

Body-Worn Cameras

440.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the use of a body-worn camera (BWC) by members of this department and for the access, use, and retention of department BWC media.

The provisions of this policy, including notice, documentation, access, and retention, also apply to other portable audio/video recording devices used by members, where applicable.

This policy does not apply to undercover operations, wiretaps, or eavesdropping (concealed listening devices).

440.1.1 DEFINITIONS

Definitions related to this policy include:

Activate - To place a BWC in active mode (also called event mode). In active mode, the BWC records both video and audio.

BWC media - The video, audio, and images captured by department BWCs and the associated metadata.

BWC media systems - Any software, including web-based programs and mobile applications, used by the Department to upload/download, store, view, transfer, and otherwise maintain BWC media.

Deactivate - To place a BWC in buffering mode (also called ready or pre-event mode). In buffering mode, the BWC records video (without audio) in short, predetermined intervals that are retained only temporarily. However, when a BWC is activated, the interval recorded immediately prior to activation is then stored as part of the BWC media. Deactivate does not mean powering off the BWC.

Event - A general term referring to a set of circumstances that may, but does not necessarily, correlate directly to a single public safety incident.

440.2 POLICY

It is the policy of the Department to use BWCs and BWC media for evidence collection and to accurately document events in a way that promotes member safety and department accountability and transparency while also protecting the privacy of members of the public.

440.3 RESPONSIBILITIES

440.3.1 BWC COORDINATOR RESPONSIBILITIES

The Chief of Police or the authorized designee should delegate certain responsibilities to a BWC coordinator.

The responsibilities of the coordinator include:

Vail Police Department

Vail PD Policy Manual

Body-Worn Cameras

- (a) Serving as a liaison between the Department and the BWC manufacturer/distributor and any third-party media storage vendor.
- (b) Acquiring sufficient BWCs to equip all members required to wear BWCs on-duty (CRS § 24-31-902).
- (c) Developing inventory procedures for issuing and tracking BWC equipment, including properly marking BWCs as property of the Department and recording the date each BWC is placed into or taken out of service.
- (d) Assisting with troubleshooting and maintenance of BWC equipment and media systems and, when necessary, coordinating the repair or replacement of BWCs.
 - 1. All equipment and system malfunctions and their resolutions should be documented, and maintenance and repair records should be maintained for all BWCs.
- (e) Managing BWC media systems so that:
 - 1. Access is limited to the minimum necessary authorized users and user privileges are restricted to those necessary for the member to conduct assigned department duties.
 - 2. Security requirements, such as two-factor authentication and appropriate password parameters, are in place for user credentials.
- (f) Configuring BWC media systems, or developing manual procedures, so that media is appropriately categorized and retained according to the event type tagged by members.
- (g) Retaining audit logs or records of all access, alteration, and deletion of BWC media and media systems, and conducting periodic audits to ensure compliance with applicable laws, regulations, and department policy.
- (h) Developing and updating BWC training for members who are assigned a BWC or given access to BWC media systems.
- (i) Coordinating with the community relations coordinator to (see the Community Relations Policy):
 - 1. Provide the public with notice of the department's use of BWCs (e.g., posting on the department website or social media pages).
 - 2. Gain insight into community expectations regarding BWC use.
- (j) Coordinating with the Records Manager to (see the Records Section and Records Maintenance and Release policies):
 - 1. Determine and apply proper retention periods to BWC media.
 - 2. Develop procedures for the appropriate release of BWC media.
- (k) Coordinating with the Property and Evidence Section to develop procedures for the transfer, storage, and backup of evidentiary BWC media (see the Property and Evidence Policy).

Vail Police Department

Vail PD Policy Manual

Body-Worn Cameras

440.3.2 MEMBER RESPONSIBILITIES

Every member issued a BWC is responsible for its proper use, safekeeping, and maintenance.

At the beginning of each shift or period of BWC use, the member should inspect their assigned BWC to confirm it is charged and in good working order. As part of the inspection, the member should perform a function test by activating the BWC and recording a brief video stating their name, identification number, assignment, and the date and time.

