

County of Santa Clara Office of the District Attorney Surveillance Use Policy

Body-Worn Camera (BWC) System

1. Purpose

This Policy requires County of Santa Clara Office of the District Attorney (DAO) Bureau of Investigation (BOI) and assigned peace officers and legal process servers (hereafter, “investigators”) to follow specific rules in their operation of the BWC System, which includes body-worn cameras (BWCs), BWC-recorded data, and the associated off-site Evidence Management System (EMS) managed by the BWC vendor.

BWCs are small video cameras typically attached to an investigator’s clothing or tactical vest. They capture, from an investigator’s point of view, video, and audio recordings of the investigator’s activities, including potential traffic stops, arranged arrests, planned searches, planned interrogations, and critical incidents such as investigator-involved shootings. They provide documentary evidence for criminal investigations, internal or administrative investigations, and civil litigation. BWCs also provide transparency for the community as well as individual and organizational accountability by building trust and improving conduct.

Investigators employed by the Santa Clara County DAO BOI shall utilize its BWC system appropriately and in accordance with the provisions in this Policy to maximize the effectiveness of the audio/video documentation, to achieve operational objectives, and to ensure evidence integrity.

Pursuant to this Policy, it shall be permissible for investigators to use BWCs, within the requirements and limitations described herein, during the performance of their official duties for preplanned law enforcement operations. Investigators shall only use the BWCs issued and approved by the District Attorney’s Office for official duties. BWCs shall not have biometric capabilities such as facial recognition.

2. Authorized and Prohibited Uses

The DAO’s BWC System shall be used only in criminal investigations, civil litigation, and administrative investigations (e.g., allegations of investigator misconduct) to enhance the accuracy of investigators’ reports and courtroom testimony. It shall also be permissible to use the BWC System for law enforcement-related training unless otherwise prohibited by this Policy.

Ensuring BWC Functionality

At the beginning of each planned operation or law enforcement event, investigators shall determine whether the BWC is functioning in accordance with the BWC manufacturer’s specifications. If a problem is found, the investigator shall arrange for repair or adjustment of the equipment. The investigator shall also ensure that the camera is fully charged and that the data from the previous event has been downloaded to the EMS. If the data cannot be properly downloaded, the investigator shall immediately report this to their supervisor.

During a law enforcement event, investigators shall ensure that the BWC is properly worn in a conspicuous manner and is positioned to record events. If a BWC malfunctions or becomes inoperable during a law enforcement event, the investigator shall note the issue in all written reports so that there is a contemporaneous record.

Activation of BWCs

Recording contacts shall be the rule and not the exception. If circumstances prevent an investigator from recording any contact where activation of the BWC is mandated by this Policy or County DAO BOI Policy Manual Section 610, the investigator must explain those circumstances in any subsequent investigative report.

Investigators shall activate their BWCs prior to making contact in any of the following circumstances:

- Planned enforcement encounters where there is a reasonable suspicion that the subject is involved in criminal activity or a violation of law. This includes all detentions and consensual encounters.
- Any other contact with members of the public during a planned operation, including service of search or arrest warrants.
- Any contact that becomes confrontational, assaultive, or enforcement oriented.
- Any time an investigator believes its use would be appropriate and/or valuable to document an incident.

Notwithstanding the requirements above, DAO Special Operations Group (SOG) personnel who are issued BWCs and are engaged in an active Tactical SOG event shall defer to the SOG Tactical Commander for direction regarding the activation of the BWC.

Investigators are not required to advise or obtain consent from a private person when in a public space, any jail or jail facility, or any location in which the investigator is lawfully present and there is no reasonable expectation of privacy. In locations where individuals have a reasonable expectation of privacy,¹ such as a residence, investigators may only record if the investigator obtains consent from the individual(s) subject to the recording, or if the recording is being made pursuant to an arrest or search of the residence or the individuals.

Investigators shall use reasonable caution in recording in sensitive areas, including public locker room, changing room, restroom, hospital or health facility, doctor's or lawyer's office, or other places where individuals unrelated to the investigation are present and would have a heightened expectation of privacy. Investigators should not record the provision of patient care at any

¹ The Fourth Amendment to the United States Constitution guarantees that people will be safe from unreasonable searches and seizures. A "search" occurs for purposes of the Fourth Amendment when the Government violates a person's "reasonable expectation of privacy." People have reasonable expectations of privacy in their own person, house, vehicles, and business offices. They also have a reasonable expectation of privacy in their personal communications such as telephone calls, letters, and journals. In contrast, people have no reasonable expectation of privacy in things knowingly exposed to the public or held out to public view.

hospital or health facility unless the circumstances dictate the need for BWC activation, such as the patient becoming uncooperative or resistive with medical staff or investigators. Investigators 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.

