BODY-WORN CAMERAS

GENERAL ORDER #10.06

Adopted: 5/29/19	**Pages:** 13
Persons Affected: All personnel	**Authority:** Laura Wilson, Director
IALCEA Standards: 9.1.7	

Revision History

Replaces SUDPS G.O. #10.06 (5/23/2018)

PURPOSE AND SCOPE

This policy is intended to provide deputies with guidelines on when and how to use body-worn cameras (BWCs), including both audio and video recording, so that deputies may reliably record their contacts with the public, arrestees, and inmates in accordance with the law. BWCs provide documentary evidence for criminal investigations, internal or administrative investigations, and civil litigation. *Stanford University Department of Public Safety (SUDPS) deputies* shall utilize this device appropriately and in accordance with the provisions in this General Order to maximize the effectiveness of the audio/video documentation, to achieve operational objectives, and to ensure evidence integrity. While BWC recordings can provide an objective record of events, it is understood that video/audio recordings may not necessarily reflect the entire experience or state of mind of the individual employee(s) in a given incident. In some circumstances, the BWC will capture information that may not have been heard and/or observed by the involved *employee(s).* Similarly, there will be situations where the BWC will not capture information that was heard and/or observed by the involved *employee(s).* BWCs have also been proven to be valuable in their ability to direct and supplement deputy training. BWCs also provide transparency for the community as well as individual and organizational accountability. BWCs can help build community trust, improve conduct and behavior, and reinforce community policing.

BWCs are small video cameras typically attached to a deputy's clothing. They capture, from a deputy's point of view, video and audio recordings of the deputy's activities, including traffic stops, arrests, searches, interrogations, and critical incidents such as deputy-involved shootings. The primary objective of the BWC system is to document deputy contacts, arrests, and critical incidents. Video footage collected by the BWCs will be used as evidence in both criminal and administrative investigations.

Video footage not relevant to any investigation will be discarded after a defined retention period.

SUDPS's BWCs comply with the Criminal Justice Information System (CJIS) requirements for transfer and storage of BWC obtained data stored on-site. It does so by encrypting BWC obtained data in-transit and storing it at rest in an on-site, firewalled server that is physically secured, and to which there is controlled access.

POLICY

It is the policy of the Sheriff's Office and the *SUDPS* that deputies shall activate the BWCs when such use is appropriate in the proper performance of his or her official duties, where the recordings are consistent with this policy and law.

This policy does not govern the use of surreptitious recording devices used in investigative operations. The *SUDPS* will provide sworn personnel BWCs for use during the performance of their official duties. Deputies will only use the BWC system issued and approved by the *SUDPS* for official duties. The wearing of any other personal video recorder for the same purpose is not authorized without permission of the *Director of Public Safety or his or her designee.*

DEFINTIONS

TERM	DEFINITION
Files	*Refers to all sounds, images, and associated Metadata captured by a Body Worn Camera (BWC)*

PROCEDURES *(IACLEA 9.1.7)*

A. GENERAL USE

1. Authorized Use of BWC Footage:

- Use as evidence in criminal investigations
- Use as evidence in administrative investigations (e.g., allegations of deputy misconduct)

- Use to enhance the accuracy of deputies' reports and testimony in court, unless otherwise prohibited by this Policy
- Use for deputy evaluation and training
- Use as a training aid, if an incident captured on a recording has training value
- Supervisors will randomly audit BWC recordings to ensure that the equipment is operating properly and that deputies are using BWCs appropriately and in accordance with policy and procedure.

B. USE OF BODY WORN CAMERA

Each SUDPS deputy is assigned a specific BWC. Deputies will use their assigned BWC. When not in use all SUDPS BWCs are to be stored in the BWC transfer station.

1. At the beginning of each shift, deputies shall determine whether their recording equipment is operational in accordance with the BWC manufacturer's specifications. The deputy shall ensure that the camera is fully charged *by checking the BWC's battery indicator on the LCD screen. Deputies will also verify* that the data from the previous shift has been downloaded *by confirming the recording indicator on the LCD screen indicates "0%."*

If a problem is found, with their BWC, the deputy shall arrange for repair or adjustment *by notifying SUDPS IT Services. When a deputy's assigned BWC malfunctions or is out for repair, spare BWCs are available in the transfer station along with a sign out log. It will be the deputy's responsibility to check out a spare BWC and complete the log prior to going into service.* If the *BWC* system is malfunctioning, the deputy shall immediately report this to their *sergeant or other on-duty supervisor.*