Members should wear their assigned BWC on their outermost garment positioned at or near chest level and as close to the center of their body as practicable. Members are responsible for ensuring there are no obstructions and that the BWC remains in a position suitable for recording.

When a BWC is not in the physical possession of the member to which it is assigned, it should be placed on the charging dock and stored in a secure location.

Members shall report any malfunction or damage to the BWC coordinator or on-duty supervisor as soon as practicable and, if possible, obtain a functioning BWC to use either temporarily while repairs are being made to the member's BWC or as a permanent replacement.

440.4 BWC USE

The following guidelines apply to the use of BWCs:

- (a) Only department-issued BWCs should be used. Members are prohibited from using any other BWC without the express consent of the Chief of Police or the authorized designee.
- (b) BWCs should only be used by the member or members to whom it was issued unless otherwise authorized by a supervisor.
- (c) The use of department-issued BWCs shall be strictly limited to department-related activities.
- (d) Members shall not use BWCs or BWC media systems for which they have not received prior authorization and appropriate training.
- (e) Members shall immediately report unauthorized access or use of BWCs or BWC media systems by another member to their supervisor or the Chief of Police.

440.4.1 PROHIBITIONS

BWCs should not be used to record:

- (a) Routine administrative activities of the Department that do not involve interactions with the public. Care should be taken to avoid incidentally recording confidential documents that the Department has a duty to keep secure (i.e., criminal justice information).
- (b) Areas within the department facilities where members have a reasonable expectation of privacy (e.g., locker rooms or dressing areas, breakrooms) unless responding to a call for service or conducting an investigation.
- (c) Conversations of other members without their knowledge.

Vail Police Department

Vail PD Policy Manual

Body-Worn Cameras

- (d) When a member is taking an authorized break or otherwise engaged in personal activities.
- (e) In a courtroom unless responding to a call for service or emergency situation.
- (f) Interactions with undercover officers or confidential informants.
- (g) Strip searches.

BWCs shall not be used for the purpose of embarrassment, harassment, or ridicule of any individual or group.

440.5 ACTIVATION OF BWC

Members shall activate their BWC during all calls for service and the performance of law enforcement-related functions (CRS § 24-31-902). Members are not required to activate their BWC during casual or informal contacts with members of the public that are not part of or related to law enforcement functions. However, members should activate their BWC any time a contact with an individual becomes hostile or adversarial.

Unless otherwise authorized by this policy or approved by a supervisor, BWCs should remain activated until the call for service or law enforcement-related function has concluded. A member may cease recording if they are simply waiting for a tow truck or a family member to arrive, or in other similar situations.

At no time is a member expected to jeopardize their safety to activate their BWC. However, the BWC should be activated as soon as reasonably practicable in required situations.

If a member attempts to activate their BWC but the BWC fails to record an event, the member should notify their supervisor as soon as practicable.

440.5.1 NOTICE OF RECORDING

Unless otherwise approved based on unique circumstances, a member should wear the BWC in a manner that is conspicuous and shall answer truthfully if asked whether they are equipped with a BWC or if their BWC is activated.

440.5.2 PRIVACY CONSIDERATIONS

Members should remain sensitive to the dignity of individuals being recorded and should exercise sound discretion with respect to privacy concerns.

When responding to a place where individuals have an expectation of privacy (e.g., private residences, medical or mental health facilities, restrooms) or to a sensitive situation (e.g., individuals partially or fully unclothed), members are permitted to mute or deactivate their BWC if it reasonably appears that the privacy concern outweighs any legitimate department interest in recording the event. Members may also mute or deactivate their BWC (CRS § 24-31-902):

- (a) To avoid recording personal information that is not related to the case.
- (b) When there is a long break in the incident.

Vail Police Department

Vail PD Policy Manual

Body-Worn Cameras

- (c) In administrative, tactical, and management discussions when civilians are not present.

Members should choose to mute rather than deactivate BWCs when practicable. Deactivation should only be used when muting the BWC will not accomplish the level of privacy necessary for the situation.