The BWC System shall not be used for illegal purposes, and shall not be used to harass, intimidate, or discriminate against any individual or group.

Deactivation of BWCs

Once a BWC is activated, the investigator shall not intentionally mute or terminate the recording until:

- The investigator's direct participation in the incident is complete;
- The situation no longer fits the criteria for activation (e.g., location of warrant service secured with no further enforcement actions);
- There is an exchanging of confidential information;
- Crime victims, confidential informants, or witnesses refuse to be recorded (examples of this can include witness interviews or victim interviews on sensitive cases, e.g., sexual assault, human trafficking, etc.); or
- Tactical, safety, privacy concerns, or practical reasons dictate otherwise.

If the recording is terminated prior to the conclusion of the incident or contact, the reasons for the premature termination must be documented in the investigative report. When the justification for premature termination no longer exists, but the incident or contact remains active, the officer shall re-activate and/or unmute the camera. In the event no report is prepared, the fact that the recording was terminated prematurely must be documented in a report and provided to the investigator's supervisor.

Uploading BWC Data

Investigators shall ensure that all data captured by a BWC is promptly uploaded to the BOI's EMS. Personnel authorized to access the EMS may view stored EMS data to the extent consistent with law, the BOI Policy Manual, and this Policy. Authorized users who access BWC data in the EMS shall share the data only with other members of the prosecution team or as otherwise required by law. Investigators shall not use the BWC System for personal purposes. They shall not make any copies of BWC recordings for personal use or disseminate those recordings in any form or manner outside the parameters of this Policy or the BOI Policy Manual. Accessing, copying, or releasing files for non-law enforcement purposes is prohibited. Investigators shall not edit or delete any files recorded by the BWC without supervisor approval.

//

//

//

3. Data Collection

BWCs collect video and audio recordings of events occurring in the user's presence. As each video is created, the camera automatically stamps the recording with the current date and time, as well as the BWC 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 the category of contact, the disposition of contact, and the associated case number.

All data obtained through the BWC System must be used and handled pursuant to this Policy. Unauthorized use, duplication, and/or distribution of BWC data is prohibited. Personnel shall not share or make copies of any BWC file for their personal use, upload files to public or social media internet web sites without the authorization of the District Attorney, or use a recording device, such as a phone camera or secondary video camera, to record BWC files.

Any recorded media, images, audio, and data from the BWC System shall not be copied, released, or disseminated in any form or manner outside the parameters of this policy without the express consent of the District Attorney or their designee.

The BWC recordings and associated data should be uploaded in a timely manner.

4. Data Access

DAO personnel shall access and review BWC recordings and associated data only from DAO-authorized computers. Investigators shall access the recordings through the EMS, which shall be created so that only investigators and their supervisors have access to the content. For data to be accessible to members of the DAO who are not in the BOI, such as attorneys and paralegals, the assigned investigator and BOI support staff must digitally transfer a copy of the data to the case management system accessible only to those authorized employees. DAO personnel shall only access BWC data under the following circumstances:

- By a DAO supervisor reviewing a specific incident, such as a personnel complaint or an administrative inquiry.²
- By a DAO investigator who is participating in an official investigation, such as a criminal investigation.
- By a DAO investigator for their involvement in an incident and in order to complete a criminal investigation and/or prepare official reports.
- By a DAO investigator prior to providing a deposition testimony, or for courtroom presentation.
- By members of the prosecution team, including prosecutors and investigators, during

² In an Officer-Involved Incident (OII), as defined by the Santa Clara County Police Chiefs' Association Protocol, or in an OII involving serious bodily injury, the investigator involved in the incident shall not have an opportunity to review recordings until they have provided an initial statement to investigators investigating the incident. After providing an initial statement and after a subsequent review of the BWC footage, the involved investigator may provide a supplemental statement if desired. An investigator may review the BWC file prior to completing an incident report for other events that are not defined as Officer-Involved Incidents or incidents involving serious bodily injury.

all stages of litigation who have a right and need to access the data. Examples include case review, filing, and courtroom presentation.

