

EXHIBIT B: SPEED SAFETY SYSTEM USE POLICY

SPEED SAFETY SYSTEM USE POLICY

CITY OF GLENDALE

Per California Assembly Bill 645, the City of Glendale has been chosen to implement a Speed Safety Pilot Program until January 1, 2032.

The purpose of this program is to advance the City of Glendale's transportation safety and equity. This technology has the potential to reduce speed-related collisions and injuries and the trajectory of speed safety hazards to reduce speed-related collisions and injuries. Photo enforcement through a speed safety system is a key component which aligns with Glendale's Safe & Healthy Streets Plan to improve street safety.

The City of Glendale is committed to becoming a safer environment for residents in all transportation modes and across all abilities.

OVERVIEW

TECHNOLOGY AND TRAFFIC SAFETY

Existing law establishes a basic speed law that prohibits a person from driving a vehicle upon a highway at a speed greater than is reasonable given the weather, visibility, traffic, and highway conditions. However, regardless of preexisting law, speed-related incidents have been a recurring issue. Vehicular speed is a concern.

Reducing potential speed-related collisions can improve overall safety for pedestrians, cyclists, and operators of motor vehicles and their passengers.

i. System Description

- a) A "speed safety system" or "system" is a fixed or mobile radar or laser system or any other electronic device that utilizes automated equipment to detect a violation of speed laws and obtains a clear photograph of a speeding vehicle's rear license plate. The system only captures data of a speeding vehicle's rear license plate and does not capture data of non-speeding vehicles.
- b) Speed safety systems in each location will detect violations for both directions of travel.

ii. System Benefits

- a) Speed safety systems are a proven effective tool for reducing speeding, crashes, and traffic related injuries and fatalities.
- b) Implementation of speed safety systems can assist cities in addressing excessive speeding and speed-related collisions.
- c) Speed safety systems can improve and advance equity in traffic enforcement.
- d) System implementation can make speeding traffic enforcement more predictable and effective, which can help modify driver behavior.

DATA COLLECTION

The City of Glendale shall use any information that is retrieved from the Speed Safety System for these authorized purposes:

1. *To enforce speed limits on City streets in accordance with California Vehicle Code sections 22425 – 22434, otherwise known as the Speed Safety System Pilot Program.*
2. *To analyze and report on speed enforcement in the Speed Safety System Pilot Program for the City of Glendale.*

The City of Glendale may use information collected from technology only for legally authorized purposes and may not use that information to unlawfully discriminate against people based on race, ethnicity, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, sexual orientation or activity, or genetic and/or biometric data.

DATA STORAGE

Data will be stored and encrypted in cloud or local storage and in software as a service product. The vendor of the system as well as the City of Glendale shall be responsible for the storing and protection of data. Data shall be stored at the discretion of the vendor. Improper data storage that results in improper access of PII data, or data that is personally identifiable, is subject to criminal and/or civil prosecution.

DATA SHARING

In order to maintain the security and privacy of surveillance technology data, the department will not share this information with other departments or entities within the City of Glendale. Under California Vehicle Code section 22425(l)(5), the City of Glendale cannot disclose or share data from speed safety security systems with anyone, including state or federal government agencies or officials for any purpose, except as required by state or federal law, court order, or in response to a subpoena in an individual case or proceeding. Improper data sharing that results in improper access of PII data, or data that is personally identifiable is subject to criminal and/or civil prosecution.

PHOTOGRAPHIC EVIDENCE AND DATA RETENTION

The use of any facial recognition technology in a speed safety system is prohibited by California state law. Any information that is collected from the surveillance system that does not result in warning or violation notice shall be destroyed and removed from the administrative system within five business days after the photograph was first taken. The City of Glendale may retain information that a vehicle has been cited by the Speed Safety System and fined for a violation for up to three years.

Confidential records and evidence may be retained for up to 60 days after final disposition of the notice of violation.

Administrative records regarding speed safety system violations may be retained for up to 120 days after final disposition of the notice of violation. Notwithstanding any other law, the

SPEED SAFETY SYSTEM USE POLICY CITY OF GLENDALE

confidential records and evidence shall be destroyed in a manner that maintains the confidentiality of any person included in the record or evidence.

