14. PURPOSE

The purpose of this policy is to provide members a policy that addresses the proper use, maintenance, and storage of body worn cameras; that requires the data recorded by body worn cameras to be retained and produced in accordance with state law; and that provides for a periodic review of the policy.

14.1. REVISION HISTORY

Date	Rev. No.	Change	Reference Section
12/27/16	1.0	New Policy	N/A
04/15/19	1.1	Entire Policy	Finalized Testing Policy
11/12/20	1.2	Entire Policy due to new Cameras	Throughout

14.2. PERSONS AFFECTED

All Police Personnel

14.3. POLICY

It is the policy of the Sunrise Police Department that members shall activate the body worn cameras when the recordings are consistent with what is outlined in this policy. This policy does not govern the use of surreptitious recording devices used in undercover operations.

14.4. DEFINITIONS

14.4.1. Body Worn Camera (BWC) – A portable electronic recording device that is worn on a member's person that records audio and video.

14.4.2. BWC Supervisor - Department member with full administrator rights who assigns and tracks BWC equipment, controls passwords, acts as a liaison with equipment vendor representatives,

manages the department's BWC devices, and is responsible for overseeing the retention and dissemination of body worn camera media.

14.4.3. BWC Coordinator – Assigned Police Information Technology Employee.

14.4.4. Data – Audio, video and metadata captured on the BWC.

14.4.5. Evidentiary Value - A recording of an incident or encounter has evidentiary value if it could be considered useful for investigative or prosecutorial purposes, including, but not limited to, a crime, arrest, a search, an inventory, response to resistance incident, pursuit, expedited or emergency response, or incidents involving injury or death.

14.4.6. DEMS - Cloud based digital evidence management system, containing all evidence captured, obtained or imported into the database.

14.4.7. Field Activities – Assignments or tasks that place or could reasonably be expected to place members in situations where they would be required to act in enforcement rather than administrative or support capacities.

14.4.8. Filename – A name used to uniquely identify a computer file stored in a file system. For the purposes of this policy, filename will refer to the Data file created by a BWC System.

14.5. RESPONSIBILITIES

14.5.1. All police personnel are responsible for complying with this policy. Supervisory Personnel are responsible for the enforcement of this policy. Unjustified violations may result in disciplinary action, up to and including termination.

14.5.2. This policy is not intended to be all-inclusive. It is intended to be a general guideline to be read in conjunction with all other Department rules, regulations, policies and procedures, as well as other City rules and ordinances.

14.6. PROCEDURES

14.6.1. General:

14.6.1.1. The Department has adopted the use of the BWCs to accomplish several objectives. The primary objectives are as follows:

14.6.1.1.1. BWCs allow for documentation of police-public contacts, arrests, and critical incidents.

14.6.1.1.2. BWC Data enhances the Department's ability to review probable cause for arrest, member and suspect interaction, and evidence for investigative and prosecutorial purposes. BWCs also provide additional information for member evaluation and training.

14.6.1.1.3. The BWC may also be useful in documenting crime and accident scenes or other events that include the confiscation and documentation of evidence or contraband.

14.6.1.2. All leased or purchased BWCs and BWC equipment and all Data are the property of the Sunrise Police Department, and only BWCs and BWC equipment approved by the Department shall be worn.

14.6.1.3. BWC placement on the user shall be in accordance with the BWC systems manufacturer's instructions using the issued camera mounts. The BWC must be worn on the front of the torso, between the collar bone and navel, and must be unobstructed.

14.6.1.4. The configuration of the BWC's capabilities will be set for 30 second pre-event buffering without audio.

14.6.1.5. If there is no Evidentiary Value, BWC users shall ensure their BWC is docked/uploaded at least once every shift.

14.6.1.6. If the BWC captures any media of evidentiary value, BWC users shall ensure their BWC data is uploaded before the end of their shift. The BWC user in lieu of uploading the video at the PSB, may choose to upload the video at their residence utilizing a department issued single bay dock at the conclusion of their shift. The BWC user may also use an Axon sync cable connected to their departmental issued laptop to upload videos both, during, or at the conclusion of their shift. If a user is unable to upload their Data prior to the end of their shift, and cannot utilize the aforementioned uploading mechanisms, they shall obtain approval from a supervisor.

14.6.1.7. BWC users shall ensure that all captured videos are properly categorized and labeled with the proper retention categories and, when applicable, the properly formatted agency case number for all videos (for example, 42-1234-567890).

