Body Worn Camera Recorders

448.1 PURPOSE AND SCOPE

This policy provides guidelines for the use, management, access, storage, retrieval and retention of audio-visual media recorded by Body Worn Camera(s) (“BWC”) systems as prescribed by law. Compliance with these guidelines is mandatory, but it is recognized that deputies must also attend to other primary duties and the safety of all concerned, sometimes in circumstances that are tense, uncertain and rapidly evolving. This policy applies to all Dakota County Sheriff’s Office (DCSO) personnel. This policy governs the use of BWC in the course of official duties. It does not apply to the use of squad-based (dash camera) recording systems, see Mobile Video Recorder System, Dakota County Sheriff’s Office Policy 444, or the use of BWC in the Dakota County Jail by correctional staff, see Body Worn Mobile Video Recorder System in Dakota County Sheriff’s Custody Manual, Policy 530. The Sheriff or Sheriff’s designee may supersede this policy to individual deputies by providing specific instructions or standard operating procedures for BWC use in official duties other than patrol.

This policy does not apply to audio/video recordings of interviews or interrogations conducted at any DCSO facilities, jail, undercover operations, wiretaps or eavesdropping (concealed listening devices) unless captured by a BWC device. -

448.1.1 DEFINITIONS

Definitions related to this policy:

Body Worn Camera - a device worn by a licensed deputy that is capable of both video and audio recording of the deputy’s activities and interactions with others or collecting digital multimedia evidence as part of an investigation. This does not include a DCSO-issued phone.

Body Worn Camera (“BWC”) Administrator – the administrator designated by the Sheriff to carry out the duties contained in this policy and the statutory responsibilities governing BWC.

County – the County of Dakota.

Deputy – a licensed peace officer employed by the DCSO.

Official duties – for purposes of this policy, official duties means that the deputy is on duty and performing authorized law enforcement services on behalf of the DCSO.

448.2 POLICY

The DCSO may provide deputies with access to BWC for use during the performance of their official duties. The use of BWC is intended to enhance the mission of the DCSO by accurately capturing contacts between DCSO deputies and the public. Deputy safety is the primary consideration for the use and activation of the BWC.
448.2.1 BWC OBJECTIVES

The DCSO has adopted the use of BWC to accomplish the following objectives:

(a) To enhance deputy safety;
(b) To document statements and events during the course of an incident, in addition to using an audio recorder;
(c) To enhance the deputy’s ability to document and review statements and actions for both internal reporting requirements and for courtroom preparation and presentation;
(d) To preserve visual and audio information for use in current and future investigations;
(e) To provide a tool for self-critique and field evaluation during deputy training and to assist with on-going training and evaluation;
(f) To enhance the public trust by preserving factual representations of deputy-citizen interactions in the form of recorded media; and
(g) To assist with the defense of civil actions against deputies and the County.

448.3 BWC ADMINISTRATOR RESPONSIBILITIES

The BWC Administrator, or designee, is responsible for:

(a) Ordering, issuing, retrieving, and storing all BWC;
(b) Deleting BWC data when required pursuant to a court order or in accordance with the DCSO records retentions schedule or applicable laws;
(c) Keeping logs reflecting BWC assignments, including each BWC’s serial number, dates used, deputies assigned, and history of malfunction or system failure;
(d) Working with the assigned data practices liaison to coordinate the use, access, and release of information to ensure that procedures comply with requirements of the Minnesota Government Data Practices Act (MGDPA) (Minn. Stat. Ch.13), this policy, County policies and procedures, and other applicable data retention and privacy laws (see, Records Maintenance and Release Policy 809 and Protected Information Policy 811);
(e) Maintaining an inventory including:
   (1) Total number of BWC devices owned or maintained by the DCSO;
   (2) Daily record of the total number of BWC deployed and used by deputies and, if applicable, the locale in which the BWC were used;
   (3) Total amount of recorded audio and video data collected by the BWC and maintained by the DCSO; and
   (4) The procedures for destruction of the data;
(f) Notifying the Minnesota Bureau of Criminal Apprehension (BCA) within ten days when the DCSO obtains new equipment that expands the type or scope of surveillance capabilities (beyond video or audio recording) of the DCSO’s BWC system, along with a description of the technology and its surveillance capability and intended uses; and
(g) Implementing secure storage and backup of the BWC data.

448.4 SUPERVISOR RESPONSIBILITIES

Supervisors are responsible for:

(a) Ensuring that deputies are properly trained and supervised in the use of BWC per this policy, written procedures and governing law;
(b) Determining the corrective action when a deputy reports a malfunctioning BWC or system failure;
(c) Reporting the malfunction or system failure to the BWC Administrator;
(d) Authorizing deactivation of the BWC in situations covered under Section 448.9(e);
(e) Ensuring that BWC recorded media is properly uploaded when an incident arises that requires the immediate retrieval of the BWC’s recorded media (e.g., serious crime scenes, peace officer-involved shootings, department-involved collisions) and prompt notification of the upload to the BWC Administrator; and
(f) Randomly reviewing and documenting BWC usage and access at least once per month to ensure compliance with this policy and to identify any performance areas in which additional training or guidance is required.