DATA DISPOSAL

The City of Glendale will automatically dispose of raw speed safety camera system data (e.g., speed safety camera system data that has not been anonymized or aggregated) after the applicable data retention period. In accordance with the California Vehicle Code Section 4, 22425(l)(3), photographic evidence and other confidential information from the DMV will be destroyed in a manner that ensures the confidentiality of any individuals included in the record or evidence.

TYPE(S) OF DATA COLLECTED AND VIOLATION NOTIFICATION

Speed safety systems shall capture images of rear license plates of vehicles driving at least 11 miles per hour above the posted speed limit, as well as include a real-time notification to the driver of when violations are detected.

Data collected by the speed safety system will be encrypted and secure in transit from the camera system to the vendor's cloud storage.

Violation recipients are to receive a real-time notification via photographic camera flash at each of the speed safety camera locations. This notification system implementation ensures drivers are promptly alerted to any violations they may have committed.

The use of a camera flash provides a visual cue that is easily perceptible to violation recipients.

To the extent possible, the speed safety system shall be angled only to capture speeding violation photographs and not to capture other identifying images of vehicles, drivers, or pedestrians.

DATA ACCESS

Data or information collected from the speed safety system shall not be disclosed to any other persons and is considered confidential. The only exception is that data may be released to the registered owner or to a person identified by the registered owner as the driver at the time of an alleged violation, who may receive a copy of photographic evidence that was collected. The manufacturer or supplier of the contracted speed safety system is prohibited from sharing, repurposing, or monetizing data. Third-party data sharing is prohibited.

Data regarding the number of violations issued or speeds at which they were issued for is not photographic or administrative data and therefore not considered confidential.

Representatives from the City of Glendale who have access to the data from the speed safety system shall comply with the California Public Records Act, the requirements of the Federal and State Constitutions, Federal and State civil procedure laws and rules, and the following applicable provisions from the City of Glendale's Administrative Policy Manual, Chapter 6, Policy 6-14:

ACCEPTABLE USE POLICY: DATA, EMAIL, INTERNET, AND COMPUTERS

C. POLICY

SPEED SAFETY SYSTEM USE POLICY

CITY OF GLENDALE

1. *Institute Appropriate Controls* – City will institute mandatory appropriate controls for all Users subject to this policy to protect the City Information Assets from all threats, internal or external, deliberate or accidental, as well as ensure compliance with all applicable laws, regulations and legal obligations.
2. *Security Policy Awareness and Compliance* – All current Users who log-on to City computer systems shall read and sign a copy of this policy, known as “Acceptable Use Policy.” Prior to first accessing a City’s Information Assets new Users shall read this policy and, by signing it, acknowledge that they read and understood the policy.
3. *Affirmation and Acceptance* – Each User who accesses City Confidential Data and Information Assets shall be required to receive and affirm their understanding and acceptance of this Acceptable Use Policy.
4. *Obligation of Users* – All Users subject to this Acceptable Use Policy shall:
 - a. Comply with all applicable laws;
 - b. Protect the City’s Data and Information Assets; and
 - c. Avoid creating risk to the City by misuse of Data or Information Assets
5. *Consequences of Violation*- Violation of this policy and the Standards listed below may result in disciplinary action up to and including termination for employees, termination of business relations in the case of contractors or consultants, and dismissal for interns and volunteers. Additionally, individuals who fail to comply with this policy will be subject to loss of City Data resources access and civil and/or criminal prosecution.
6. This policy applies to all Users as defined in the Definition Section including Police and Fire Department personnel. Before any Police or Fire Department personnel initiate, access or conduct any e-related activity prohibited by this policy, he/she shall establish and substantiate a legitimate need, directly related to a public safety enforcement matter or criminal investigation, and be authorized by the Police Chief, Fire Chief, Police Captain or Fire Battalion Chief.

D. ACCEPTABLE USE POLICY RATIONALE

1. *Comply with Security Laws* – Security is everyone’s responsibility. Users shall comply with all relevant laws, regulations, and contractual requirements related to information security, thus avoiding penalties and adverse actions against them or the City.
2. *Important to Protect Assets* – Protecting City Information Assets (and any citizen or customer Data within its custody) by safeguarding their Confidentiality, Integrity and Availability is of paramount importance. By using a risk-based approach, the City will manage the risk of security compromise or improper exposure of City’s Information assets.
3. *Policy to Minimize Risk* – An Acceptable Use Policy minimizes risk by protecting City Information Assets, as well as Users. Among the most valuable of City resources is its data. This set of policies is aimed at protecting the City’s Information Assets as well as the City itself from legal liability.