14.6.1.8. Prior to deactivating the BWC, users shall make a recorded announcement as to the reason the device is being deactivated. After a BWC is deactivated, it is the user's responsibility to ensure they reactivate their BWC should the circumstances require it.

14.6.1.9. BWC users who inadvertently fail to activate their BWC at the onset of an incident that requires recording shall activate the BWC as soon as it is safe to do so. If a user inadvertently fails to activate, interrupts or deactivates their BWC during any portion of a situation that requires recording, the user shall notify their supervisor

14.6.1.10. The BWC shall remain affixed to the user in the same position it was worn throughout the event and shall not be removed unless necessary to render emergency medical attention. The lead investigator or designee will coordinate the response of the BWC Supervisor or designee, who will retrieve the BWC from the user(s) and process it according to the agency's evidence handling standards. The BWC Supervisor will be responsible for the recovery and storage of all evidence captured by the BWC.

14.6.1.11. Unless otherwise directed by the Chief of Police or designee, all members who are (a) on-duty and engaged in patrol or other Field Activities or (b) off-duty and working a special detail, will be required to wear the BWC at all times. This does not include follow-up interviews

being conducted by investigative personnel assigned to the Investigations Division or members engaged in dignitary protection.

14.6.1.12. Each BWC will be assigned to an individual member, and no member shall use a BWC not assigned to the member.

14.6.1.13. The activation and deactivation of BWCs will be documented in all incidents which require documentation to be generated (e.g., incident reports, field interview cards, response to resistance, etc.). If the member is involved in a situation where no written documentation is required to be generated and the member feels it necessary to document the incident, the member will initiate a written report. BWC Data is not a replacement for written reports. (CFA: 32.02D)

14.6.1.5.1. The first part of the documented narrative shall read, “BWC used during events”.

14.6.2. Recording Protocol (CFA: 32.02B):

14.6.2.1. Power On/Off:

14.6.2.1.1. At the beginning of a Field Activity shift the BWC shall be powered on and remain on for the entire shift.

14.6.2.1.2. Members shall never power off the BWC while on duty, unless:

14.6.2.1.2.1. Using the restroom.

14.6.2.1.2.2. Ordered by a judge in a courtroom.

14.6.2.1.2.3. Discussing any personal business with a doctor.

14.6.2.1.2.4. Discussing information with an attorney or union representative related to an Internal Affairs Investigation or providing a statement. The BWC shall be powered off during any dialogue with City of Sunrise counsel.

14.6.2.1.2.5. During any Department approved leave.

14.6.2.2. Activation/Deactivation:

14.6.2.2.1. Members shall begin recording with their BWCs in the below circumstances unless doing so would be unsafe, impossible, or impractical. If members are unable to begin recording with the BWC due to circumstances making it unsafe, impossible, or impractical to do so, members shall begin recording with the BWC at the first reasonable opportunity to do so.

14.6.2.2.2. At the initiation of a call, when the member arrives on scene for service or other activity that is investigative or enforcement in nature, or an encounter between the member of the Department and a member of the public that is investigative or enforcement in nature.

14.6.2.2.3. Any encounter that becomes confrontational after the initial contact.

14.6.2.2.4. Any other instance where the member believes that Data would assist in the investigation or prosecution of a crime or would assist in documenting the incident for later investigation or review.

14.6.2.2.5. Once the BWC has been activated, the BWC shall not be deactivated (recording stopped) unless:

14.6.2.2.5.1. The event or encounter has fully concluded; or

14.6.2.2.5.2. The member leaves the scene and anticipates no further involvement in the event; or

14.6.2.2.5.3. A supervisor or Department policy has authorized that a recording may cease because the member is no longer engaged in a related enforcement or investigative activity; or

14.6.2.2.5.4. Victims, witnesses, or other individuals wish to make a statement or share information, but refuse to do so while being recorded, or request that the BWC be turned off; or

14.6.2.2.5.5. The member is discussing strategic, investigative, tactical or administrative operations.

14.6.2.2.5.6. The member is at a city or county designated holding facility (i.e. BAT, Sunrise Police Department Holding Facility, etc.) and the prisoner is secured in a cell, unless the member feels that circumstances make it necessary to record.

