evidence Policy.

XI. ACCOUNTABILITY AND SAFEGUARDS

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

1. 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.

2. Employees approved to access ALPR data under these guidelines are permitted to access that 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.

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

4. Every ALPR Detection Browsing Inquiry must be documented by the associated Bloomfield Township Police Department incident number and the reason for the inquiry.

XII. ALPR DATA DETECTION BROWSING AUDIT

A. It is the responsibility of the Chief of Police or their designee to ensure that an audit is conducted of the ALPR Detection Browsing Inquiries bi-annually. 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 authorized users. The audit shall randomly select at least 10 inquiries to determine if each inquiry meets the requirements established by policy. The audit shall be documented on a department memorandum to the Chief of Police. The report shall include any data errors found and any violations of this policy.

XIII. RELEASING ALPR DATA

A. 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. 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 purpose for obtaining the information.

B. The request is reviewed by the Chief of Police or their designee and approved before the request is fulfilled.

C. The request is retained on file.

D. Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be declined unless otherwise authorized by the FOIA.

E. Any changes in technology which becomes more intrusive (i.e. facial recognition) shall be presented to Township Board for review.

I have read and understand this Policy.