SPEED SAFETY SYSTEM USE POLICY CITY OF GLENDALE

F. COMPUTER ACCEPTABLE USE

1. *User Accounts* – User accounts and passwords given to individual authorized users are Confidential, and may not be shared. The City shall have the right to assign control and limit access to its computers through exclusive passwords. If it ever necessary for ITD staff to have User account access, ITD staff shall use that password only in the presence in the account holder and shall have the authorized user reset the password in the ITD staff member's presence. The ITD staff member shall not know this second password.
2. *Passwords* – Passwords shall not be transmitted by email. Initial account setup or password change shall have a finite expiration time, not greater than 24 hours, and shall not be the same as other passwords, or constitute a predictable pattern.
3. *Use of Disk Encryption* – Full disk encryption shall be used on all City-owned laptops regardless of data sensitivity. Full disk encryption shall be used on all desktops containing City restricted and/or confidential data.
5. *Use of Wireless Information Assets* – City-owned Wireless Information Assets, such as smart phones and tablet devices shall employ a City-provided and controlled mobile device management and security architecture (MDMS), as designated by the Director of Information Technology. The MDMS shall encrypt, control, and require a password for the device. Unless directly authorized by the Director of Information Technology. The MDMS shall encrypt, control, and require a password for the device. Unless directly authorized by the Director of Information Technology or designee, no User shall disable, remove, circumvent, or otherwise tamper with the MDMS used on any Information Asset.
6. *Bring Your Own Device (BYOD)* – If a staff member's Personal Computing Device is brought to the workplace to conduct City business, such use shall be authorized and approved by the Department Head or designee. The Personal Computing Device may not be attached to the City network, and may only use a guest or commercial wireless (cellular) network ("WWAN"). Personal smart phones and tablet devices (personal device) shall employ a City-provided and controlled Mobile Device Management System (MDMS), as designated by the Director of Information Technology. The MDMS encrypts and controls a "container" or "partition" on the personal device. **Placement of City Confidential Data is prohibited on any Personally Owned Computing Device except within the City-controlled "partition".** A Personally Owned computer is subject to the same criteria regarding privacy as City-owned equipment (including anti-malware, current patch level, firewall, and remove wipe capabilities), and it shall not be used for the transmittal or storage of City data.
7. *Copyright Law* – Users subject to this policy shall abide by all copyright laws related to computer system usage.

G. INFORMATION ACCEPTABLE USE

1. *IT Security Prohibitions* – Except for authorized personnel for job-related purposes, all users are expressly forbidden from accessing the computer *security* system. Users shall not download, install or run security programs or utilities such as password cracking programs, packet sniffers, or port scanners that reveal or exploit weaknesses in the

SPEED SAFETY SYSTEM USE POLICY

CITY OF GLENDALE

security of a City Information Asset unless approved in writing by the Director of Information Technology.

2. *Tampering Prohibited* – Staff is expressly prohibited from tampering with or attempting to tamper with, the City Information Assets security system with the intent or result of the obstruction, destruction or modification of City data.
3. *Report Security Weaknesses* – All suspected intrusions via the Internet or by unauthorized staff are to be reported to the Information Technology Department's Information Security Information Manager and appropriate Department management personnel immediately. Users shall report any suspected weaknesses in City Information Asset security to the Information Technology Department's Information Security Manager. Weaknesses in Information Asset security include unexpected software or system behavior, which may result in unintentional disclosure of data or exposure to security threats.
4. *Report Security Violations* – Users shall report any incidents of possible misuse or violation of this Acceptable Use Policy through the use of a documented report sent to ITD, or reporting to the ITD department by a traceable means. This includes reporting incidents to the Service Desk (Help Desk) at (818) 548-4085 or by sending an e-mail to Service Desk by typing "HELP" in the e-mail address box. Reporting incidents to a supervisor who then informs ITD is also acceptable.
5. *Unauthorized Access Prohibited* – Users shall not attempt to access any data, documents, email correspondence, or programs contained on City Information Assets for which they do not have the authorization.
6. *System Access Information Security* – Systems administrators and authorized users shall not divulge passwords, accounts, remote connection modem phone numbers or other access points of City computer resources to anyone without proper authorization.
7. *End User Access Information Security* – Users shall not share their account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or similar data or devices used for identification and authorization purposes.
8. *Software Copying Prohibited* – Users shall not make unauthorized copies of City-owned software.
9. *Users Software Installation Prohibited* – Users shall not use or install any non-City approved software. The use of non-standard shareware or freeware software without the appropriate ITD approval is strictly prohibited. All software purchases and installation shall be preapproved by ITD in writing. Furthermore, all installation shall only be performed by authorized ITD staff.
10. *Degradation or Circumvention of Authorizations Prohibited* – Users shall not engage in activity that may degrade the performance of City Data Assets; deprive an authorized user access to City Information Assets; obtain extra Information Assets beyond those allocated; or circumvent City Information Asset measures.