448.5 DEPUTY RESPONSIBILITIES

Deputies issued BWC are responsible for knowing and complying with this policy and any governing written procedures and training including, but not limited to:

(a) Use of BWC only in the performance of official duties for the DCSO or when otherwise performing authorized law enforcement services as an employee of the DCSO and authorized by this policy;
(b) Performing a function test of the BWC prior to going into service to ensure it is operating properly;
(c) Reporting of any BWC malfunctioning or system failure to the supervisor and obtaining a functioning BWC as soon as reasonably possible;
(d) Recording his/her name, badge number, and the current date and time at the beginning and end of a shift, regardless of whether any activity is recorded (this is required if the system does not automate this function);
(e) Placement of the BWC at the location on the body as specified in training;
(f) Proper activation, deactivation, termination, cessation and pausing of the BWC;
(g) Documenting the reason for deactivating the BWC in a written report or other official record, including any instance where the BWC malfunctioned or the deputy deactivated the BWC before the end of the encounter;
(h) Documenting the existence of a recording in a written report or other official record of the contact; and
(i) When using a spare BWC, or one that is not assigned to the deputy, notifying the BWC Administrator of the reason the deputy is unable to use his/her issued BWC to ensure that the evidence that was recorded on the spare device can be reassigned to the deputy in the recording database.

448.6 GENERAL GUIDELINES

(a) All recordings made by deputies on the BWC at any time are the property of the DCSO.
(b) Deputies have no expectation of privacy or ownership interest in the content of the BWC recordings.
(c) Deputies have no affirmative duty to inform people that a BWC is being operated or that they are being recorded. However, if the BWC is activated, deputies have an affirmative duty to acknowledge that it is activated if asked, and in the event of this disclosure, the encounter must continue to be recorded until the encounter has concluded. During the encounter, the deputy may deactivate the BWC under those circumstances outlined in section 448.9. Deputies may not inform people that the BWC is activated, if it is not.
(d) At no time is a deputy expected to jeopardize his/her safety or the safety of others in
order to activate a BWC. However, the BWC should be activated in accordance with this policy as soon as reasonably practicable.

448.7 PROHIBITED USE

DCSO personnel are prohibited from:

(a) Programming personally owned devices, including but not limited to computers and mobile devices, to access or view BWC data;

(b) Using personally owned devices for audio or video recording purposes while on-duty without the express consent of a supervisor. Any deputy who uses a personally owned recorder for DCSO-related activities, after express permission from a supervisor, must comply with the provisions of this policy, including retention and release requirements;

(c) Using the BWC and recording media for personal use;

(d) Making personal copies of recordings created while on-duty or while acting in their official capacity;

(e) Using their BWC to record other DCSO personnel during non-enforcement related activities, such as during pre-and-post-shift time in locker rooms, during meal breaks, or during other private conversations, unless such recording is authorized as part of an administrative or criminal investigation;

(f) Accessing, duplicating, or distributing BWC recordings for non-business reasons including, but not limited to, uploading BWC data recorded or maintained by the DCSO to public and social media websites; and

(g) Using the BWC for the purpose of embarrassment or ridicule.

448.8 ACTIVATION

448.8.1 MANDATORY ACTIVATION

Deputies who are issued a BWC must activate the BWC:

(a) During all law enforcement-related encounters and activities with the public including, but not limited to, responding to calls for service or assistance, pursuits, Terry stops of motorists or pedestrians, arrests, and searches pursuant to a lawful arrest;

(b) During entry in the execution of a search warrant; and

(c) During any police-citizen contact that becomes adversarial or requires the use of force.

Deputies need not activate the BWC when it is unsafe, impossible, or impracticable to do so, but such instances must be documented as specified in this policy.

448.8.2 DISCRETIONARY ACTIVATION

Deputies may, in the exercise of sound discretion, activate the BWC:

(a) During any police-public encounter not governed by Section 448.8.1(a) if there is reason to believe the recording would potentially yield information having evidentiary value, unless such recording is otherwise expressly prohibited;

(b) To take recorded statements when the deputy’s primary recording device is unavailable or inoperable from persons believed to be victims of or witnesses to crimes, or the persons suspected of committing crimes, after first considering the needs of the investigation and circumstances pertaining to the victim, witness, or suspect;
(c) To record the transportation and physical transfer of persons in the deputy’s custody to hospitals, detox and mental health care facilities, juvenile detention centers, and jails if the deputy anticipates witnessing a criminal event or being involved in or witnessing an adversarial encounter or use-of-force incident; and
(d) At any time the deputy believes it would be appropriate or valuable to activate the BWC in accordance with this policy.