2. If a BWC malfunctions or is inoperable *during the course of a shift* and the deputy cannot utilize a BWC during *a call for service where activation of the BWC would be expected*, this shall be noted in all written reports, *including the deputy's daily activity report and the shift log*, so that there is a contemporaneous record. *Upon learning that the BWC is not operating, the deputy shall make an effort to replace the BWC with an operable BWC as soon as possible.*

3. During their shift, deputies shall:

a. Ensure that the BWC is properly worn and positioned to record events.

b. Wear the recorder in a conspicuous manner.

c. Make every reasonable effort to activate the BWC prior to making contact in any of the following incidents:

1) Any investigative encounter to confirm, or dispel a suspicion that the person may be involved in criminal activity. This includes detentions, vehicle stops, jail altercations, pedestrian stops, and consensual encounters.

2) Probation searches, parole searches, post release community supervision searches, mandatory supervision, cell extractions, or consent searches; however, strip searches shall not be recorded unless a confrontation occurs.

3) Service of search or arrest warrants.

4) All suspect statements.

d. Make every reasonable effort to record any contact should the contact become confrontational, assaultive, or enforcement-oriented.

4. The deputy will not edit or delete any files recorded by the BWC without supervisor approval.

5. This policy is not intended to describe every possible circumstance. In addition to the required conditions of operation, deputies should activate the system any time they feel its use would be appropriate and/or valuable to document an incident. Recording such contacts shall be the rule and not the exception. If circumstances prevent a deputy from recording such a contact, then this must be noted along with the explanation in any subsequent report.

6. Deputies shall make every effort to activate their BWC prior to making contact in any of the following circumstances:

a. Enforcement encounters where there is a reasonable suspicion that the person is involved in criminal activity or a violation of law. This includes, but is not limited to, dispatched calls where criminal activity is reported and/or suspected, self-initiated activities, consensual contacts, traffic stops, pedestrian checks, or any other investigative or enforcement encounters.

b. Any other contact that becomes adversarial after the initial contact in a situation that would not otherwise require recording.

7. Deputies may activate the BWC before/during any other incident at their discretion.

8. Unless it is unsafe or impractical to do so, or mechanical issues impede the use of the device, it is recommended that deputies record any interview, pedestrian or inmate contacts, and other events.

9. Personnel shall not use the BWC to record any conversations of or between another department member or employee without the member's/employee's knowledge or consent.

10. Once activated, the recording should not be intentionally terminated until the deputy's participation in the incident is complete; or the situation no longer fits the criteria for activation (e.g. prisoner in custody and seated in a patrol car); or for purposes of exchanging confidential information or conducting interviews with crime victims, confidential informants or witnesses who do not wish to be recorded (examples of this can include witness interviews or victim interviews on sensitive cases, e.g. sexual assault, child abuse, etc.) or unless tactical, safety, privacy concerns or practical reasons dictate otherwise. If the recording is terminated prior to the conclusion of the incident or contact for reasons other than those contemplated by this section, or if the mute feature is utilized under such circumstances, the reasons for the premature termination or muting of the audio must be documented in the report. In the event no report is prepared, then the fact that the recording was terminated prematurely or muting feature was activated must be documented in an Employee's Report *(ER)* and provided to the *deputy's* supervisor.

a. *Prior to utilizing the mute feature, employees should state the reason for muting the sound. The purpose of doing so is to make it obvious to the viewer why the audio is not being recorded. Reasons for muting could be:*

- *Training discussion*
- *Debriefing*
- *Confidential information exchange*

11. Deputies are not required to advise or obtain consent from a private person when:

a. In a public place,

b. At any jail or the jail facilities, or

c. In a location where there is an expectation of privacy but the deputy is lawfully present.

12. Whenever possible, deputies should inform individuals that they are being recorded. In locations where individuals have a reasonable expectation of privacy, such as a residence, they may decline to be recorded unless the recording is being made pursuant to an arrest or search of the residence or the individuals. The BWC shall remain activated until the event is completed in order to ensure the integrity of the recording unless the contact moves into an area restricted by this policy.

13. In general, deputies should not activate the BWC and/or use caution when entering a public locker room, changing room, restroom, the office of a doctor or lawyer, or another place where individuals unrelated to the investigation are present and would have a heightened expectation of privacy. Deputies should not record the provision of patient care at any hospital or health facility unless the circumstances

dictate the need for BWC activation, such as the contact becoming uncooperative or resistive.

