Personal Privacy Statement

A: License Plate Readers (LPR) capture point in time data on a vehicle, not a person.

B: LPR does not capture personal information; it is anonymous data. A string of numbers and letters with a date, time, and location – That is all. It is only with a defined permissible purpose that law enforcement may "link" a license plate to an individual using another system to access DMV data.

C: The LPR interface allows for end-users to report and correct misreads, or data errors. Our vendors, Vigilant Solutions and 3M, employ an OCR Engine Improvement Diagnostics tool to monitor the performance of its various OCR engines around the world. The OCR Engine Improvement Diagnostics tool works by collecting random samples of anonymous data from both mobile and fixed systems deployed in the field. The data collected includes elements such as character height, system type (fixed or mobile), agency ID, OCR engine version, quality score, and other anonymous bits of data that allow Vigilant Solutions to continuously monitor and improve the performance of its engines. Using this data, Vigilant Solutions' team of over 60 software engineers identifies and investigates potential issues that may result from new license plate designs, aging of the plate population, or even improper camera aiming. Once issues are identified and confirmed, the Vigilant Solutions team works to quickly correct the issues.

License Plate Reader (LPR) Standard Operating Procedures.

The following procedures will be followed for the LPR system as per LVPD policy section 427.2.1:

A: The La Verne Police department is currently using Vigilant Solutions to provide our fixed Automated License Plate Reader (ALPR) cameras and 3M for our mobile ALPR cameras. All data collected by our ALPR cameras are downloaded into Vigilant's LEARN database.

B: The current system administrators have been designated by the Chief of Police as Lieutenant Chris Fenner and Information Systems Specialist Jose Reyes.

C: Only personnel who have been trained on the system can log in and/or use it. The training will either be facilitated by the system administrator or by the vendor provided online course. Only qualified personnel who have passed the department training will be provided with a log on to the system. Employees will only use their log on credentials to access APLR data for official law enforcement purposes. Employees will not share their log on credentials or password with anyone.

D: The system administrators will conduct regular, routine audits and random inquiries into the ALPR database to ensure adherence to the department's usage policy. An official case number and reason will be provided for each inquiry into the system.

Automated License Plate Readers (ALPRs)

427.1 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.

427.2 ADMINISTRATION

The ALPR technology, also known as License Plate Recognition (LPR), allows for the automated detection of license plates. It is used by the La Verne 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, 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 Support Services Division Commander. The Support Services Division Commander will assign members under his/her command to administer the day-to-day operation of the ALPR equipment and data.

427.2.1 ALPR ADMINISTRATOR

The Support Services Division Commander shall be responsible for developing guidelines and procedures to comply with the requirements of Civil Code § 1798.90.5 et seq. This includes, but is not limited to (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

(a) A description of the job title or other designation of the members and independent contractors who are authorized to use or access the ALPR system or to collect ALPR information.

(b) Training requirements for authorized users.

(c) A description of how the ALPR system will be monitored to ensure the security of the information and compliance with applicable privacy laws.

(d) Procedures for system operators to maintain records of access in compliance with Civil Code § 1798.90.52.

(e) The title and name of the current designee in overseeing the ALPR operation.

(f) Working with the Custodian of Records on the retention and destruction of ALPR data.

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

427.3 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 (Civil Code § 1798.90.51; Civil Code § 1798.90.53).

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

Adoption Date: 2016/03/24

(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-equipped cars 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 department, state or federal data unless otherwise authorized to do so.

(f) If practicable, the officer should verify an ALPR response through the California Law Enforcement Telecommunications System (CLETS) before taking enforcement action that is based solely on an ALPR alert.

427.4 DATA COLLECTION AND RETENTION

The Support Services Division Commander is responsible for ensuring systems and processes are in place for the proper collection and retention of ALPR data. Data will be transferred from vehicles to the designated storage in accordance with department procedures.

All ALPR data downloaded to the server should be stored for a minimum of one year (Government Code § 34090.6) 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.

427.5 ACCOUNTABILITY

All data will be closely safeguarded and protected by both procedural and technological means. The La Verne Police Department will observe the following safeguards regarding access to and use of stored data (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

(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 (Civil Code § 1798.90.52).

(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.

For security or data breaches, see the Records Release and Maintenance Policy.

427.6 POLICY

The policy of the La Verne 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.

427.7 RELEASING ALPR DATA

The ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law, using the following procedures:

(a) The agency makes a written 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 Support Services Division Commander 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 Maintenance and Release Policy (Civil Code § 1798.90.55).

427.8 TRAINING

The Training Lieutenant should ensure that members receive department-approved training for those authorized to use or access the ALPR system (Civil Code § 1798.90.51; Civil Code § 1798.90.53).