14.6.2.2.5.6.1. The BWC must be activated immediately upon removing a prisoner out of a cell.

14.6.2.2.6. Administrative Services will keep an approved list of triggers designated by the Chief of Police that will be available for review by any member upon request. Triggers are an available technology that can automatically activate the BWC.

14.6.2.3. Prohibitions and Restrictions: (CFA: 32.02C)

14.6.2.3.1. Members are prohibited from using privately-owned BWCs and BWC equipment while on duty.

14.6.2.3.2. Members shall not activate a BWC to record:

14.6.2.3.2.1. During administrative activities.

14.6.2.3.2.2. When directed by a Supervisor.

14.6.2.3.2.3. Non-work related personal activity or personal use.

14.6.2.3.2.4. During or while discussing strategic, investigative, tactical or administrative operations. If a BWC needs to be deactivated during these instances, the member shall provide a brief verbal narrative detailing such.

14.6.2.3.2.5. Any purpose other than their official law enforcement duties.

14.6.2.3.2.6. Undercover personnel and confidential sources/informants.

14.6.2.4. Except as provided in sections 14.6.2.1.2. and 14.6.2.3.2., members must fully document the reason for:

14.6.2.4.1. Failing to activate the BWC prior to initiating a law enforcement or investigative contact when required.

14.6.2.4.2. Failing to record the entire contact.

14.6.2.4.3. Interrupting a recording for any reason to include turning the BWC off or muting the recording.

14.6.2.5. Except as authorized by the Chief of Police and Department policy, copying, recording, releasing, altering, erasing, or allowing unauthorized viewing of Department BWC Data (or portion thereof) is prohibited and may subject a member to disciplinary action and/or criminal and civil liability. (CFA: 32.02E)

14.6.2.6. With the exception of tagging BWC Data with a Filename for indexing purposes, members shall not erase, alter, modify or tamper with BWC Data, and shall not post BWC Data to social media without permission from the Chief of Police or designee.

14.6.2.7. When victims, witnesses, or other individuals wish to make a statement or share information, but refuse to do so while being recorded, or request that the BWC be deactivated, members may deactivate the BWC in order to obtain the statement or information. If the encounter begins when the BWC was not actively recording, the member may, but is not required to, temporarily activate the BWC for the sole purpose of documenting the individual's refusal to be recorded. The circumstances and reasons will be documented in these situations.

14.6.2.8. Members may notify, individuals, as soon as practical, that they are being recorded, unless it is unsafe, impractical, or impossible to do so.

14.6.2.9. Members are not required to obtain consent from individuals when the officer is engaged in an investigative or enforcement activity.

14.6.2.10. Members are not required to initiate or cease recording an event, situation or circumstance solely at the demand of an individual.

14.6.3. Docking / Storage and Security Procedures:

14.6.3.1. At the end of a BWC user's shift, they will securely download the Data contained on their BWC utilizing the approved download procedures (docking station). BWC Data will be stored utilizing a secure storage server. All Data will be stored utilizing approved security methods in compliance with Criminal Justice Information Services (CJIS) standards.

14.6.3.2. By the end of a BWC user's shift, anything of Evidentiary Value on their tablet shall be uploaded. The user shall utilize the authorized Wi-Fi access points in city buildings or their marked vehicle if equipped.

14.6.3.3. At no time shall any department member, other than the user issued the BWC touch, handle, or remove the BWC from the docking station. The only exception is removal by the BWC Supervisor for a maintenance related issue. If an investigator is working an administrative or criminal investigation where the BWC contains evidence related to an active investigation, the investigator will contact the BWC Supervisor to have the BWC removed from the docks.

14.6.3.4. Files will be securely stored in accordance with state records retention laws. However, files may be retained for longer than state record retention laws require if there is an investigative, prosecutorial, or training need for the files.

14.6.3.5. Data related to criminal or administrative investigations will be treated as any other digital evidence and proper chain of custody will be followed.

14.6.3.6. Data will be retained and disposed of in accordance with the State of Florida General Records Retention Schedules by designated personnel. (CFA: 32.02E)

14.6.3.7. All BWC Data shall be securely saved and stored with security and access control governed by audit trails and access logs.

14.6.3.8. The Department shall retain an unedited original version of stored Data. Anytime the Data is viewed, for what length of time and by whom, as well as any copying or editing should be automatically logged via the software.