- By a DAO supervisor conducting an administrative investigation of the conduct of an investigator while equipped with a BWC.³

Intra-County Data Access and Data Sharing

There shall be no intra-County access to the BWC recordings stored on the EMS or the DAO case management system. BWC recordings and associated data shall only be released following approval of a formal request to the District Attorney, Chief Assistant District Attorney, Chief Investigator, or their written designee. If the requestor has its own contract with the vendor that provides the EMS that the BOI uses to store the data, then that platform shall be used for all secure data sharing. If the requestor does not subscribe to that EMS, then data sharing shall be done through secure electronic download links or downloads to secure storage devices such as DVDs, CDs, and external drives.

Data Used for Training

It shall be permissible for BWC data to be used for training purposes, and it shall be permissible for DAO personnel receiving a DAO training to view BWC data that has been designated for that training. Prior to using BWC recordings for training purposes, Chief Investigator and/or Training Coordinator must approve the recording for use in training.⁴

For data sharing rules specific to members of the public and third parties, see Section 7 (Public Access) and Section 8 (Third-Party Data Sharing).

5. Data Protection

Uploading to EMS

Body camera recordings and associated data will be uploaded to a Criminal Justice Information System (CJIS) compliant off-site Evidence Management System (EMS) managed by the BWC vendor. CJIS standards include strict requirements for data security, including 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 accesses to video footage.

³ Should there be a specific complaint made against an investigator or the supervisor, Administrative Investigation personnel may access BWC recordings for administrative investigations limited to the specific complaint against the investigator(s). 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 comply with all contractual and statutory procedures.

⁴ Prior to BWC recordings being used for training purposes, BOI shall contact any investigators involved or depicted in the footage and advise them of the desire to present said footage for training. If an involved investigator or employee objects to the showing of a recording, their objection will be submitted to the Training Coordinator to determine if the investigator's or employee's objection outweighs the training value. If the Training Coordinator allows the footage to be used, the investigator or employee will be provided notice at least 24 hours before the footage is presented. The investigator may appeal this decision to the Chief Investigator or designee prior to the display of BWC 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.

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

As soon as practicable, the appropriate supervisor will take charge of all BWCs when an investigator is involved in an investigator-involved shooting, an incident resulting in death, or some other use-of-force incident. The appropriate supervisor will be responsible for uploading the files from the BWC(s).

Data Copying

In accordance with the processes and limitations provided by this Policy, BWC recordings and associated data may only be copied by authorized personnel in Records, Administration, or BOI for evidence pursuant to the direction of a BOI lieutenant or assigned prosecutor, District Attorney requests, or other approved reasons, such as CPRA requests, subpoenas, and court orders under the direction of a BOI lieutenant or Assistant District Attorney. Other than as provided in DAO policies and procedures, no member of BOI shall download any video onto any computer, device, drive, CD, DVD, or any other format without the express consent of the unit supervisor or their designee. No member of BOI shall use an external recording device to copy or record BWC recordings when they are displayed on another computer or device.

Data Security

All images and sounds recorded by the BWC are the exclusive property of the BOI. All access to BWC data (images, sounds, and metadata) must be specifically authorized by the District Attorney, or their designee. All access shall be audited to ensure only authorized users are accessing the data for legitimate and authorized purposes.

6. Data Retention

Recordings and associated data collected by BWCs shall be maintained in accordance with this Policy, applicable state and federal laws, and the Santa Clara County District Attorney's Office Record Retention and Destruction Policy approved by the Board of Supervisors.

Data that is relevant to administrative/personnel-related matters shall be retained through the adjudication of any administrative case or civil case in a recognized court of law, as well as allotment of time for appeals process and statute of limitations. All BWC recordings and data in the District Attorney's Office's possession relating to Internal Affairs complaints (whether externally or internally generated) shall be preserved under the direction of BOI's Chief and in

accordance with Penal Code section 832.18, or until the statute of limitations has expired for any criminal, administrative, or civil proceeding, whichever is later.

To the extent that data is not delineated in this section, the data shall be destroyed no later than two years after (1) the time for an appeals process expires; (2) the statute of limitations expires; and (3) for data regarding a County employee's administrative investigation, the date the employee's employment for the County terminates.