Records Maintenance and Release

804.1 PURPOSE AND SCOPE

This policy provides guidance on the maintenance and release of department records. Protected information is separately covered in the Protected Information Policy.

804.2 POLICY

The La Verne Police Department is committed to providing public access to records in a manner that is consistent with the California Public Records Act (Government Code § 6250 et seq.).

804.3 CUSTODIAN OF RECORDS RESPONSIBILITIES

The Chief of Police shall designate a Custodian of Records . The responsibilities of the Custodian of Records include, but are not limited to:

(a) Managing the records management system for the Department, including the retention, archiving, release and destruction of department public records.

(b) Maintaining and updating the department records retention schedule including:

1. Identifying the minimum length of time the Department must keep records.
2. Identifying the department division responsible for the original record.

(c) Establishing rules regarding the inspection and copying of department public records as reasonably necessary for the protection of such records.

(d) Identifying records or portions of records that are confidential under state or federal law and not open for inspection or copying.

(e) Establishing rules regarding the processing of subpoenas for the production of records.

(f) Ensuring a current schedule of fees for public records as allowed by law is available (Government Code § 6253).

804.4 PROCESSING REQUESTS FOR PUBLIC RECORDS

Any department member who receives a request for records shall route the request to the Custodian of Records or the authorized designee.

804.4.1 REQUESTS FOR RECORDS

Any member of the public, including the media and elected officials, may access unrestricted records of this department, during regular business hours by submitting a written and signed request that reasonably describes each record sought and paying any associated fees (Government Code § 6253).

The processing of requests for records is subject to the following (Government Code § 6253):

(a) The Department is not required to create records that do not exist.

(b) Victims of an incident or their authorized representative shall not be required to show proof of legal presence in the United States to obtain department records or information. If

Adoption Date: 2016/04/05

identification is required, a current driver's license or identification card issued by any state in the United States, a current passport issued by the United States or a foreign government with which the United States has a diplomatic relationship or current Matricula Consular card is acceptable (Government Code § 6254.30).

(c) Either the requested record or the reason for non-disclosure will be provided promptly, but no later than 10 days from the date of request, unless unusual circumstances preclude doing so. If more time is needed, an extension of up to 14 additional days may be authorized by the Custodian of Records or the authorized designee. If an extension is authorized, the Department shall provide the requester written notice that includes the reason for the extension and the anticipated date of the response.

1. When the request does not reasonably describe the records sought, the Custodian of Records shall assist the requester in making the request focused and effective in a way to identify the records or information that would be responsive to the request including providing assistance for overcoming any practical basis for denying access to the records or information. The Custodian of Records shall also assist in describing the information technology and physical location in which the record exists (Government Code § 6253.1).

(d) Upon request, a record shall be provided in an electronic format utilized by the Department. Records shall not be provided only in electronic format unless specifically requested (Government Code § 6253.9).

(e) When a record contains material with release restrictions and material that is not subject to release restrictions, the restricted material shall be redacted and the unrestricted material released.

1. A copy of the redacted release should be maintained in the case file for proof of what was actually released and as a place to document the reasons for the redactions.

(f) If a record request is denied in whole or part, the requester shall be provided a written response that includes the statutory exemption for withholding the record or facts that the public interest served by nondisclosure outweighs the interest served by disclosure (Government Code § 6255). The written response shall also include the names, titles or positions of each person responsible for the denial.

804.5 RELEASE RESTRICTIONS

Examples of release restrictions include:

(a) Personal identifying information, including an individual's photograph; Social Security and driver identification numbers; name, address and telephone number; and medical or disability information that is contained in any driver license record, motor vehicle record or any department record, including traffic collision reports, are restricted except as authorized by the Department, and only when such use or disclosure is permitted or required by law to carry out a legitimate law enforcement purpose (18 USC § 2721; 18 USC § 2722).

(b) Social Security numbers (Government Code § 6254.29).

(c) Personnel records, medical records and similar records which would involve an unwarranted invasion of personal privacy (Government Code § 6254; Penal Code § 832.7; Penal Code § 832.8; Evidence Code § 1043 et seq.).

1. Peace officer personnel records are deemed confidential and shall not be made public or otherwise released to unauthorized individuals or entities absent a valid court order.
2. The identity of any officer subject to any criminal or administrative investigation shall not be released without the consent of the involved officer, prior approval of the Chief of Police or as required by law.

(d) Victim information that may be protected by statutes, including victims of certain crimes who have requested that their identifying information be kept confidential, victims who are minors and victims of certain offenses (e.g., sex crimes, Penal Code § 293). Addresses and telephone numbers of a victim or a witness to any arrested person or to any person who may be a defendant in a criminal action shall not be disclosed, unless it is required by law (Government Code § 6254; Penal Code § 841.5).

