Body Worn Camera Policy

Policy Number: 50	**Dated**: April 8, 2024	**Distribution**: All Employees
Replaces: October 20, 2022	**References**: Minn. Stat. §§ 13.43; 13.82; 13.825; 609; 626.8473	

I. Policy Statement

In the use of body worn camera equipment, Alcohol and Gambling Enforcement seeks to enhance accountability and public trust, maintain the safety of our special agents, and collect evidence by preserving a record of interactions with citizens to assist special agents by providing a record independent from their individual perceptions and recollections, and serve as a training tool for best practices in the division.

The purpose of this policy is to provide authorization and guidance for the use and management of body worn camera equipment and provide parameters for administration of body worn camera data as provided by law.

II. Definitions

A. **Activation**: an action that causes the BWC to record audio or video data. Can only occur when the BWC is already powered on.

B. **Adversarial**: an incident in which an individual becomes confrontational, expresses anger, resentment, or hostility toward another, or argues, threatens, yells, shouts. Also includes anytime an individual demands to be recorded.

C. **Body Worn Camera (BWC)**: portable audio-video recording equipment designed to be worn on a person.

D. **Critical Incident**: for purposes of this policy, an incident occurring in the line of duty involving the use of deadly force by or against an employee, death or great bodily harm incurred by an employee, death or great bodily harm incurred by a person under the custody or control of an employee, or an action by an employee that causes or is intended to cause death or great bodily harm.

E. **Data Subject**: for purposes of BWC data, any individual or entity whose image or voice is documented in the data including the special agent who collected the data and any other peace officer regardless of whether that officer is or can be identified. *Minn. Stat. § 13.825, subd. 4(a).*

F. **Deadly Force**: force used with the purpose to cause, or should reasonably know creates, a substantial risk of causing death or great bodily harm. The intentional discharge of a firearm, other than a firearm loaded with less lethal munitions and used by a peace officer within the scope of official duties, in the direction of another person or at a vehicle in which another person is believed to be, constitutes deadly force. *Minn. Stat. § 609.066, subd. 1.*

G. **Director**: the director of the division. At any time, the director may designate another person to satisfy responsibilities or requirements under this policy.

H. **Division**: Alcohol and Gambling Enforcement (AGE) division of the Department of Public Safety.

I. **Employee**: all division staff including full-time, part-time, temporary, intermittent, seasonal, or emergency workers, interns and student workers.

J. **Evidentiary Value**: information which may be useful in an ongoing investigation; as proof in a criminal, civil or administrative proceeding; or in considering an allegation against a law enforcement agency or employee; including a stop, arrest, and search.

K. **General Citizen Contact**: an informal encounter with a citizen that is not likely to become adversarial or yield information relevant to an ongoing investigation. Examples include, but are not limited to, assisting a motorist with directions or discussing general crime trends with a citizen.

L. **Great Bodily Harm**: bodily injury which creates a high probability of death, causes serious permanent disfigurement, or a permanent or protracted loss or impairment of the function of any bodily member or organ or other serious bodily harm. *Minn. Stat. § 609.02, subd. 8.*

M. **Powered On**: requires setting the BWC "On/Off" switch to "On," enabling power to the BWC. This must occur prior to and is distinct from activation.

N. **Special Agent (SA)**: a sworn peace officer employed by the division.

III. Use Guidelines

A. Wearing BWCs

1. SAs working in the field during non-covert/non-undercover assignments shall wear a BWC and keep it powered on at all times it can be reasonably anticipated they may become involved in a situation for which activation is appropriate in accordance with this policy.
2. SAs do not need to wear a BWC during plainclothes covert or undercover assignments in which it has been determined the BWC would compromise the operation.
3. SAs shall wear their BWC forward facing, at or above the mid-line of the waist in a position that maximizes the BWC's capacity to record video footage of the SA's activities. *Minn. Stat. § 626.8473, subd. 3(b)(2).*