SPEED SAFETY SYSTEM USE POLICY
CITY OF GLENDALE

11. *Use of City Information Assets Remotely* – Access to the Internet from City-owned Information Assets from off campus locations such as home, or publicly available networks are subject to this policy. While connected to the City network users shall use their City-owned Information Assets as if physically on campus. Specifically, users shall comply with the email policy as described herein, as well as refrain from visiting web sites prohibited by the city regardless of the user's physical location. This policy is in effect at all times including non-work hours and during personal vacation. Users shall not allow family members or other users subject to this policy to access City Information Assets.
12. *Disclosure of City Information* – Users shall take all necessary steps to avoid unintended disclosure of City Information. While the city is subject to the California Public Records Act, the City has an established process for handling such requests and asserting lawful exemptions when appropriate. Users shall exercise due care when accessing City Information remotely when performing their duties to protect such Information from disclosure. Willful misuse of City Information is in violation of this policy.
13. *Report Security Issues* - Any security issues discovered by Users subject to this policy shall be reported to the Director of Information Technology, or designee, for follow-up investigation.
14. *Use of Anti-Malware Software* - Users shall use ITD-approved anti-malware- scanning software on all files downloaded from the Internet or City network. This software shall be configured to update automatically at least once per day. The anti- malware software shall not have a user configuration enabled that allows Users to turn off the software, except with the written permission of the Director of ITD.
15. *Conform to Authorized Access Processes* - Each Internet or e-mail user shall follow the authorized access process, logon procedures and password protection requirements at all times. Users subject to this policy shall not use any account or password unless specifically authorized.
16. *Email Access Policy* - Users may not access another's e-mail messages, unless this access shall be by proxy, (i.e. as a delegate granted access privileges by the e-mail account "owner" and not by sharing passwords). E-mail messages may be forwarded to City staff unless specifically identified by the email's author as confidential. Emails containing attorney/client privileged data shall not be forwarded to non-city personnel.
17. *Conform to Authorized Access for Confidential & Medical Records* - Users subject to this Policy are expressly prohibited from accessing or attempting to access any secured confidential personal or medical information on the City's Information Assets or from disclosing any confidential personal or medical information. Access or disclosure of such information may only occur by directive of the City Manager, or designee, or as necessary for the Confidential conduct of personnel management or litigation purposes, in any case, such information may not be released until specifically permitted by the City Attorney and as required by law.
18. *City Information Assets are Property of City* - Electronic files created, sent, received, or stored on Information Assets owned, leased, administered, or otherwise under the custody and control of the City are the property of the City and employee use of these

SPEED SAFETY SYSTEM USE POLICY

CITY OF GLENDALE

files is neither personal nor private. Authorized ITD Security staff may access all such files at any time without knowledge of the Information Assets User or owner for purposes of maintaining the security of City Information Assets.

19. *Restrictions on Local or Removable Storage* - All data stored, created, or accessed, shall be accessed directly from the City network or from the network through a security architecture provided and controlled by the City, local and removable storage shall only be used if the data sensitivity is low, or the local or removable drives are encrypted with an ITD approved encryption method. Local and removable storage are always intended to be temporary. Data file backup copies shall always be stored on the City network.

TRAINING

To reduce the possibility that surveillance technology or its associated data will be misused or used contrary to its authorized use, all individuals requiring access must receive training on data security policies and procedures before being granted access to systems containing confidential data.

