



Surveillance Use Policy

DFR- Drone as First Responder Systems San Diego Police Department

PURPOSE

A Drone as First Responder (DFR) Program utilizes an Unmanned Aircraft System (UAS) to respond to police and public safety incidents such as crimes in progress, missing persons and all-hazard events (e.g., fires, floods). The DFR is launched from remotely positioned docking stations located throughout the city, and controlled by a pilot on the ground. A UAS is battery-operated, weighs less than 55 pounds, has several rotors and is equipped with a video camera and an onboard computer.

DFR systems gather and transmit real-time data from incident scenes. Integration with existing systems, such as computer-aided dispatch (CAD) and 911 software, will allow rapid response and close coordination among first responders and command centers to enhance safety and situational awareness.

USE

DFR systems shall be for legitimate law enforcement purposes only.

Legitimate law enforcement purposes include, but are not limited to:

1. Providing remote aerial camera observation and imagery during dispatched incidents for safety and situational awareness.
2. Search and Rescue support for lost, missing, stranded persons, or suspects.
3. Providing aerial observation and imagery in support of fire response, all-hazard, disaster response and critical incidents.
4. Providing video digital media recordings in support of crime scene evidence collection and mapping.
5. DFR pilot training

The following uses of DFR shall be expressly prohibited:

- To violate any Constitutional rights or 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.
- Any use in a discriminatory manner that targets 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, in accordance with Department Policy 9.31.
- Any usage that does not conform with Police Department Policy and Procedure or FAA Regulations.

The following technological modifications to DFR and usage shall be expressly prohibited:

- The weaponization of DFR.
- The use of integrated facial recognition/biometrics technology or Automated License Plate Recognition Technology (ALPR).



Surveillance Use Policy

DFR- Drone as First Responder Systems San Diego Police Department

Per Department Policy 1.01, 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 DFR systems are:

- 8.23 – Use of Small Unmanned Aircraft System
- 1.57 – Military Equipment
- 3.02 – Impound, Release, and Disposal of Property, Evidence and Articles Missing Identification Marks

DATA COLLECTION

DFR systems equipment does not automatically record video. The DFR pilot manually controls when the DFR system will record.

Data collected by DFR systems is similar to a handheld “point-and-shoot” camera or a Body-Worn Camera.

DFR systems can collect video in multiple visual spectrums, such as Red, Green, and Blue (RGB) light spectrum, Forward Looking Infrared (FLIR) spectrum commonly known as “thermal imagery,” the infrared spectrum commonly known as “IR,” “Night Vision” or “Low-Light,” and Light Detection and Ranging (LIDAR). These capabilities are dependent on the camera payload attached to the DFR systems.

While on scene, the DFR pilot will manually activate the video recording capability of the DFR system. This captured video is regarded as Digital Media Evidence (DME) and is treated as evidence throughout the remainder of the operation until the DME is properly impounded and documented by the DFR pilot assigned to the operation.

The DFR systems pilot will not activate the video recording function until the DFR system is on scene and will discontinue recording before departing the incident scene. During all operations, the DFR pilot is trained to make every effort to only capture visual imagery of the law enforcement contact or the intended target of observation.

All DME captured on the DFR system is retained onboard the DFR system until it returns to its docking station. Upon arrival at the docking station, the DFR pilot in command of that flight will be responsible for transferring the DME to the Department’s DME storage database (e.g., evidence.com)

The DFR system also collects flight information data, including its own location, altitude, and flight time. This information does not contain any personal identifying information (PII) and is not considered DME. This information is included in the report that the DFR pilot will complete at the conclusion of each flight.

DATA ACCESS

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.

Recorded data and images may be reviewed in accordance with the following criteria:



Surveillance Use Policy

DFR- Drone as First Responder Systems San Diego Police Department

- By a Department employee conducting an official investigation.
- By members of the City Attorney's Office or Risk Management in connection with pending litigation.
- Pursuant to lawful process or by court personnel otherwise authorized to view evidence in a related case.
- The Chief of Police has the discretion to allow the viewing or release of data and images if they determine it is in the best interest of the Department.
- As part of Department-approved training.

Accessing, copying, forwarding, or releasing any digital evidence 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.