B. Activating BWCs *Minn. Stat. § 626.8473, subd. 3(b)(8)*

1. SAs shall activate their BWC at any time they interact with the public while conducting an investigatory or enforcement action related to a potential criminal or regulatory offense.
2. SAs shall also active their BWC at any other time directed to by a division supervisor.
3. Exceptions
    a. SAs need not activate their BWC when it would be unsafe, impossible, or impractical to do so, but such instances of not recording when otherwise required must be documented in a written report.
    b. BWCs need not be activated when executing a search warrant in a controlled facility or environment (for example, at a financial institution).
    c. SAs have the discretion to not activate their BWC when doing so would serve only to record symptoms or behaviors believed to be attributable to an apparent mental health crisis or to record persons being provided medical care unless there is reason to believe the recording would document an instance of enforcement action or adversarial contact.
4. Once activated, the BWC should continue recording until the conclusion of the incident or encounter, or until it becomes apparent that additional recording is unlikely to capture information having evidentiary value. If a SA purposefully deactivates their BWC while an incident is ongoing, the SA shall state the reason before deactivation. *Minn. Stat. § 626.8473, subd. 3(b)(10).*
5. If a BWC is not activated prior to an incident in which activation is required or if the situation changes to require activation, the BWC shall be activated as soon as it is safe and reasonably feasible to do so.
6. At their discretion, SAs may use a BWC to take recorded statements related to an investigation in lieu of an audio recorder.

C. Restrictions.

1. SAs shall not intentionally block the BWC's audio or visual recording functionality to defeat the purpose of this policy. This does not include, however, situations in which the momentary blocking of such functionalities would be appropriate and preferred in contrast to deactivating and reactivating the BWC. For example, to avoid capturing irrelevant images of an undressed bystander within a private home, images of a screen displaying private or confidential data, or audio of SAs conferring about a tactical situation.
2. SAs shall not use their BWCs to record other employees during non-enforcement related activities, such as during meal breaks or while engaging in private conversations, unless recording is otherwise authorized under this policy.

IV. Roles and Responsibilities

A. Division Responsibilities

1. The division is responsible for the review and revision of this policy as necessary and facilitating the biennial audit required under Minn. Stat. § 13.825, subd. 9. *Minn. Stat. § 13.825, subd. 5(3).*
2. The division shall provide training to all employees on this policy, including the appropriate use and operation of BWCs and the BWC data storage platform, prior to being assigned or operating a BWC and prior to accessing the BWC data storage platform.
3. The division is responsible for maintaining the following records and documents relating to BWC use, which are classified as public data. *Minn. Stat. § 13.825, subd. 5*.
   a. The total number of BWCs owned and maintained by the division.
   b. A daily record of the total number of BWCs actually deployed and used by SAs.
   c. The total amount of recorded BWC data collected and maintained by the division, the division's retention schedule for the data, and the division's procedures for destruction of data.
4. Notice to Data Subjects
   a. Upon notification of an action commenced under Minn. Stat. § 13.825, subd. 2(g), the division shall forward notice of the action to any known data subjects related to the action if notice has not already been provided.
   b. Upon written request by a data subject to retain BWC data beyond the applicable retention period, up to an additional 180 days from the request, the division shall notify the requestor that the data will be destroyed at the end of the extension or when the applicable retention period has passed, whichever is later, unless a new written request is received.
5. If the division acquires new BWC technology that expands the type or scope of surveillance capability beyond video or audio recording, the division shall notify the BCA within ten (10) days. *Minn. Stat. § 13.825, subd. 10*.

B. SA Responsibilities

1. SAs may only use a BWC issued and maintained by the division and shall wear and operate it consistent with this policy and only in the performance of official duties for the division or while performing law enforcement activities under the command and control of another chief law enforcement officer or federal law enforcement official. *Minn. Stat. §§ 13.825, subd. 6; 626.8473, subd. 3(b)(3)*.
2. SAs shall not permit any person not employed by the division to use or wear their BWC without approval by a division supervisor.
3. SAs are required to report any misconduct or violation of this policy to their supervisor as soon as practical.
4. SAs have no affirmative duty to inform the public that a BWC is being operated or that an individual is being recorded. If asked, the SA should inform those inquiring that a BWC is in use, unless doing so would be unsafe for the SA or members of the public.
5. A SA who fails to activate a BWC, including when a BWC is not operational or is otherwise unavailable, or fails to record for the entire duration of an assignment as required by this policy shall make a written report documenting the reasons for the failure or delay. *Minn. Stat. § 626.8473, subd. 3(b)(7)*.
6. BWC Maintenance and Malfunctions
   a. SAs are responsible for ensuring their BWC is in good working order at all times.
   b. At least monthly, SA shall ensure the firmware on their BWC is up to date.
   c. SAs shall ensure their BWC is fully charged at the start of each shift.
   d. At the beginning of each shift in which the SA will be wearing a BWC in accordance with this policy, the SA shall ensure the BWC is functioning properly by powering on the BWC, confirming it syncs with the app on the SA's phone and live viewing the BWC through the app. *Minn. Stat. § 626.8473, subd. 3(b)(6)*.