The City of Glendale shall require all elected officials, employees, consultants, volunteers, and vendors working with the technology on its behalf to read and formally acknowledge all authorized and prohibited uses dictated by this policy.

The City of Glendale shall also require that all individuals requesting data or regularly requiring data access receive appropriate training before being granted access to systems containing PII data, or data and information that can identify individuals from others.

The City of Glendale shall ensure employees and vendors are trained on how to use the speed safety systems correctly and ensure data is used for its intended use only. Training includes explaining how employees and vendors can use data and how to report problems with the speed safety camera system.

The responsible party of the City of Glendale will develop a specified process for confidentiality training and processes.

All parties requesting access must adhere to the following rules and processes:

- Only authorized users may use speed safety camera technology or access data.
- Authorized users must log into tablet or computer, as applicable, to access speed safety camera system data.
- Data that is accessed shall be secured with multi-factor authentication and secure passwords as a minimum safeguard.

EMPLOYEE ACCESS

Once collected, the following roles and job titles are authorized to access and use data collected, retained, processed or shared by the surveillance technology:

- Representatives from the City of Glendale

PUBLIC ACCESS

SPEED SAFETY SYSTEM USE POLICY

CITY OF GLENDALE

The City of Glendale will comply with the California Public Records Act, the requirements of the federal and State Constitutions, and federal and State civil procedure laws and rules. Collected data that is classified as Level 1-Public data may be made available for public access under the City of Glendale's discretion. No record shall be withheld from disclosure in its entirety unless all information contained in it is exempt from disclosure under express provisions of the California Public Records Act or some other statute.

DATA SECURITY

The City of Glendale shall secure photographic or administrative data against unauthorized or unlawful processing or disclosure; unwarranted access, manipulation, or misuse; and accidental loss, destruction, or damage. Surveillance technology data collected and retained by the City of Glendale shall be protected by the safeguards appropriate for its classification level(s) as defined by the National Institute of Standards and Technology (NIST) security framework 800-53, or equivalent requirements from other major cybersecurity frameworks selected by the City.

The City of Glendale will secure any PII against unauthorized access, processing, disclosure, and accidental loss, destruction, or damage. Speed safety camera system data collected and retained by the City of Glendale will be protected by the safeguards appropriate for its classification level(s). To protect speed safety camera data from unauthorized access, including misuse, the City of Glendale shall, at minimum, apply the following safeguards:

- Authorized users will log in credentials with multi-factor authentication, and use complex passwords to access the speed safety camera system technology.
- All access to and activity in the speed safety camera system data will be logged and be audited.

OVERSIGHT PERSONNEL

The Department of Public Works shall assign representatives from the Department of Public Works to oversee Policy compliance by the City of Glendale and third parties.

POLICY VIOLATIONS

Failure to comply with this Policy may result in appropriate disciplinary measures based on the severity of the violation. These measures may include written warnings, suspensions, or termination of employment.

CIVIL PENALTIES

Speed limits promote road safety by establishing an upper limit on speed appropriate for the street's design, vehicle volume and pedestrian density. Civil penalties or fines can reduce speeding and speed-related incidents.

FINES

The following fines will be issued for these scenarios:

- a. Fifty dollars (\$50) for driving at a speed of 11 to 15 miles per hour over the posted speed limit.
- b. One hundred dollars (\$100) for driving at a speed of 16 to 25 miles per hour over the posted speed limit.
- c. Two hundred dollars (\$200) for driving at a speed of 26 miles per hour or more over the posted speed limit.
- d. Five hundred dollars (\$500) for driving at a speed of 100 miles or more per hour.

VIOLATIONS

A vehicle's first violation within designated jurisdiction for traveling speeds 11 to 15 miles per hour above the posted speed limit shall receive a warning notice. Violations made within the first 60 days of program implementation shall be issued warning notices rather than notice of violation. Warnings and violation notices shall be issued to registered owner of the vehicle.

Diversion programs shall be offered through the City of Glendale. A diversion program shall be offered for indigent speed safety system violation recipients with performance of community service in lieu of paying civil penalties otherwise indigent speed safety system violation recipients shall have the ability to pay civil penalties over a period of time with monthly installments of no more than twenty-five dollars (\$25) per month. Applicable fines and penalties have the ability to be reduced by 80 percent for indigent persons, and by 50 percent for individuals up to 250 percent above the federal poverty level. Indigent speed safety system violation recipients may also perform community service in lieu of paying the penalty for a speed system violation.