14. If a deputy fails to activate the BWC, fails to record the entire contact, or interrupts the recording, the deputy shall document why a recording was not made, was interrupted, or was terminated. *This shall be documented in the deputy's report or if no report is completed an ER report will be completed and forwarded to their supervisor. The documentation shall state when and where the incident occurred, why the BWC was not activated, and that the device failed to record the entire incident or why the recording was interrupted.*

15. *Deputies shall note in the arrest and other reports when BWC records are made during the course of an incident. The report will include:*

a. *A statement that the incident was audio/video recorded using the department issued BWC*

b. *A synopsis of the incident*

c. *A statement that for complete details refer to the recorded file.*

16. Deputies are not required to activate the BWC when engaged in privileged communication as defined by the Evidence Code.

C. PROHIBITED USES

1. Prohibited uses of the BWC system include:

- Using the BWC system for personal purposes
- Recording conversations between other employees without their consent
- Making copies of BWC videos for personal use, or disseminating those videos in any form or manner outside the parameters of this *Body Worn Camera Policy, such as,* accessing, copying, or releasing files for non-law enforcement purposes is prohibited
- Removing, dismantling, or tampering with any hardware and/or software component of the BWC system
- Recording the provision of patient care at any hospital or health facility, unless the circumstances dictate the need for BWC activation, such as the patient becoming uncooperative or resistive/assaultive *or to capture a dying declaration related to a criminal investigation*.

D. DATA COLLECTION

1. The BWC collects video and audio recordings of events occurring in the user's presence. As each video is created, the system automatically stamps the video with the current date/time and the camera user's identity. The user has the option to add metadata manually to existing recordings after they are created. Such metadata may include but is not limited to:

- Category of contact (from Sheriffs' Office defined list)
- Disposition of contact (arrest, citation, etc.)
- Associated case number

2. Any data obtained through the BWC footage must be used and handled pursuant to this policy.

3. Recordings

a. Unauthorized use, duplication, and/or distribution of BWC files is prohibited.

1) Personnel shall not make copies of any BWC file for their personal use, to include but not limited to, uploading files to public or social media internet web sites, and are prohibited from using a recording device such as a phone camera or secondary video camera to record BWC files.

2) All recorded media, images, and audio from the BWC shall not be copied, released, or disseminated in any form or manner outside the parameters of this policy without the express consent of the Sheriff or his or her designee.

3) The BWC data should be uploaded in a timely manner.

b. Deputies shall not remove, dismantle, or tamper with any hardware and/or software component or part of the BWC.

E. DATA ACCESS AND PUBLIC REQUEST

1. Departmental File Review

a. *SUDPS* personnel may review BWC files as follows:

1) For their involvement in an incident, in order to complete a criminal investigation and/or prepare official reports.

2) Prior to courtroom or deposition testimony or for courtroom presentation.

3) By a supervisor reviewing a specific incident

4) By a Sheriff's Office or *SUDPS* detective or investigator who is participating in an official investigation, such as a criminal investigation, a personnel complaint or an administrative inquiry;

5) By others with the permission of a supervisor if they are participating in an official investigation or other official reasons.

b. In accordance with the "Officer-Involved Incident," as defined by the Santa Clara County Police Chiefs Protocol or case involving a serious bodily injury, the involved deputy will provide an initial statement to investigators prior to reviewing any recorded footage of the incident. The involved deputy will have an opportunity to review recordings after the initial statement has been taken and provide a supplemental statement if desired. A deputy may review the BWC file prior to completing an incident report for other events that are not an "Officer-Involved Incident," or case involving a serious bodily injury.

c. Critical Incidents: Deputies will be allowed to consult legal representation prior to providing a statement pursuant to an administrative and/or criminal inquiry.

1) When safe and practical, an on scene supervisor may retrieve the BWC from the involved deputy(ies) at the scene. The supervisor will be responsible for assuring the camera is docked and uploaded to the storage server.

2) Following a time sensitive critical incident, a video may only be viewed by the on-scene supervisor prior to being uploaded to the storage server:

a) When exigent circumstances occur, such as when a deputy is injured, or to obtain identifying suspect information or other pertinent information.

b) To allow investigators, such as Internal Affairs personnel, to view video in order to assist in an investigation.

d. The server shall only be accessed from Department authorized computers.

2. BWC File Request

a. Departmental Requests

1) Copies of the BWC data shall only be released to authorized personnel following a formal request to the relevant Division Commander, *SUDPS Director of Public Safety, the* Assistant Sheriff, Undersheriff or Sheriff *of Santa Clara County*.