14.6.4. Off-Duty Details:

14.6.4.1. All sworn personnel, regardless or rank, shall adhere to all aforementioned guidelines and procedures regarding the BWC. While engaged in off-duty details, BWC users shall upload their BWC Data at the beginning of their next regularly scheduled shift.
The exceptions requiring immediate uploading are as follows:

14.6.4.1.1. Make or capture an arrest

14.6.4.1.2. Response to resistance

14.6.4.1.3. Incidents involving injury or death

14.6.4.1.4. Absence longer than the BWC users regular days off

14.6.4.1.5. Searches of individuals, vehicles or property

14.6.5. Off-Duty:

14.6.5.1. It is recognized that off-duty officers may have to take enforcement action. This action may result in incidents not being recorded. When this occurs, department members shall document their actions and reason for not having their BWC in the incident report

14.6.6. Public Records Request:

14.6.6.1. Requests for Data will be handled in accordance with Chapter 119 of the Florida Statutes.

14.6.6.2. Any portion of the Data which has an exemption from public records shall be redacted prior to production under a public records request, the statutory citation which is the basis of the exemption shall be identified to the requesting party, and the remainder of the Data will be produced under the public records law.

14.6.4.6.1. Records Specialists in conjunction with the BWC Coordinator and Internal Affairs will fulfill public records.

14.6.6.2.2. Once the response to public records request is gathered and any applicable redactions are made, members from the Police IT Unit will forward the redacted Data to Internal Affairs for final review.

14.6.6.3. Internal Affairs or a person designated by the Chief of Police will review and after determining that the Data has been appropriately redacted or not redacted, shall release the public records request to the party making the request.

14.6.6.4. The assigned Detectives are responsible for reviewing the BWC Data of their assigned cases prior to submittal to the State Attorney's Office or any outside entity.

14.6.7. Report Writing, Court Presentation, Investigations and Training Purposes:

14.6.7.1. Members may review their own BWC Data for report writing, training purposes, preparation for court appearances, depositions, statements and investigations, if the BWC has the capability.

14.6.7.2. The Training Unit has the ability to review BWC Data for training purposes, provided approval has been given by the Administrative Lieutenant.

14.6.7.3. Supervisors may review Data for the following purposes:

14.6.7.3.1. Conducting administrative investigations.

14.6.7.3.2. Performance Review.

14.6.7.3.3. Review of a member's report, training purposes, preparation for court appearances and investigations, if the BWC has the capability.

14.6.7.3.4. Any other reason deemed necessary by the Chief of Police or designee.

14.6.8. Supervisory Responsibilities:

14.6.8.1. Supervisory personnel shall ensure that members equipped with BWCs utilize them in accordance with policy and procedures defined herein.

14.6.8.2. Supervisors shall monitor assigned members' use of the BWC for inappropriate usage, violations of policy and any possible reoccurrence. The supervisor will follow the Department's disciplinary procedures. (CFA: 32.02D)

14.6.8.2.1. All Supervisors will note their Supervisory review on the Data file each time they log in to review an assigned member's BWC Data.

14.6.8.3. Supervisors and Internal Affairs shall review BWC video involving Use of Force (Response to Resistance), Pursuit (Vehicle or Foot), Employee Traffic Accident, and Employee Injury.

14.6.8.4. At the scene of officer involved shootings, in-custody deaths, or serious bodily injury, and once the scene is deemed safe, supervisors will:

14.6.8.4.1. Make personal contact with the subject Officer

14.6.8.4.2. State on camera "I (rank/name/IBM.) will be deactivating this camera due to the scene being deemed safe."

14.6.8.4.3. Deactivate and power off the BWC.

14.6.8.4.4. Ensure the BWC remains in place on the Officer until Crime Scene arrives to remove it

14.6.8.4.5. The BWC Supervisor will respond to upload the video in the presence of a representative from the investigating unit.

14.6.8.5.. Members are permitted to review BWC Data, upon his or her own initiative or request, before writing a report or providing a statement regarding any event arising within the scope of his or her official duties. A member has an inherent duty to immediately disclose information necessary to secure an active crime scene or to identify suspects or witnesses regardless of whether or not the member has reviewed the BWC Data.

14.6.9. Equipment Inspection, Maintenance, Storage and Repair:

14.6.9.1. The member will perform a function check of the BWC at the beginning of each shift to ensure the BWC is operationally ready.

14.6.9.2. Damage, loss or theft must immediately be reported to the member's immediate supervisor. An incident report must be completed when a BWC is damaged, lost or stolen. The member's supervisor will ensure that the incident report is received by the BWC Coordinator via chain of command immediately.