California Code, Business and Professions Code Section 6213 deems an "Indigent person" as a person whose income is (1) 125 percent or less of the current poverty threshold established by the United States Office of Management and Budget, or (2) who is eligible for Supplemental Security Income or free services under the Older Americans Act or Developmentally Disabled Assistance Act.

The person may demonstrate that they are indigent or are up to 250 percent above the poverty level by providing either of the following information, as applicable:

1. Proof of income from a pay stub or another form of proof of earnings, such as a bank statement, that shows that the person meets the income criteria set forth in subdivision (b) of Section 68632 of the California Government Code, subject to review and approval by the City of Glendale by emailing SpeedSafety@glendaleca.gov. The processing agency or its designee shall not unreasonably withhold its approval.

SPEED SAFETY SYSTEM USE POLICY CITY OF GLENDALE

2. Proof of receipt of benefits under the programs described in subdivision (a) of Section 68632 of the California Government Code, including, but not limited to, an electronic benefits transfer card or another card, subject to review and approval by the processing agency.

PAYMENTS

The Glendale Police Department does not accept any form of payment.

Speed Safety System Citations to be paid to The Parking Enforcement Service Center.

If violation recipients have questions regarding speed safety system citations, they may contact The City of Glendale parking citation service center at (866) 470-3088. Violation recipients are to citation information ready when calling.

Pay Online

Pay online at <https://www.dsparkingportal.com/glendale>. Those paying online will be required to enter some citation information. Most major credit cards and debit cards displaying the Visa or Mastercard logo are accepted. There is a \$3.95 fee for this service.

Pay by Phone

Call (866) 470-3088 to pay by phone. Violation recipients are to citation information ready when calling. Most major credit cards and debit cards displaying the Visa or Mastercard logo are accepted. There is a \$3.95 fee for this service.

Pay by Mail

Violation recipients shall not send cash. Check or money order are applicable and payable to the City of Glendale. Violation recipients are to denote citation number on the written check or money order. If recipients were not provided an envelope, they shall submit payment to the following address:

The City of Glendale
Parking Enforcement Service Center
P.O. Box 6010
Inglewood, CA 90312-6010

CONTESTING A SPEED SAFETY SYSTEM CITATION

The City of Glendale adheres to the guidelines prescribed by the California Vehicle Code with regard to the contesting of speed safety system citations. Contesting a speed safety system citation is a three-step process. In order to participate in this process violation recipients must adhere to the following guidelines:

1. Administrative Review

Violation recipients must submit requests within twenty-one (21) calendar days of the date the citation was issued, or fourteen (14) calendar days from the mailing of a Notice of Violation. Recipients of a speed safety system citation may contest their citation online at:

<https://www.dsparkingportal.com/glendale>

***SPEED SAFETY SYSTEM USE POLICY
CITY OF GLENDALE***

2. Administrative Hearing

If the received citation was upheld in Step 1, violation recipients may proceed with an administrative hearing. Violation recipients shall be sure to carefully follow the instructions on the Administrative Review Decision - Liable form that was mailed to the recipient. State Law requires that violation recipients submit payment owed on the citation when proceeding with this step except as provided in Section 40215 (b) of the California Vehicle Code.

Request and payments must be received no later than twenty-one (21) calendar days of the mailing of the results of the Administrative Review in Step 1. Failing to meet these requirements will result in the citation being upheld and will have waived the ability to further contest the citation.

3. Court Appeal

If the citation is upheld in Step 2, violation recipients may file an appeal of the finding with the Los Angeles Superior Court, 111 N. Hill Street, Los Angeles, CA 90012. Notice of Appeal form from the court must be obtained. There is a court-imposed filing fee of \$25 for this process. The appeal must be filed within thirty (30) calendar days of the mailing of the Administrative Hearing officer's findings. A copy of the appeal must also be filed with the City of Glendale, Office of the City Attorney, located at 613 E. Broadway, Glendale, CA 91206-4394. Failure to timely file this appeal will result in waiver to have the matter heard by the court.

If the presiding Judge dismisses a citation, the \$25 filing fee along with the parking fine will be refunded to individual the citation was given to.