e. In the event a BWC is missing, damaged or malfunctioning, including a loss of battery power, the SA shall immediately notify their supervisor. The SA shall also notify the Assistant Special Agent in Charge (ASAIC) overseeing the BWC program by email, copying the Special Agent in Charge (SAIC), as soon as practical.

f. In the event a SA is required to wear their BWC under this policy but it is not operational or is otherwise unavailable, the SA shall confer with their supervisor to determine any possible remedies and if the SA shall continue with the assignment without a BWC. If it is determined that the SA shall continue with the assignment without a BWC, the SA shall document in writing the reason for the missing BWC data. *Minn. Stat. § 626.8473, subd. 3(b)(7)*.

7. Transferring BWC Data

a. SAs are responsible for ensuring the timely transfer of BWC data to the BWC data storage platform. In the case a SA is involved in a critical incident, however, another employee may take custody of the involved SA's BWC and assume responsibility for transferring the data. *Minn. Stat. § 626.8473, subd. 3(b)(11)*.

b. SAs shall ensure the following information associated with all data transferred from their BWC to the BWC data storage platform is accurate.

i. The ID. SAs shall label the data with the AGE case number as the ID. In the event the data is not related to a case, such as data related to training, testing, or created accidentally, the data shall be assigned the ID AGE999.

ii. The category. SAs shall assign at least one of the following categories to all BWC data so as to allocate the proper retention to the data in accordance with the division Records Retention Schedule. SAs are responsible for updating the category if circumstances change.

A. Critical Incident: data documenting a critical incident event as defined by this policy (permanent retention).

B. Pursuit or Use of Force: data documenting a pursuit or use of force that does not meet the level of a critical incident (seven year retention).

C. Case Evidence: data with evidentiary value with respect to an investigation, when an employee seizes property from an individual or directs an individual to dispose of property, or the incident involved an adversarial encounter or resulted in a complaint against an employee (seven year retention).

D. Miscellaneous, Training, Other: the data does not contain any of the foregoing categories of information and has no apparent evidentiary value such as recordings of general citizen contacts and unintentionally recorded footage (ninety day retention).

iii. Tags Limiting Disclosure. If known, SAs shall add the following tags relevant to the BWC data to identify that the data's disclosure may be limited. Data containing such tags will be reviewed before disclosure to determine if the data may be released.

A. Victim/Witness: the data discloses a victim or witness that has requested not to be identified publicly.

B. Informant: the data reveals the identity of a paid or unpaid informant.

C. Offensive: the data contains images or audio that are clearly offensive to common sensibilities.

D. Mandated Reporter: the data identifies a mandated reporter, including an insurer or insurance professional who disclosed possible insurance fraud and a public employee or public officer who reported the unlawful use or misuse of public property or funds.

E. Juvenile: the data includes the identity of a juvenile witness or a juvenile who is or may be delinquent or engaged in a criminal act.

F. Other: any other situation in which the data may be legally protected from public disclosure.

C. Supervisor Responsibilities

1. Supervisors are responsible for ensuring that all employees are in compliance with this policy.
2. On a monthly basis, supervisors shall complete a random review of BWC usage by each SA in which a BWC has been issued or is available for use to ensure compliance and identify any performance areas in which additional training or guidance may be necessary. *Minn. Stat. § 626.8473, subd. 3(b)(12)*.
3. When notified of a BWC malfunction, the supervisor shall ensure all appropriate follow-up measures are taken including, but not limited to, replacing the BWC if possible and confirming the SA notified the SAIC and ASAIC overseeing the BWC program of the malfunction.
    a. Further, if the SA has an assignment in which a BWC would otherwise be required to be worn under this policy, the supervisor shall determine if the SA should continue with the assignment without a BWC and ensure any required documentation is completed.
4. In the event of a critical incident, the supervisor on duty shall ensure that that BWC of each involved SA is obtained by another employee and the data is transferred to the BWC data storage platform.