2) BWC recordings shall be treated as other forms of direct evidence and subject to discovery and disclosure in accordance with law.

b. Non-Departmental requests must be approved by the Sheriff or his/her designee and in accordance with the following:

1) All other requests for a BWC file shall be accepted and processed in accordance with federal, state, local statues and Departmental policy as set forth in General Order 16.01 Release of Records and Information.

2) Media inquiries and/or requests shall be received and processed in accordance with General Order 24.00.

3) Any identifiable personnel captured on either audio or video will be advised in writing, prior to any release under CPRA (California Public Records Act) and the guidelines consistent with the General Orders and Penal Code §832.5.

4) An individual who has filed an officer-misconduct complaint against Sheriff's Office personnel may view applicable BWC footage with Sheriffs Administrative Investigators, subject to the following conditions

a) When viewing the BWC footage is not prohibited by applicable law as determined by County Counsel;

b) When the BWC footage is not part of a criminal investigation, civil lawsuit, or government tort claim process;

c) When the person viewing the BWC footage is the subject or recipient of the alleged officer misconduct;

d) When viewing the BWC footage will not hinder or damage subsequent investigative processes or violate the integrity of the investigation, as determined by the investigating agency;

e) When privacy protections are utilized to protect the privacy interests of other individuals who may appear in the footage.

3. Copying Procedures

a. A copy of the BWC file may be made by Records, Administration or Investigations personnel in accordance with the provisions of this *Body Worn Camera Policy* for evidence, District Attorney request or other approved reasons.

b. If a video is evidence in a case, Investigations personnel shall make a copy of the video, and book the copy into evidence. (*Not applicable to SUDPS as BWC files are stored on firewalled, on-site, physically secure primary and backup servers.*)

c. Other than as provided in this General Order, no member of this Department shall download any video onto any computer, device, drive, CD, DVD or any other format without the express consent of the *Director of Public Safety* or his/her designee.

d. No member of this Department shall use an external recording device to copy or record BWC video when the video is displayed on another computer or device.

F. DATA PROTECTION AND RETENTION

BWC data will be uploaded to a Criminal Justice Information System (CJIS) compliant *on*-site Evidence Management System (EMS) managed by the BWC vendor. CJIS standards include very strict requirements for data security, including in-transit encryption, at-rest encryption, strict access control to the physical data center, and background checks for all employees who have access to the servers. The system contains detailed configurable permissions limiting access to specific groups of videos to authorized users. An audit log is maintained of all access to video footage.

Once a successful upload of the data to the EMS has occurred, the uploaded data will be evaluated and authenticated. At this point, all the data on the BWC device will be automatically deleted. The stored data will be held in the EMS for the data retention period explained below. The BWCs will be stored in restricted areas not accessible to the general public. Except for a brief period while the BWCs are uploading their data, BWCs stored in this manner will have no data stored on them.

1. Storage

a. All files for each BWC deployed on a shift shall be securely uploaded by the individual deputy to whom the BWC was issued periodically and no later than the end of each shift. Uploading should occur during the deputy's regularly schedule shift. Deputies must secure prior approval from their supervisor for overtime if upload after the end of each shift is necessary. Each file shall contain information related to the date, BWC identifier, the type of event or incident and assigned deputy.

1) As soon as it is practicable, the appropriate supervisor will take charge of a/all deputy's(ies') BWC(s) if the deputy(ies) has/have been involved in a deputy-involved-shooting, or an incident resulting in a death, or other use-of-force incident. The appropriate supervisor will be responsible for uploading the files from the BWC(s).

b. All images and sounds recorded by the BWC are the exclusive property of this department.

c. All access to BWC data (images, sounds, and metadata) must be specifically authorized by the Sheriff, or his or her designee, and all access is to be audited

to ensure that only authorized users are accessing the data for legitimate and authorized purposes.

d. Files should be securely stored in accordance with California records retention laws and no longer than useful for the purposes of training or for use in an investigation or prosecution. In capital punishment prosecutions, recordings shall be kept until the offender is no longer under control of a criminal justice agency.

e. Files will be stored *in an on-site* internal server and managed *by the SUDPS's IT Administrator* with the necessary infrastructure to securely maintain restricted information in accordance with legal requirements.