1. Victims of domestic violence or their representative shall be provided, without charge, one copy of all domestic violence incident report face sheets, one copy of all domestic violence incident reports, or both, pursuant to the requirements and time frames of Family Code § 6228.

(e) Information involving confidential informants, intelligence information, information that would endanger the safety of any person involved or information that would endanger the successful completion of the investigation or a related investigation. This includes analysis and conclusions of investigating officers (Evidence Code § 1041; Government Code § 6254).

1. Absent a statutory exemption to the contrary or other lawful reason to deem information from reports confidential, information from unrestricted agency reports shall be made public as outlined in Government Code § 6254(f).

(f) Local criminal history information including, but not limited to, arrest history and disposition, and fingerprints shall only be subject to release to those agencies and individuals set forth in Penal Code § 13300.

1. All requests from criminal defendants and their authorized representatives (including attorneys) shall be referred to the District Attorney, City Attorney or the courts pursuant to Penal Code § 1054.5.

(g) Certain types of reports involving, but not limited to, child abuse and molestation (Penal Code § 11167.5), elder and dependent abuse (Welfare and Institutions Code § 15633) and juveniles (Welfare and Institutions Code § 827).

(h) Sealed autopsy and private medical information concerning a murdered child with the exceptions that allow dissemination of those reports to law enforcement agents, prosecutors, defendants or civil litigants under state and federal discovery laws (Code of Civil Procedure §130).

(i) Information contained in CCW permit applications or other files which would tend to reveal where the applicant is vulnerable or which contains medical or psychological information (Government Code § 6254).

(j) Traffic collision reports (and related supplemental reports) shall be considered confidential and subject to release only to the California Highway Patrol, Department of Motor

Vehicles (DMV), other law enforcement agencies and those individuals and their authorized representatives set forth in Vehicle Code § 20012.

(k) Any record created exclusively in anticipation of potential litigation involving this department (Government Code § 6254).

(l) Any memorandum from legal counsel until the pending litigation has been adjudicated or otherwise settled (Government Code § 6254.25).

(m) Records relating to the security of the department's electronic technology systems (Government Code § 6254.19).

(n) Any other record not addressed in this policy shall not be subject to release where such record is exempt or prohibited from disclosure pursuant to state or federal law, including, but not limited to, provisions of the Evidence Code relating to privilege (Government Code § 6254).

(o) Information connected with juvenile court proceedings or the detention or custody of a juvenile. Federal officials may be required to obtain a court order to obtain certain juvenile information (Welfare and Institutions Code § 827.9; Welfare and Institutions Code § 831).

804.6 SUBPOENAS AND DISCOVERY REQUESTS

Any member who receives a subpoena duces tecum or discovery request for records should promptly contact a supervisor and the Custodian of Records for review and processing. While a subpoena duces tecum may ultimately be subject to compliance, it is not an order from the court that will automatically require the release of the requested information.

Generally, discovery requests and subpoenas from criminal defendants and their authorized representatives (including attorneys) should be referred to the District Attorney, City Attorney or the courts.

All questions regarding compliance with any subpoena duces tecum or discovery request should be promptly referred to legal counsel for the Department so that a timely response can be prepared.

804.7 SECURITY BREACHES

The Information Systems Specialist shall ensure notice is given anytime there is a reasonable belief an unauthorized person has acquired unencrypted personal identifying information stored in any Department information system (Civil Code § 1798.29).

Notice shall be given as soon as reasonably practicable to all individuals whose information may have been acquired. The notification may be delayed if the Department determines that notification will impede a criminal investigation or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

For the purposes of this requirement, personal identifying information includes an individual's first name or first initial and last name in combination with any one or more of the following:

- Social security number

- Driver license number or California identification card number
- Account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account
- Medical information
- Health insurance information
- A user name or email address, in combination with a password or security question and answer that permits access to an online account
- Information or data collected by Automated License Plate Reader (ALPR) technology

804.7.1 FORM OF NOTICE

(a) The notice shall be written in plain language and include, to the extent possible, the following:

(a) The date of the notice.

(b) Name and contact information for the La Verne Police Department.

(c) A list of the types of personal information that were or are reasonably believed to have been acquired.

(d) The estimated date or date range within which the security breach occurred.

(e) Whether the notification was delayed as a result of a law enforcement investigation.

(f) A general desciption of the security breach.

(g) The tollfree telephone numbers and addresses of the major credit reporting agencies, if the breach exposed a social security number, or a driver's license or California identification card number.