IMPLEMENTATION

Implementation of surveillance technology for the Speed Safety System has been carefully assessed, reviewed and analyzed. Specific locations with enforcement cameras can expect an increase in street safety and equity. Areas chosen experience a high vehicle collision rate, or are in geographic areas that have or transport populations that are more vulnerable or susceptible to injury by vehicular collision or speeding.

The initial factors established by AB 645 for eligibility implementation include:

- **Cameras will be positioned on streets with a high rate of accidents, in school zones, on streets notorious for speed racing incidents, or meet the standards of a safety corridor under Section 22358.7 of the California Vehicle Code.**
- **Cameras cannot be located on state highways or freeways.**
- **Speed safety systems shall be in locations that are geographically and socioeconomically diverse.**

REASONING OF CAMERA SYSTEM PLACEMENT

The City of Glendale can implement up to nine speed safety cameras. This number of cameras is proportionate to, in accordance with California AB-645. AB-645 states that a jurisdiction with a population of less than 300,000 shall receive no more than nine systems, and Glendale has a population of just under 200,000 (according to the U.S. 2020 Census).

LOCATION SELECTION

The locations of the speed safety camera systems and hours of enforcement will be posted on the City of Glendale's speed safety program website, which shall be updated if the City of Glendale changes enforcement locations and/or hours of enforcement.

GlendaleSpeedSafety.com

SYSTEM REVENUE

Revenues derived from any program utilizing a speed safety system for speed limit enforcement shall first be used to recover program costs. Program costs include, but are not limited to, the construction of traffic-calming measures, the installation of speed safety systems, the adjudication of violations, and reporting speed system impacts.

PROGRAM DURATION

Systems can expect to be implemented for a duration of five years from initial implementation.

SCHOOL ZONES

Existing law states that California school zones are to have a speed limit of 25 miles per hour, and implementation of speed photo enforcement cameras can lead to a safer school zone.

Speed safety systems that are placed in school zones shall only enforce the school zone speed limit during the following times:

SPEED SAFETY SYSTEM USE POLICY CITY OF GLENDALE

- Up to one hour before regular school hours
- 10 minutes after school sessions begin
- One hour during lunch period
- Up to one hour after school sessions conclude

Flashing beacons shall be installed on a school zone sign and be active during the times that the school zone speed limit is enforced with the speed safety system.

SYSTEM REQUIREMENTS

Designated camera locations must clearly identify the presence of the speed safety system by signs stating, "Photo Enforced," along with the posted speed limit no more than 500 feet before the placement of the system. The signs shall be visible to traffic traveling on the street from the direction of travel for which the system is utilized and shall be posted at all locations as may be determined necessary by the Department of Transportation after consultation with the California Traffic Control Devices Committee.

The hours of enforcement for each speed safety camera system and the streets that have been approved for enforcement must be posted on the City of Glendale's speed safety program website, which shall be updated if the City of Glendale changes locations of enforcement.

GlendaleSpeedSafety.com

The City of Glendale shall ensure the speed safety system is regularly inspected, but no less than once every 60 days, and certifies that the system is installed and operating properly. Each camera unit shall be calibrated in accordance with the manufacturer's instructions, and at least once per year by an independent calibration laboratory. Documentation of the regular inspection, operation, and calibration of the system shall be retained at least 180 days after the date on which the system has been permanently removed from use.

A speed safety system at a specific location shall be operated for no more than 18 months after installation of a system, unless one of the following thresholds has been met:

1. A reduction in the 85th percentile speed of vehicles compared to data collected before the system was in operation.
2. A 20-percent reduction in vehicles that exceed the posted speed limit by 10 miles per hour or more compared to data collected before the system was in operation.
3. A 20-percent reduction in the number of violators who received two or more violations at the location since the system became operational.

The City of Glendale need not apply the above thresholds if traffic calming measures per AB-645 Section 4, 22425 (p) have been implemented. If the percentage of violations has not decreased by the metrics identified in California AB-645 within one year after traffic-calming measures have completed construction, the City of Glendale shall either construct additional traffic-calming measures or cease operation of the system on that street.

QUESTIONS AND CONCERNS

Public complaints or concerns may be submitted to the City of Glendale by calling the Department of Public Works at (818) 548-3900 or by emailing SpeedSafety@glendaleca.gov.

The City of Glendale shall acknowledge and respond to complaints and concerns in a timely and organized manner.