V. Data Security, Retention, Classification and Access

A. All BWC data is the property of the division. The original data shall remain intact and stored in the BWC data storage platform.

B. Data Security

1. Employees are required to transfer BWC data to the BWC data storage platform as specified in this policy. The transfer of data is encrypted end-to-end and the BWC data storage platform is FBI CJIS approved cloud storage. *Minn. Stat. §§ 13.825, subd. 11(b); 626.8473, subd. 3(b)(11)*.
2. Personally owned devices, including but not limited to computers and mobile devices, shall not be used to access or view division BWC data.
3. Altering, editing, or erasing any BWC recording or its related data or metadata prior to the expiration of the applicable retention period is prohibited unless otherwise authorized by the director in writing, except as necessary to ID and categorize the data as required by this policy. *Minn. Stat. § 626.8473, subd. 3(b)(1)*.

C. Data Retention

1. BWC data will always be retained in accordance with applicable law, this policy, and the division's Records Retention Schedule. Data may be retained past the scheduled retention period as needed.
2. In accordance with the division's Records Retention Schedule, the following categories of BWC data will be retained as indicated.
    a. Data that documents a critical incident as defined by this policy shall be retained indefinitely, including the full, unedited and unredacted recording of a peace officer using deadly force. *Minn. Stat. §§ 13.825, subd. 3(c); 626.8473, subd. 3(b)(1)*.
    b. Data documenting a pursuit or use of force that does not meet the level of a critical incident, when an employee seizes property from an individual or directs an individual to dispose of property, an adversarial encounter, data with evidentiary value with respect to an investigation and data relating to circumstances that have given rise to a formal complaint against an employee shall be retained for seven years.
    c. All other BWC data that is non-evidentiary, including data taken during training or erroneously recorded, shall be retained for ninety (90) days.
3. When data is subject to multiple categories and retention periods, it shall be maintained for the longest applicable period.
4. Upon written request by a BWC data subject, the division shall retain the data beyond the applicable retention period, up to an additional 180 days from the request. When such a request is received, the division shall notify the requestor that the data will be destroyed at the end of the extension or when the applicable retention period has passed, whichever is later, unless a new written request is received. *Minn. Stat. § 13.825, subd. 3(d)*.

D. BWC Data Classification

1. The public, non-public, or confidential classification of BWC data will be determined in accordance with applicable law, including the Minnesota Government Data Practices Act.
2. BWC data is presumptively private data on individuals or nonpublic data, subject to the following.
    a. In an instance in which an individual dies as a result of a use of force by a peace officer, the division shall allow the deceased individual's next of kin, the legal representative of the deceased individual's next of kin, and the other parent of the deceased individual's child to inspect all BWC data of the division's involved SAs documenting the incident, redacted no more than what is required by law, within five days of receiving such a request. However, the division may deny the request if the division determines that there is a compelling reason that inspection would interfere with an active investigation and the director provides a prompt, written denial to the individual who requested the data, including a short description of the compelling reason access is denied and that relief may be sought from the district court pursuant to Minn. Stat. § 13.82, subd. 7. *Minn. Stat. §§ 13.825, subd. 2(b) – (c); 626.8473, subd. 3(b)(4)*.
    b. In any instance in which an individual dies as a result of a use of force by a peace officer, the division shall release all BWC data documenting the incident, redacted no more than what is required by law, no later than 14 days after the incident, unless the director asserts in writing that the public classification would interfere with an ongoing investigation, in which case the data remains classified by Minn. Stat. § 13.82, subd. 7. *Minn. Stat. § 13.825, subd. 2(d); 626.8473, subd. 3(b)(5)*.
    c. Except as provided above, BWC data that is collected or created as part of an investigation is confidential or protected nonpublic data while the investigation is active. *Minn. Stat. §§ 13.825, subd. 2(a)(3); 13.82, subd. 7*.
    d. BWC data not collected or created as part of an investigation or that is collected or created as part of an investigation but that investigation is inactive, is subject to the following. *Minn. Stat. § 13.825, subd. 2(a)(3)*.
        i. Data that records, describes, or otherwise documents actions or circumstances surrounding the discharge of a firearm by a peace officer in the course of duty and notice is required under Minn. Stat. § 626.553, subd. 2, or the use of force by a peace officer that results in substantial bodily harm as defined in Minn. Stat. § 609.02, subd. 7a, is public data. *Minn. Stat. § 13.825, subd. 2(a)(1)*.
        ii. Data that a data subject requests to be made accessible to the public is public, subject to the redaction of any data subject who is not a peace officer and who does not consent to the release, and data on a peace officer whose identity is protected under Minn. Stat. § 13.82, subd. 17(a). *Minn. Stat. § 13.825, subd. 2(a)(2)*.
        iii. BWC data that is public personnel data under Minn. Stat. § 13.43, subd. 2(a)(5) is public data. *Minn. Stat. § 13.825, subd. 2(a)(4)*.
3. Portions of public BWC data may be redacted or withheld if those portions of data are clearly offensive to common sensibilities. *Minn. Stat. § 13.825, subd. 2(e)*.