(b) The notice may also include information about what the La Verne Police Departmnt has done to protect individuals whose information has been breached and may include information on steps that the person whose information has been breached may take to protect him/herself.

(c) When a breach involves an online account, and only a user name or email address in combination with either a password or security question and answer that would permit access to an online account, and no other personal information has been breached:

(a) Notification may be provided electronically or in another form directing the person to promptly change either his/her password or security question and answer, as applicable, or to take other appropriate steps to protect the online account with the Department in addition to any other online accounts for which the person uses the same user name or email address and password or security question and answer.

804.7.2 MANNER OF NOTICE

(a) Notice may be provided by one of the following methods:

1. Written notice.

2. Electronic notice if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 USC § 7001.

3. Substitute notice if the cost of providing notice would exceed $250,000, the number of the individuals exceeds 500,000 or the Department does not have sufficient contact information. Substitue notice shall consist of all of the following:

(a) Email notice, when the Department has an email address for the subject person.

(b) Conspicuous posting of the notice on the Department's webpage.

4. Notification to major statewide media and the California information Security Office within the California Department of Technology.

(b) If a single breach requires the Department to notify more than 500 California residents, the Department shall electronically submit a sample copy of the notification, excluding any personally identifiable information, to the Attorney General.

804.8 RELEASED RECORDS TO BE MARKED

Each page of any record released pursuant to this policy should be stamped in a colored ink or otherwise marked to indicate the department name and to whom the record was released.

804.9 EXPUNGEMENT

Expungement orders received by the Department shall be reviewed for appropriate action by the Custodian of Records. The Custodian of Records shall expunge such records as ordered by the court. Records may include, but are not limited to, a record of arrest, investigation, detention or conviction. Once the record is expunged, members shall respond to any inquiry as though the record did not exist.

804.10 SECURITY BREACHES

The Records Supervisor shall ensure notice is given anytime there is a reasonable belief an unauthorized person has acquired unencrypted personal identifying information stored in any Department information system (Civil Code § 1798.29).

Notice shall be given as soon as reasonably practicable to all individuals whose information may have been acquired. The notification may be delayed if the Department determines that notification will impede a criminal investigation or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

For the purposes of this requirement, personal identifying information includes an individual’s first name or first initial and last name in combination with any one or more of the following:

- Social Security number
- Driver license number or California identification card number
- Account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual’s financial account

- Medical information
- Health insurance information
- A username or email address, in combination with a password or security question and answer that permits access to an online account
- Information or data collected by Automated License Plate Reader (ALPR) technology

804.10.1 FORM OF NOTICE

(a) The notice shall be written in plain language, be consistent with the format provided in Civil Code § 1798.29 and include, to the extent possible, the following:

1. The date of the notice.
2. Name and contact information for the La Verne Police Department.
3. A list of the types of personal information that were or are reasonably believed to have been acquired.
4. The estimated date or date range within which the security breach occurred.
5. Whether the notification was delayed as a result of a law enforcement investigation.
6. A general description of the security breach.
7. The toll-free telephone numbers and addresses of the major credit reporting agencies, if the breach exposed a Social Security number or a driver license or California identification card number.

(b) The notice may also include information about what the La Verne Police Department has done to protect individuals whose information has been breached and may include information on steps that the person whose information has been breached may take to protect him/herself (Civil Code § 1798.29).

(c) When a breach involves an online account, and only a username or email address in combination with either a password or security question and answer that would permit access to an online account, and no other personal information has been breached (Civil Code § 1798.29):

1. Notification may be provided electronically or in another form directing the person to promptly change either his/her password or security question and answer, as applicable, or to take other appropriate steps to protect the online account with the Department in addition to any other online accounts for which the person uses the same username or email address and password or security question and answer.
2. When the breach involves an email address that was furnished by the La Verne Police Department, notification of the breach should not be sent to that email address but should instead be made by another appropriate medium as prescribed by Civil Code § 1798.29.

804.10.2 MANNER OF NOTICE

(a) Notice may be provided by one of the following methods (Civil Code § 1798.29):

1. Written notice.
2. Electronic notice if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 USC § 7001.
3. Substitute notice if the cost of providing notice would exceed $250,000, the number of individuals exceeds 500,000 or the Department does not have sufficient contact information. Substitute notice shall consist of all of the following:
    (a) Email notice when the Department has an email address for the subject person.
    (b) Conspicuous posting of the notice on the department's webpage for a minimum of 30 days.
4. Notification to major statewide media and the California Information Security Office within the California Department of Technology.

(b) If a single breach requires the Department to notify more than 500 California residents, the Department shall electronically submit a sample copy of the notification, excluding any personally identifiable information, to the Attorney General.