14.6.9.3. Malfunctioning or damaged equipment will be sent by the member to the BWC Coordinator or designee for repair or replacement with the approval of the member's immediate supervisor. If it is determined that a malfunction caused an incident to not be recorded, a memorandum via chain of command will be submitted detailing the incident and subsequent cause of the malfunction. The member who possessed the BWC at the time of the malfunction will prepare this memorandum.

14.6.9.4. Members will remove the BWC from vehicles when not on duty.

14.6.10. Training (CFA: 32.02A):

14.6.10.1. All employees who are assigned BWCs must complete an agency approved training program. The training will be carried out by the Training Unit and/or the BWC Coordinator. The training program will include:

14.6.10.1.1. BWC operation to include powering on and off, activation and deactivation.

14.6.10.1.2. Proper placement of the BWC on the uniform.

14.6.10.1.3. Department policy and procedures and relevant state and federal laws on BWC usage.

14.6.10.1.4. Review of procedures for Data and files to be used as evidence.

14.6.10.1.5. Basic maintenance.

14.6.10.1.6. Scenario-based exercises that replicate situations that members might encounter in the field.

14.6.10.1.7. Procedures for downloading and tagging recorded Data.

14.6.10.1.8. Procedures for accessing and reviewing recorded Data (only for personnel authorized to access the Data).

14.6.10.1.9. Procedures for documenting and reporting any BWC or BWC equipment, to include maintenance and malfunctions.

14.6.10.2. All employees who use, maintain, store, or release Data recorded by BWC shall be trained in the Department's policy and procedures.

14.6.11. Annual Review:

14.6.11.1. The Internal Affairs Lieutenant or designee will conduct a documented annual administrative review of the Department's practices to ensure conformity with the Department's policies, procedures and Florida law regarding BWCs.

14.6.11.1.1. The review should also include, but not be limited to, security and access controls.

14.6.11.1.2. The review will be documented on a Department memorandum to the Chief of Police via chain of command.

14.6.12. BWC Supervisor:

14.6.12.1. The BWC Supervisor is responsible for the BWC systems' overall maintenance, management, and retention, and acts as the technology liaison to the Crime Scene Unit and associated vendors. The BWC Supervisor also has the following duties:

14.6.12.1.1. Ensuring that all users are trained in the use of the BWC system and equipment prior to being issued their equipment.

14.6.12.1.2. Configuration of the evidence storage system and assigning access roles under direction of the Chief of Police or designee.

14.6.12.1.2.1. BWC users have access only to their recordings

14.6.12.1.2.2. Detectives can access all videos for investigation purposes.

14.6.12.1.2.3. The BWC Supervisor has access to all recordings on the system.

14.6.12.1.2.4. PIO and the Public Records Coordinator have access to all files.

14.6.12.1.3. Managing BWC inventory, issuing devices, training and updating device settings.

14.6.12.1.4. Assisting with manual uploads to the external cloud server.

14.6.12.1.5. Managing recordings to include restricted/prohibited footage pursuant to direction from the Chief of Police. Notifying the Chief of Police when video evidence software logs indicate deleted, copied and/or edited recordings.

14.6.12.1.6. Managing the list of retention categories and notifying supervisors when users fail to categorize their BWC recordings or otherwise fail to properly use, store or maintain their issued BWC.

14.6.12.1.7. Performing an audit of the DEMS, to ensure users are in compliance with the BWC policy. This will include department members activating their BWCs on calls for service and uploading their digital evidence as required.

14.6.12.1.8. Providing support to department employees in all aspects of the BWC system.

14.6.12.1.9. Maintenance of an audit system that monitors and logs access to recorded data.

14.6.12.1.10. Ensuring that all evidence categories have the correct records retention settings..

14.6.12.1.11. Conducting forensic reviews when directed by the Chief of Police or designee to determine whether BWC equipment and/or recorded data have been tampered with.

14.6.12.1.12. Continuously monitoring this policy with a documented analysis to identify necessary modifications and/or continuations. The documented analysis shall be forwarded to the Chief of Police via the Chain of Command for the purposes of evaluating the effectiveness of using the BWCs.

14.6.12.1.13. Perform a periodic review of actual BWC practices, including but not limited to recorded media, to ensure conformity with the agency's policies and procedures, in accordance with § 943.1718, Florida Statutes.