Before muting or deactivating their BWC, the member should verbally narrate the reason on the recording. As soon as possible once the privacy concern is no longer an issue, or when circumstances change so that the privacy concern no longer outweighs the department's interest in recording the event (e.g., the individual becomes combative, the conversation ends), the member should unmute or reactivate their BWC and verbally note that recording has resumed.

440.5.3 LIVESTREAMING

Livestreaming enables authorized individuals to remotely view the audio and video captured by a member's BWC in real time. Only supervisors and dispatchers approved by the Chief of Police or the authorized designee shall have access to livestreaming capabilities.

Livestreaming should only be activated:

- (a) For purposes of member safety when the member is not responding to their radio or there is some other indication of distress.
- (b) To assist with situational awareness or tactical decisions during a significant incident.
- (c) When requested by the member.

440.5.4 DOCUMENTATION

Members are encouraged to provide narration while using a BWC when it would be useful to provide context or clarification of the events being recorded. However, the use of a BWC is not a replacement for written reports and should not be referred to in a written report in place of detailing the event.

Every report prepared by a member who is issued a BWC should state "BWC available" or "BWC unavailable," as applicable, and should document:

- (a) To the extent practicable and relevant, the identity of individuals appearing in the BWC media.
- (b) An explanation of why BWC media is unavailable including any malfunction, damage, or battery issue that resulted in the failure of the BWC to capture all or part of the event.
- (c) Any exigency or other circumstances that prevented the member from immediately activating the recording at the beginning of the event.
- (d) Any period of the event in which the member deactivated or muted their BWC and the reason for such action.
- (e) If livestreaming was activated during the event, the reason for livestreaming and the members who communicated or participated in the event through BWC livestreaming.

Body-Worn Cameras

440.6 UPLOADING BWC MEDIA

Unless otherwise authorized by a supervisor, all media from a member's BWC should be properly uploaded and tagged before the end of their shift. BWC media related to a serious or high-profile event (e.g., search for a missing child, active shooter situation) should be uploaded and tagged as soon as practicable upon returning to the Department.

Following an officer involved shooting or death or other event deemed necessary, a supervisor should take possession of the BWC for each member present and upload and tag the BWC media.

440.6.1 TAGGING BWC MEDIA

Members should tag all media captured by their BWC with their name and/or identification number, the case or incident number, and the event type. BWC media should be tagged upon uploading or, if capabilities permit tagging in the field, as close to the time of the event as possible. If more than one event type applies to BWC media, it should be tagged with each event type. If BWC media can only be tagged with a single event type, the media should be tagged using the event type with the longest retention period.

BWC media depicting sensitive circumstances or events should be tagged as restricted. BWC media should be flagged for supervisor review when it pertains to a significant event such as:

- (a) An incident that is the basis of a formal or informal complaint or is likely to result in a complaint.
- (b) When a member has sustained a serious injury or a line-of-duty death has occurred.
- (c) When a firearm discharge or use of force incident has occurred.
- (d) An event that has attracted or is likely to attract significant media attention.

Supervisors should conduct audits at regular intervals to confirm BWC media is being properly uploaded and tagged by their subordinates.

440.7 BWC MEDIA

All BWC media is the sole property of the Department. Members shall have no expectation of privacy or ownership interest in the content of BWC media.

All BWC media shall be stored and transferred in a manner that is physically and digitally secure with appropriate safeguards to prevent unauthorized modification, use, release, or transfer. Contracts with any third-party vendors for the storage of BWC media should include provisions specifying that all BWC media remains the property of the Department and shall not be used by the vendor for any purpose without explicit approval of the Chief of Police or the authorized designee.

Members shall not alter, copy, delete, release, or permit access to BWC media other than as permitted in this policy without the express consent of the Chief of Police or the authorized designee.

BWC media systems should not be accessed using personal devices unless authorized by the Chief of Police or the authorized designee.

Vail Police Department

Vail PD Policy Manual

Body-Worn Cameras

440.7.1 ACCESS AND USE OF BWC MEDIA

BWC media systems shall only be accessed by authorized members using the member's own login credentials and in accordance with the Information Technology Use Policy.