In the event of an accidental activation of a BWC where the resulting recording is of no investigative or evidentiary value, an investigator may request the recording be deleted by submitting an email request to the unit supervisor or designee with sufficient information to locate the recording. The unit supervisor or designee shall review the file, and if the request is approved, determine how long the recording shall be retained before forwarding the request to delete to the System Administrator (Administrative Lieutenant) for action. The unit supervisor or designee shall not approve a deletion request if the underlying data has investigative or evidentiary value. The requesting employee shall be notified of the outcome.

In the event of an activation of a BWC where the District Attorney or their designee 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, the recording may be deleted at the direction of the District Attorney or their designee.

7. Public Access

Absent a court order, the public shall not have direct access to BWC recordings and associated data. If a California Public Records Act (CPRA) request, request pursuant to Penal Code section 832.7(b), subpoena, or court order is issued for BWC recordings and/or associated data, the records shall be made public, or deemed exempt from public disclosure, pursuant to state or federal law, after consultation with the Office of the County Counsel as needed. Any identifiable personnel captured on either audio or video will be advised in writing, prior to any release under the CPRA and the guidelines consistent with Penal Code section 832.5.

Media inquiries and/or requests shall be received and processed in accordance with DAO policy. Any identifiable DAO personnel captured on either audio or video will be advised in writing, prior to any release under the CPRA and the guidelines consistent with Penal Code section 832.5.

An individual who has filed a misconduct complaint against District Attorney's Office personnel may view applicable BWC footage with District Attorney's Administrative Investigators, subject to the following circumstances: 1) when viewing the BWC footage is not prohibited by applicable law as determined in consultation with the Office of the County Counsel; 2) when the BWC footage is not part of a criminal investigation, civil lawsuit, or government tort claim process; 3) when the person viewing the BWC footage is the subject or recipient of the alleged officer misconduct; 4) 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; and 5) when privacy protections are utilized to protect the privacy interests of other individuals who may appear in the footage.

8. Third-Party Data-Sharing

BWC recordings shall be treated as other forms of physical evidence and are thereby subject to discovery and disclosure in accordance with applicable law. To the extent that recordings are shared, BOI personnel shall share the evidence with authorized persons using the data-sharing capacities embedded in the EMS.

The documented sharing of BWC recordings and associated data shall be limited to the following third parties:

- Law enforcement agencies when relevant to an ongoing specific investigation or prosecution;
- Defense and appellate counsel and pro se litigants pursuant to Penal Code section 1054 et seq. and *Brady v. Maryland*;
- Individuals who have obtained a valid court order, subpoena, or otherwise approved in writing by the District Attorney or written designee;
- Parties in a civil litigation involving the County, in response to a subpoena or civil discovery;
- County Personnel Board and an employee's representative if the data is used as a basis for discipline, or an arbitrator or court regarding a County administrative action or litigation.

9. Training

DAO personnel involved in the use of BWCs shall receive training on the operation of the camera and software necessary to implement the BWC program. They shall also receive training regarding the applicable rules and policies governing the use of the BWC System and operation of the BWC equipment and software, including this Policy.

Investigators shall not use any BWC devices unless they have successfully completed training in the proper use of such equipment. Training shall include field applications, a review of the proper function and use of recording devices, mandatory use, recommended use, and BOI policy and procedures as they pertain to the use of the BWCs. A written record of the training provided will be completed by the trainer and maintained in the investigator's training file.

10. Oversight

District Attorney's Office Administration shall ensure compliance with this Policy and all applicable laws. The District Attorney or their written designee shall maintain records of access to the BWC System, including maintaining records of all written designations of data access pursuant to this Policy. The District Attorney or their written designee shall audit compliance with this Policy at least annually. Sanctions for violation of this Policy may range from counseling to termination, and in more serious breaches, may result in criminal prosecution.

//

At least on a monthly basis, supervisors will conduct audits of BWC recordings to ensure that the equipment is operating properly and that investigators are using the devices appropriately and in accordance with Policy. It is not the intent of this Policy that supervisors review BWC recordings to proactively discover policy violations. However, supervisors may review BWC recordings in order to evaluate an investigator's performance to develop training curriculum to improve performance. Supervisors who inadvertently discover non-criminal policy violations shall have the discretion to resolve the violation with training, counseling, or formal discipline based on the nature and severity of the misconduct. Should the policy violation rise to the level of formal discipline, the supervisor will adhere to all contractual and statutory procedures.

Approved as to Form and Legality

 1-16-24

Sam Cretcher
Office of the County Counsel