448.8.3 PROHIBITED ACTIVATION

Deputies are prohibited from activating the BWC:

(a) When there is medical care being provided, unless there is reason to believe the recording would document information having evidentiary value, including responding to an apparent mental health crisis or event, as necessary to document any use of force and the basis for it; and
(b) All prohibited uses under Section 448.7.

448.9 DEACTIVATION GUIDELINES

(a) Once the BWC system is activated it should remain on until the incident has concluded. For these purposes conclusion of an incident has occurred when all arrests have been made or when the deputy reasonably believes that additional recording will no longer provide data of evidentiary value.
(b) The BWC may be deactivated if the incident or event is of such duration that the BWC is deactivated to conserve recording times and/or battery life.
(c) The BWC may be deactivated whenever it reasonably appears to the deputy that an individual’s privacy may outweigh any legitimate law enforcement interest in recording. Request from the public to stop recording based on privacy concerns should be considered using this same criteria. Recording should resume when privacy is no longer at issue unless the circumstances no longer fit the criteria for recording.
(d) Deputies may temporarily pause the recording or mute the audio to exchange information with other law enforcement officers or legal counsel. Deputies may obstruct the BWC lens to avoid capturing images of undercover officers, informants, or citizens when based on the training, experience, and judgement of the deputy, a recording would not be appropriate or consistent with this policy. The intention to pause and resume the recording (or to mute the audio or obstruct the lens) will be noted by the deputy either verbally on the BWC or in a written report.
(e) In an officer-involved shooting or use-of-force incident that results in substantial bodily harm the BWC will remain activated until the supervisor on scene authorizes deactivation.

Deactivation must be documented in accordance with Section 448.5(g) of this policy.

448.10 DATA SECURITY SAFEGUARDS AND MISCELLANEOUS COMPLIANCE

(a) The DCSO employs data security safeguards that, at a minimum, meet the requirements of the MGDA and other applicable law. The DCSO will maintain more detailed security and storage safeguards in procedures that are specific to the selected BWC system.
(b) The DCSO will maintain backups of BWC data.
(c) The DCSO will require audit and logging capabilities for its selected BWC system.
(d) The DCSO will maintain logs that include, at minimum, the following information: the date and time BWC data were collected and the applicable classification of the data.
(e) DCSO personnel must not intentionally edit, alter, or erase any BWC recording unless otherwise expressly authorized by the Sheriff, the Sheriff's designee, or this policy.

(f) The DCSO will establish procedures for accessing data and recordings. These procedures must include the process to obtain written authorization by the Sheriff or the Sheriff's designee for access to non-public data by DCSO personnel and members of other governmental entities and agencies for a legitimate, specified law enforcement purpose.

(g) The DCSO will establish procedures for transferring, downloading, tagging or marking events.

(h) The DCSO will prepare an independent biennial audit as required in Minn. Stat. § 13.825, subd. 9.

448.11 RETENTION OF RECORDINGS

(a) All BWC data must be retained for a minimum period of 90 days. There are no exceptions for erroneous recordings or non-evidentiary data.

(b) BWC data that document the discharge of a firearm by a deputy in the course of duty, other than for training or the killing of a sick, injured, or dangerous animal, must be maintained for a minimum period of one year.

(c) BWC data that document the use of force by a deputy that results in substantial bodily harm must be maintained for a minimum period of one year.

(d) If a formal complaint is made against a deputy related to an incident, the BWC data documenting that incident must be maintained for a minimum period of one year.

(e) If an individual captured in a BWC recording submits a written request, the BWC recording must be retained for an additional time period as requested, but not to exceed 180 days. The DCSO will notify the requestor upon receipt of the request that the recording will be retained for a specific time period, after which it will be destroyed unless a new written request is received or it is being retained for a longer period in accordance with applicable law and/or this policy.

(f) Other BWC data having evidentiary value must be retained for the period specified in the DCSO’s records retention schedule.

(g) When a particular BWC recording is subject to multiple retention periods, it must be maintained for the longest applicable period.

448.12 BWC DATA CLASSIFICATION AND ACCESS

448.12.1 BWC CLASSIFICATION

(a) **Data subjects.** Under Minnesota law, the following are considered data subjects for purposes of administering access to BWC data:

(1) Any person or entity whose image or voice is documented in the data;

(2) The deputy who collected the data; and

(3) Any other deputy whose voice or image is documented in the data, regardless of whether that deputy can be identified by the recording.