2. Request for Deletion of Accidental Recording

a. In the event of an accidental activation of the BWC where the resulting recording is of no investigative or evidentiary value, a deputy may request the recording be deleted by submitting an email request to their *Director of Public Safety or his or her* designee with sufficient information to locate the recording. The *Director of Public Safety* or designee shall review the file, approve or deny the request, and forward to the *SUDPS IT* Administrator for action. The requesting employee shall be notified of the outcome.

b. In the event of an activation of a BWC where the Sheriff, his or her designee, *or the Director of Public Safety*, determines that a BWC recording contains personal and/or private conversations or images of any individual unrelated to an ongoing criminal or internal affairs investigation, or otherwise has no valid official purposes, and which has no apparent evidentiary or investigatory value, may be deleted.

3. Retention

a. All BWC recordings/files (including copies) in the Sheriff's Office's *and SUDPS's* possession relating to incidents where criminal charges are filed shall be retained in the Investigation file according to the relevant evidentiary statute.

b. All BWC recordings/files (including copies) in the Sheriffs Office's *and SUDPS's* possession relating to potential criminal charges that are not filed shall be retained for no longer than one year after the statute of limitations has expired.

c. All BWC recordings/files (including copies) in the Sheriff's Office's *and SUDPS's* possession relating to Internal Affairs Complaints (whether externally or internally generated) shall be preserved in accordance with Penal Code §832.18, or until the statute of limitations has expired for any criminal, administrative, or civil proceeding, whichever is later. BWC recordings/files (including copies) in the Sheriff's Office's possession shall then be deleted.

d. All BWC recordings/files (including copies) in the Sheriff's Office's *and SUDPS's*

possession of routine events that are not associated with either a criminal or administrative investigation or a civil 1itigation or administrative matter shall be retained for no longer than one year.

G. THIRD PARTY SHARING

The Evidence Management System is customizable and can allow or deny any level of data- sharing. Sheriff's Office *and SUDPS* limits but recognizes the need for data-sharing. The following agencies or situations are some of the potential third party data-sharing:

- Other law enforcement agencies with respect to a criminal or administrative investigation
- District Attorney's Office for use as evidence to aid in prosecution, in accordance with the laws governing evidence
- An outside administrative investigator who has been retained by *the Sheriff's* Administration *or SUDPS. Authorization for the sharing of information with an outside investigator will be the responsibility of the Sheriff's Office.*

H. TRAINING

Training conducted by the vendor for the BWC Unit will include operation of the camera and software necessary to implement the BWC program. Training conducted by the Sheriff's Office BWC Unit *or SUDPS's Personnel and Training Unit* will cover the applicable policy governing the use of the BWC system and operation of the BWC equipment and software. BWC training shall be provided in Sheriff's Office training academies.

1. Deputies should not use any BWC devices unless they have successfully completed training in the proper use of such equipment.

2. Training will include field applications, a review of the proper function and use of recording devices, mandatory use, recommended use, and agency policy and procedures as they pertain to the use of the BWCs.

3. A written record of the training provided will be completed by the trainer and maintained in the deputy's training file.

I. OVERSIGHT

1. Audit and Other Use of BWC Files

a. An account must be created for each BWC user in the BWC system.

b. At least on a monthly basis, supervisors will randomly review BWC recordings to ensure that the equipment is operating properly and that deputies are using the devices appropriately and in accordance with policy and to identify any areas in which additional training or guidance is required. It is not the intent of the policy for supervisors to review BWC recordings to proactively discover policy violations. However, Supervisors may review BWC recordings in order to evaluate a deputy's performance for the purpose of meeting standards set forth in the General Orders or develop training curriculum to improve performance. Supervisors who inadvertently discover non-criminal policy violations shall have the discretion to resolve the violation with training or counseling or formal discipline. Should the policy violation rise to the level of formal discipline, the supervisor will adhere to all contractual and statutory procedures.

c. Should there be a specific complaint made against a deputy, the Supervisor or Internal Affairs personnel may access BWC recordings for administrative investigations limited to the specific complaint against the deputy(ies). The investigation may be expanded due to inadvertent discovery of other allegations, policy violations or other impermissible conduct during the initial review. Such expansions of investigations will be in compliance with all contractual and statutory procedures.

d. Field Training Officers (FTO) and FTO supervisors may review BWC recordings to evaluate the performance of deputies in the field training program.

e. Prior to using BWC footage for training purposes, the Department will contact any deputies involved or depicted in the footage and advise them of the desire to present said footage for training.

If an involved deputy or employee objects to the showing of a recording, his/her objection will be submitted to the *Director of Public Safety or his or her designee* to determine if the deputy's or employee's objection outweighs the training value. If the *Director of Public Safety or his or her designee* allows the footage to be used, the deputy or employee will be provided notice at least 24 hours before the footage is presented.