All DME is retained onboard the DFR systems until the UAS has returned to its dock. Only DFR systems pilots may possess DFR systems or DME collected by those systems until the data is uploaded to the Department's DME storage database.

DATA PROTECTION

All DME will be retained within the DFR system until the data is removed from the aircraft and uploaded to the Department's DME storage database.

Other (non-PII) data that is recorded by the DFR system, including the UAS's location, altitude, and flight times, is accessible remotely by the DFR pilot and DFR systems manager only. Direct access to this information is password-protected and can only be accessed by designated DFR systems personnel. This information does not contain any critically vulnerable data, nor information that would violate an individual's civil rights or infringe upon their privacy. This information is included as part of the post-operation documentation report and is publicly accessible information that documents every DFR system operation.

Once DME has been impounded, data protection becomes the responsibility of the Property Unit or the Department's DME storage database and all such evidence is controlled and regulated by SDPD Procedure 3.02 – Impound, Release, and Disposal of Property, Evidence and Articles Missing Identification marks.

DATA RETENTION

Once DME has been impounded, evidence retention is the responsibility of the SDPD Property Unit or the Department's DME storage database and all such evidence is controlled and regulated by SDPD Procedure 3.02 – Impound, Release, and Disposal of Property, Evidence and Articles Missing Identification marks.



Surveillance Use Policy

DFR- Drone as First Responder Systems
San Diego Police Department

PUBLIC ACCESS

DFR system-collected DME can only be accessed by DFR system personnel prior to evidence impound. Once DFR system collected DME is impounded by DFR system personnel into the Department's DME storage database, access to this DME is controlled and regulated by SDPD Procedure 3.02 – Impound, Release, and Disposal of Property, Evidence and Articles Missing Identification marks.

If DME is evidence in litigation, then the laws of discovery and evidentiary privilege govern requests and disputes related to disclosure.

THIRD PARTY DATA SHARING

The Department only shares DFR data 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:

- Share DFR 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, as required by California Government Code 7284.6 - The California Values Act.
- Release DFR 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, in accordance with California Penal Code 423.2, the California FACE Act and Penal Code 13778.2.
- Sell DFR data obtained or received by SDPD.

TRAINING

Only personnel designated by the DFR systems manager may operate the DFR systems.

Designated DFR pilots are the only personnel who are authorized to be in possession of or use any of the Department's DFR systems.

DFR pilots in training are authorized to operate the DFR systems under the direction of a designated DFR pilot.

Pilot candidates must complete the following training prior to being designated as a DFR pilot:

1. FAA CFR Part 107 Small Unmanned Aircraft System Certification
2. DFR system manufacturer's training
3. SDPD UAS Pilot Academy - Approximately 80 hours of specialized UAS Flight and classroom training to include procedures on evidence collection, retention, impounding, and the protection of citizens' privacy, civil rights, and Fourth Amendment during operations.



Surveillance Use Policy

DFR- Drone as First Responder Systems
San Diego Police Department

AUDITING AND OVERSIGHT

The DFR systems manager is the primary oversight and approver of DFR operations, including DFR flights, data collection, evidence impounding, and documentation by the DFR pilot. The DFR systems manager is responsible for ensuring all actions by DFR personnel comply with SDPD Department Procedures and the Surveillance Use Policy for DFR systems.

The DFR administrator, who holds a supervisory rank, is the primary oversight and auditor for all DFR operations.

Audits include:

- Confirming compliance with state and local laws, including compliance with the Department's Use Policy.
- Confirming that equipment is functioning properly.
- Confirming data is being impounded and retained per Department Policy 3.02.
- Confirming users have current training and authorization to use the system.
- Confirming that each use is properly logged and documented.
- Confirming that the complete case and incident numbers are being used.

Internal records for DFR operations are managed by, and can only be accessed by, the DFR manager or their designee. The DFR systems manager will generate and publish monthly and annual audit reports on DFR operations in accordance with federal, state, and local laws in addition to Department policies and procedures.

MAINTENANCE

DFR systems equipment will be inspected and maintained in accordance with the manufacturer's recommended inspection and maintenance schedules.

DFR systems equipment will also be inspected and maintained in accordance with applicable FAA regulations.

All inspections and maintenance procedures will be conducted by properly trained personnel. Inspection and maintenance records will be maintained and audited by the DFR systems manager or their designee.