



Surveillance Use Policy

CDS – Community Data Sharing
San Diego Police Department

PURPOSE

Many community entities, both private and public, such as Homeowners Associations, shopping centers, schools, public platforms (e.g., Citizen), and the San Diego Metropolitan Transit System (MTS) have existing systems in place to improve the safety of their community. The most common example of such a system is the usage of video cameras for security purposes, but could vary depending on the needs of the specific community entity. Community Data Sharing (CDS) would allow those private and public entities the option to provide those videos and data to the San Diego Police Department (SDPD).

USE

Any data provided through CDS shall be used by SDPD for legitimate law enforcement purposes only. Legitimate law enforcement purposes include, but are not limited to:

- Provide real-time updates to officers responding to calls for service.
- Provide evidence related to crimes being investigated by SDPD.
- Aid in locating suspects or witnesses involved in criminal activity at the location.
- Enhancing coordinated responses to critical incidents and public threats (e.g., active shooters, terrorism events).

The following uses of data shared with SDPD shall be expressly prohibited:

- To violate any Constitutional rights, federal, state, or local laws.
- To conduct random surveillance activities.
- To harass, intimidate, or discriminate against any individual or group.
- To conduct personal business of any type.
- To be used in a discriminatory manner and to target protected individual characteristics, including race, color, ethnicity, religion, national origin, age, disability, gender (to include gender identity and gender expression), lifestyle, sexual orientation, or similar personal characteristics.
- For personal uses of any kind.

All Department members shall comply with all Department Policies and Procedures and are subject to investigation and potential discipline for violations thereof.

Department procedures associated with the use of CDS systems include:

- 1.49 – Body Worn Camera/Evidence.com
- 3.02 – Impound, Release, and Disposal of Property, Evidence
- 6.06 – Crime Scene Protection and Preliminary Investigation Reporting

DATA COLLECTION

When a community entity provides data to SDPD, the entity will be provided with information on how they can connect their technology system to a separate data sharing platform that grants SDPD access (CDS platform). The type and amount of data shared with SDPD through the CDS platform will be at the



Surveillance Use Policy

CDS – Community Data Sharing San Diego Police Department

sole discretion of the provider of that data, and the provider will have the ability to establish the access level and modify or revoke remote access at any time for any reason.

The CDS platform allows SDPD access to the data provider's technology system. SDPD will only have access to the specific data within that system allowed by the entity. If the data being shared must be retained for a legitimate law enforcement purpose, such as evidence of a crime, SDPD shall collect the data being viewed. The collected data will be considered evidence and stored/impounded by SDPD in accordance with existing policy, procedure, and law.

DATA ACCESS

The San Diego Police Department shall designate in writing the personnel authorized to have access to the CDS platform. Authorized personnel who access and use the data shall comply with federal, state, and local laws, including the TRUST Ordinance, as well as applicable Department procedures.

DATA PROTECTION

All authorized users of the CDS platform shall access the data being shared with SDPD only through a login/password-protected system capable of documenting all access to information by name, date, and time.

Accessing, copying, forwarding, or releasing any evidence collected via a community entity's technology system other than for official law enforcement use and contrary to department policies and procedures is strictly prohibited. Public release of digital evidence is prohibited unless approved by the Chief of Police or designee.

The City's Department of Information Technology oversees the IT governance process and works with SDPD's Department of IT regarding project execution and risk assessment, selecting, and approving technology solutions.

DATA RETENTION

Once any saved data has been collected as evidence, evidence retention will be governed by SDPD Procedure 3.02 – Impound, Release, and Disposal of Property, Evidence.

PUBLIC ACCESS

The San Diego Police Department considers all data collected as evidence to be investigative records and is for official use only.

THIRD PARTY DATA SHARING

The San Diego Police Department may only share data collected as evidence via CDS with other law enforcement agencies for legitimate law enforcement purposes, with the San Diego City Attorney or the San Diego District Attorney in connection with legal proceedings, or in response to a valid court or judicial order, all in accordance with this Use Policy.

SDPD shall not:



Surveillance Use Policy

CDS – Community Data Sharing
San Diego Police Department

- Share images, video or data with Immigration and Customs Enforcement (ICE), Border Patrol, or any other law enforcement agency for the purpose of enforcing immigration laws.
- Release images, video or data to aid in the prosecution of any individual for providing, obtaining, or assisting in the provision or obtention of an abortion or any reproductive care.

TRAINING

All personnel designated as system users shall receive training in the operation of the CDS platform by the program administrator and subject matter experts approved by the Department.

All employees authorized to access shared data via the CDS platform shall be provided a copy of this Surveillance Use Policy, along with instructions on the constitutional protections (e.g., Fourth Amendment, etc.) and case law requirements associated with its use.

The San Diego Police Department will provide training that includes guidance on the use of shared data systems via the CDS platform and interaction with dispatch and patrol operations, along with a review regarding relevant policies and procedures. The training should also address applicable laws related to the use of video recording equipment and privacy.

AUDITING AND OVERSIGHT

The San Diego Police Department shall maintain a list of personnel who are authorized to have access to the CDS platform. The authorization shall ensure that their access to and use of the technology data shared with SDPD comply with federal, state, and local laws, the TRUST Ordinance, and applicable Department policies and procedures.

The program administrator, who holds a supervisory rank, shall conduct system audits quarterly.

Audits shall include:

- Confirming compliance with state and local laws, including compliance with the Department's Use Policy.
- Confirming users have current training and authorization to access the shared data.
- Confirming that any access to shared data has a corresponding case number or incident number.
- Confirming that complete case numbers and incident numbers are being used.

Subject to the provisions of this policy, the Chief of Police or their designee has the discretion to prohibit the review of any shared data by Department employees if it is in the best interest of the Department or the City of San Diego.

MAINTENANCE

The program administrator will ensure all transmissions and connections used by community entities to share their technology data are made using secure connections, and all security protocols are maintained.

Any required maintenance of a technology system sharing data with SDPD will be the responsibility of the owner of the technology system (i.e., the community entity that has volunteered to share its data with SDPD).