(b) **BWC data are presumptively private or nonpublic.** BWC recordings are classified as private or nonpublic data, unless there is a specific law that provides otherwise. As a result:

(1) BWC data pertaining to individuals as defined in Minn. Stat. § 13.02, subd. 8 (i.e. natural person, but not a business) are presumed to be private data;

(2) BWC data not on individuals (e.g. a business, agency) are presumed to be nonpublic data;

(3) Some BWC data are classified as confidential (see, (c) below); and
(4) Some BWC data are classified as public (see, (d) below).

(c) **Confidential data.** BWC data that are collected or created as part of an active criminal investigation are governed by Minn. Stat. § 13.82, subd. 7 and are classified as “confidential” or “protected nonpublic data”. This classification takes precedence over the “private” classification listed above and "public" classifications listed below.

(d) **Public data.** The following BWC data are public:

1. Data that document the discharge of a firearm by a peace officer in the course of duty, other than for training or the killing of an animal that is sick, injured or dangerous;
2. Data that document the use of force by a peace officer that result in substantial bodily harm;
3. Data that a data subject requests to be made accessible to the public, subject to redaction. Data on any subject (other than a peace officer) who has not consented to the public release must be redacted. In addition, any data on undercover officers must be redacted; and
4. Data that are public personnel data under Minn. Stat. § 13.43, subd. 2(5).

**Exception:** If another provision of MGDPA classifies data as private or otherwise not public, the data retains that other classification. For instance, data that reveals protected identities under Minn. Stat. 13.82, subd. 17 (e.g., certain victims, witnesses and others) or other applicable law must not be released even if it would otherwise fit into one of the public categories listed above.

**Exception:** The Sheriff may withhold otherwise public data if it is clearly offensive to common sensibilities.

448.12.2 ACCESS TO BWC DATA

(a) **Access to BWC data by data subjects and the public.** DCSO personnel must refer members of the media or public seeking access to BWC data to the data practices liaison, who will process the request in accordance with the MGDPA, this policy, County policies and procedures, and other applicable laws. In particular:

1. An individual must be allowed to view (inspection only, no copying) recorded BWC data about him or herself and other data subjects in the recording, but access must not be granted:
   - if the data were collected or created as part of an active investigation; or
   - to portions of the data that the DCSO would otherwise be prohibited by law from disclosing to the person seeking access, such as portions that would reveal identities protected by Minn. Stat. § 13.82, subd. 17.
2. Unless the data are part of an active investigation, an individual data subject may obtain a copy of the recording, subject to the following guidelines on redaction:
   - data on other individuals in the recording who do not consent to the release must be redacted;
   - data that would identify undercover officers must by redacted; and
   - data on other deputies who are not undercover, and who are on duty and engaged in the performance of official duties, may not be redacted.

(b) **Access to BWC data by DCSO personnel.** DCSO personnel may access and view stored BWC recordings only when there is a legitimate business need for doing so. Compliance with this paragraph satisfies the requirement for the Sheriff or designee to
authorize such access in writing. For purposes of this section, a legitimate business need includes the following:

(1) For use when preparing reports or statements or providing testimony;
(2) By a deputy or supervisor to assess proper functioning of the BWC system;
(3) By DCSO investigators assigned to a related criminal investigation, or after approval of a supervisor, for official investigations;
(4) By a supervisor investigating a specific complaint or report of deputy conduct;
(5) By a supervisor to assess deputy performance and BWC policy compliance,
(6) As permitted in the Officer-Involved Shootings and Deaths Policy 311;
(7) By a Field Training Officer to assess deputy performance; or
(8) For data administration purposes, including responding to a request for data under the MGDPA.

DCSO personnel must document their reasons for accessing stored BWC data in the manner provided within the database at the time of each access.

DCSO personnel seeking access to BWC data when there is not a legitimate business need must make a request for the BWC data in the same manner as any member of the public.

(c) Other authorized access to BWC data. Deputies may display portions of BWC footage to witnesses as necessary for purposes of investigation. Deputies should generally limit these displays in order to protect against the incidental disclosure of individuals whose identities are not public. Protecting against incidental disclosure could involve, for instance, showing only a portion of the video, showing only screen shots, muting the audio, or playing audio but not displaying video.

BWC recordings may be shared with other law enforcement agencies only for legitimate law enforcement purposes that are documented at the time of the disclosure and authorized by the Sheriff or his/her designee in writing, and are in accordance with written procedures.

448.13 COMPLIANCE

Violations of this policy may constitute misconduct and subject DCSO personnel to disciplinary action up to and including termination. The unauthorized access to or disclosure of BWC data may constitute misconduct and subject DCSO personnel to disciplinary action up to and including termination, and criminal penalties, pursuant to Minn. Stat. § 13.09. Any DCSO personnel who accesses, releases, or uses BWC recordings not in accordance with this policy will be subject to disciplinary action (see, the 304 Standards of Conduct and the 811 Protected Information policies). Supervisors and the BWC Administrator must monitor compliance with this policy.