E. Division Access and Use of BWC Data

1. Under no circumstances shall an employee sell, transfer, share access or distribute copies of BWC data without written permission from the director, except as authorized under this policy or other applicable law. *Minn. Stat. § 13.825, subd. 7(c)*.
2. Audit trails are created by the BWC storage platform that automatically document all access to and activities within the storage platform. This documentation will be retained in conjunction with the associated BWC data that was accessed and will be destroyed subject to the applicable retention for the associated BWC data.
3. BWC data may be accessed by employees only for legitimate, specified law enforcement or data administration purposes and must be in the course and scope of the employee's job duties, including, but not limited to, the following.
    a. Except as may be provided by the division's critical incident policy, data from an incident may be reviewed prior to preparing a report, giving a statement, or providing testimony about the incident.

b. Employees may access BWC data to review, investigate, or aid in defending against an incident that has given rise to a complaint or concern about misconduct or performance.

c. Supervisors may review BWC data as necessary for their regular review of SA's data as required under this policy, use of force reviews, or other administrative reviews.

d. Portions of BWC video may be displayed to a witness if necessary to aid in an investigation, as allowed by Minn. Stat. § 13.82, subd. 15. The display should be limited to protect against disclosure of individual identities that are not public by showing only a portion of the video, showing only screen shots, muting the audio, or playing the audio but not displaying video.

e. BWC data may be accessed to complete required necessary and lawful redaction or editing of BWC data.

4. Training

a. All requests to retain or use BWC data for training purposes must be approved by the director and will be considered on a case-by-case basis. Data approved for training may be identified with a "training" tag.

b. BWC data from an assignment involving a SA in a probationary period may be reviewed with that SA for the purpose of providing coaching and feedback on the SA's performance.

F. Sharing BWC Data with Other Government Entities

1. BWC data shall be made available to prosecutors, courts, and other criminal justice entities as provided by law.

2. The division may share BWC data with other law enforcement agencies when the request is received in writing and articulates a necessary, legitimate law enforcement purpose for the requested data. The division's data practices contact shall be the director's designee for determining authorization to not public data by law enforcement personnel as required by Minn. Stat. § 13.825, subd. 7(b). *Minn. Stat. § 13.825, subd. 8*.

3. Requests for BWC data from government agencies not provided for above will be reviewed as received and facilitated as allowed by applicable law.

G. Members of the media or public may request a copy of or access to BWC data from the division's data practices contact, who shall process the request in accordance with applicable law.

VI. Sanctions for Misuse of BWC Equipment and Data

Employees failing to adhere to this policy or applicable laws regarding BWCs and its data, including but not limited to restrictions regarding accessing such data, may be subject to disciplinary action, up to and including termination, as well as criminal penalties pursuant to Minn. Stat. § 13.09. *Minn. Stat. §§ 13.825, subd. 12; 626.8473, subd. 3(b)(12)*.

APPROVED BY DIRECTOR	
Signed: Carla Cincotta	Date: 04/08/2024