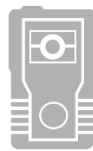




# INDEPENDENT AUDITOR'S REPORT

---

Carlton County Sheriff's Office



FEBRUARY 25TH, 2025  
RAMPART AUDIT LLC

## **Audit Overview and Recommendations**

Dear Carlton County Board and Sheriff Lake:

We have audited the body-worn camera (BWC) program of the Carlton County Sheriff's Office (CCSO) for the two-year period ended 9/13/2024. Minnesota Statute §13.825 mandates that any law enforcement agency operating a portable recording system (PRS)<sup>1</sup> program obtain an independent, biennial audit of its program. This program and its associated data are the responsibility of the Carlton County Sheriff's Office. Our responsibility is to express an opinion on the operations of this program based on our audit.

On October 18, 2024, Rampart Audit LLC (Rampart) met with Chief Deputy Dan Danielson, who provided information about CCSO's BWC program policies, procedures and operations. As part of the audit, Rampart reviewed those policies, procedures and operations for compliance with Minnesota Statute §626.8473, which sets forth the requirements for creating and implementing a BWC program, and Minnesota Statute §13.825, which governs the operation of BWC programs. In addition, Rampart also conducted a sampling of BWC data to verify CCSO's recordkeeping.

The purpose of this report is to provide an overview of this audit, and to provide recommendations to improve the CCSO BWC program and enhance compliance with statutory requirements.

### **CCSO BWC Program Implementation and Authorization**

Effective August 1, 2016, Minnesota Statute §626.8473 Subd. 2 requires that:

A local law enforcement agency must provide an opportunity for public comment before it purchases or implements a portable recording system. At a minimum, the agency must accept public comments submitted electronically or by mail, and the governing body with jurisdiction over the budget of the law enforcement agency must provide an opportunity for public comment at a regularly-scheduled meeting.

In addition, §626.8473 Subd. 3(a) requires that the law enforcement agency establish and enforce a written policy governing the use of its portable recording system, and states "[t]he written policy must be posted on the agency's Web site, if the agency has a Web site."

Rampart previously audited the Carlton County Sheriff's Office's BWC program in October of 2022. At that time, CCSO provided documentation showing that the public notification, comment and meeting requirements had been satisfied prior to the implementation of CCSO's BWC program on November 3, 2020. Specifically, CCSO furnished the following:

---

<sup>1</sup> It should be noted that Minnesota statute uses the broader term "portable recording system" (PRS), which includes body-worn cameras. Because body-worn cameras are the only type of portable recording system employed by CCSO, these terms may be used interchangeably in this report.

- A copy of a press release dated April 28, 2020, announcing CCSO's plan to implement a BWC program and inviting the public to provide comment electronically, by mail or in person at the May 12, 2020, meeting of the Carlton County Board.
- A copy of an article relaying this same information that appeared in the Cloquet, MN, *Pine Journal* newspaper.
- A copy of the minutes of the May 12, 2020, Carlton County Board meeting, which noted that CCSO "was present to facilitate a Body Worn Cameras Forum allowing the public an opportunity to provide comment regarding purchase and implementation of body worn cameras under Minnesota Statute §626.8473."

Copies of these documents have been retained in Rampart's audit files.

Rampart staff also verified that there was a working link to the Carlton County Sheriff's Office's written BWC policy on their webpage at the time of our audit.

In our opinion, CCSO met the public notice and comment requirements prior to the implementation of their BWC program.

### **CCSO BWC WRITTEN POLICY**

As part of this audit, we reviewed CCSO's BWC policy, a copy of which is attached to this report as Appendix A.

Minnesota Statute §626.8473 Subd. 3(b) requires a written BWC policy to incorporate the following, at a minimum:

1. The requirements of section 13.825 and other data classifications, access procedures, retention policies, and data safeguards that, at a minimum, meet the requirements of chapter 13 and other applicable law;
2. A prohibition on altering, erasing or destroying any recording made with a peace officer's portable recording system or data and metadata related to the recording prior the expiration of the applicable retention period under section 13.825 Subdivision 3, except that the full, unedited, and unredacted recording of a peace officer using deadly force must be maintained indefinitely;
3. A mandate that a portable recording system be worn at or above the mid-line of the waist in a position that maximizes the recording system's capacity to record video footage of the officer's activities;
4. A mandate that officers assigned a portable recording system wear and operate the system in compliance with the agency's policy adopted under this section while performing law enforcement activities under the command and control of another chief law enforcement officer or federal law enforcement official;
5. A mandate that, notwithstanding any law to the contrary, when an individual dies as a result of a use of force by a peace officer, an involved officer's law enforcement agency must 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, upon their request, to inspect all portable recording system data, redacted no more than what is required by law, documenting the incident within five days of the request, with the following exception:

- A law enforcement agency may deny a request if the agency determines that there is a compelling reason that inspection would interfere with an active investigation. If the agency denies access, the chief law enforcement officer must provide a prompt, written denial to the individual who requested the data with a short description of the compelling reason access was denied and must provide notice that relief may be sought from the district court pursuant to section 13.82 subdivision 7;
- 6. A mandate that, when an individual dies as a result of a use of force by a peace officer, an involved officer's law enforcement agency shall release all portable recording system data, redacted no more than required by law, documenting the incident no later than 14 days after the incident, unless the chief law enforcement officer asserts in writing that the public classification would interfere with an ongoing investigation, in which case the data remain classified by section 13.82 subdivision 7;
- 7. Procedures for testing the portable recording system to ensure adequate functioning;
- 8. Procedures to address a system malfunction or failure, including requirements for documentation by the officer using the system at the time of a malfunction or failure;
- 9. Circumstances where recording is mandatory, prohibited, or at the discretion of the officer using the system;
- 10. Circumstances under which a data subject must be given notice of a recording;
- 11. Circumstances under which a recording may be ended while an investigation, response, or incident is ongoing;
- 12. Procedures for the secure storage of portable recording system data and the creation of backup copies of the data; and
- 13. Procedures to ensure compliance and address violations of the policy, which must include, at a minimum, supervisory or internal audits and reviews, and the employee discipline standards for unauthorized access to data contained in section 13.09.