BWC media shall only be accessed and viewed for legitimate department-related purposes in accordance with the following guidelines:

- (a) BWC media tagged as restricted should only be accessible by those designated by the Chief of Police or the authorized designee.
- (b) Members may review their own BWC media for department-related purposes. Members should document in their report if they reviewed BWC media before completing the report.
- (c) Investigators may review BWC media pertaining to their assigned cases.
- (d) A member testifying regarding a department-related event may review the pertinent BWC media before testifying.
- (e) Supervisors are permitted to access and view BWC media of their subordinates.
 - 1. Supervisors should review BWC media that is tagged as a significant event or that the supervisor is aware pertains to a significant event.
 - 2. Supervisors should conduct documented reviews of their subordinate's BWC media at least annually to evaluate the member's performance, verify compliance with department procedures, and determine the need for additional training. The review should include a variety of event types when possible. Supervisors should review BWC media with the recording member when it would be beneficial to provide guidance or to conduct one-on-one informal training for the member.
 - 3. Supervisors should conduct periodic reviews of a sample of each subordinate's BWC media to evaluate BWC use and ensure compliance with this policy.
- (f) The Investigations Commander is permitted to access and view BWC media for training purposes.
 - 1. The Investigations Commander should conduct a quarterly review of a random sampling of BWC media to evaluate department performance and effectiveness and to identify specific areas where additional training or changes to protocols would be beneficial. Training Committee members may review BWC media as part of their review to identify training needs.
 - 2. The Investigations Commander may use BWC media for training purposes with the approval of the Chief of Police or the authorized designee. The Investigations Commander should use caution to avoid embarrassing or singling out a member and, to the extent practicable, should seek consent from the members appearing in the BWC media before its use for training. When practicable, sensitive issues depicted in BWC media should be redacted before being used for training.
- (g) The Records Manager may access BWC media when necessary to conduct department-related duties.

Vail Police Department

Vail PD Policy Manual

Body-Worn Cameras

- (h) The BWC coordinator may access BWC media and the BWC media system as needed to ensure the system is functioning properly, provide troubleshooting assistance, conduct audits, and fulfill other responsibilities related to their role.

440.7.2 PUBLIC ACCESS

Unless disclosure is required by law or a court order, BWC media should not be released to the public if it unreasonably violates a person's privacy or sense of dignity or depicts the interior of:

- (a) A private residence.
- (b) A facility that offers health care, mental health or substance abuse treatment, or social services.
- (c) A school building.
- (d) Any other building in which public access is restricted or which implicates heightened security concerns.

Requests for the release of BWC media shall be processed in accordance with the Records Maintenance and Release Policy and the Enhance Law Enforcement Integrity Act (CRS § 24-31-902). The Records Manager should review BWC media before public release.

440.8 RETENTION OF BWC MEDIA

Non-evidentiary BWC media should be retained in accordance with state records retention laws.

Unless circumstances justify continued retention, BWC media should be permanently deleted upon the expiration of the retention period in a way that it cannot be retrieved. BWC media shall not otherwise be deleted by any person without the authorization of the Chief of Police or the authorized designee.

440.8.1 EVIDENTIARY BWC MEDIA

BWC media relevant to a criminal prosecution should be exported from the BWC media system and securely transferred to digital evidence storage according to established department procedures. Evidentiary BWC media is subject to the same laws, policies, and procedures as all other evidence, including chain of custody, accessibility, and retention periods (see the Property and Evidence Policy).

440.9 TRAINING

The BWC coordinator should ensure that each member issued a BWC receives initial training before use, and periodic refresher training thereafter. Training should include:

- (a) Proper use of the BWC device and accessories.
- (b) When BWC activation is required, permitted, and prohibited.
- (c) How to respond to an individual's request to stop recording.
- (d) Proper use of the BWC media systems, including uploading and tagging procedures.
- (e) Security procedures for BWC media, including appropriate access and use.

Vail Police Department

Vail PD Policy Manual

Body-Worn Cameras

Members who are not issued a BWC but who have access to BWC media systems shall receive training on the BWC media system, including appropriate access, use, and security procedures.