In our opinion, the CCSO BWC policy is compliant with respect to clauses 7 – 11.

Due to their complexity and interrelatedness, clauses 1 and 12 are discussed separately below. Clause 13 is also discussed separately.

Clauses 2 – 6 are newly added as a result of 2023 legislation and will also be discussed separately below.

### **CCSO BWC Data Retention**

Minn. Stat. §13.825 Subd. 3(a) establishes a minimum retention period of 90 days for all BWC data not subject to a longer retention period, while §13.825 Subd. 3(b) requires that the following categories of BWC data be retained for a minimum period of one year:

- 1) any reportable firearms discharge;
- 2) any use of force by an officer that results in substantial bodily harm; and
- 3) any incident that results in a formal complaint against an officer.

Meanwhile, Subd. 3(c) requires that any portable recording system data documenting a peace officer's use of deadly force must be maintained indefinitely. Finally, Subd. 3(d) requires that an agency retain BWC recordings for an additional period of up to 180 days when so requested in writing by a data subject.

Section 422.11 of CCSO's BWC policy states that "[a]ll recordings shall be retained for a period consistent with the requirements of the organization['s] records retention schedule but in no event for a period of less than 180 days." This section of the policy also specifies a retention period of "at least [sic] one year" for the data categories listed in §13.825 Subd. 3(b).

We noted that Section 422.11 states: "If an individual captured in a recording submits a written request, the recording shall be retained for an additional time period," while §13.825 Subd. 3(d) specifies that the data subject may request an additional retention period of up to 180 days. We recommend that CCSO add language to clarify the length of the additional retention period.

The "indefinite" retention period described in §13.825 Subd. 3(c) was newly added as a result of 2023 legislative changes, and was not addressed in CCSO's BWC policy.

Prior to the issuance of this report, CCSO submitted a revised BWC policy that addresses the "indefinite" retention requirements for data contained in §13.825 Subd. 3(c), as well as clarifying that BWC data will be retained for an additional period of up to 180 days when so requested by a data subject.

The Prohibited Use of Audio/Video Recorders section of CCSO's BWC policy states that: "Members are prohibited from altering, erasing or destroying media captured by portable recorders prior to the expiration of the applicable retention period." As discussed in Clause 2 of the Policy section of this report, this prohibition must also extend to data and metadata related to such recordings.

Prior to the issuance of this report, CCSO submitted a revised BWC policy that addresses this issue by defining the term "BWC media" to include associated metadata.

CCSO employs Motorola V300 body-worn cameras and manages BWC data retention on Motorola's secure, cloud-based servers through automated retention settings in the VideoManager EL video management software. The retention period for each video is determined by the data classification assigned at the time of upload; however, this retention period can be adjusted as needed.

CCSO's BWC policy requires that each deputy transfer data from his or her body-worn camera to the Motorola server by the end of each shift, and also requires that the deputy assign the appropriate label or labels to each file to identify the nature of the data. These labels then determine the appropriate retention period for each file.

In our opinion, CCSO's revised BWC policy is compliant with respect to applicable data retention requirements.

### **CCSO BWC Data Destruction**

As discussed above, CCSO's BWC data are stored on Motorola's cloud-based servers, with data retention and deletion schedules managed automatically through the VideoManager EL video management software based on the assigned data classification of each video.

Motorola utilizes Microsoft's Azure Government environment for cloud storage. Microsoft certifies this environment as being compliant with the current Federal Bureau of Investigation Criminal Justice Information Services Division Security Policy (5.9.1), and notes that it has signed CJIS management

agreements with 45 of the 50 U.S. states, including Minnesota, to verify compliance with state CJIS requirements.

FBI CJIS policy requires that hard drives used for CJIS data storage are sanitized by overwriting at least three times or degaussing prior to being released to unauthorized individuals, while inoperable drives must be destroyed through physical means such as shredding.

In our opinion, CCSO's written BWC policy is compliant with respect to the applicable data destruction requirements.

### **CCSO BWC Data Access**

Any request for access to BWC data by data subjects would be made in writing to the CCSO Records Department, by submitting CCSO's preferred data request form. The records staff or Chief Deputy is then responsible for reviewing and fulfilling each request in accordance with the provisions of §13.825 Subd. 4(b). Recordings are provided on physical media, such as an optical disc or USB memory device.

Though not addressed in the BWC policy, Chief Deputy Danielson advised us that CCSO BWC data are shared with other law enforcement agencies for evidentiary purposes only. All such requests must be made in writing to the CCSO Records Department, and must be approved by Chief Deputy Danielson. As part of the audit, CCSO provided a copy of their BWC Data Agency Sharing Form, which requires that a designee of the requesting agency provide a signed acknowledgement of the receiving agency's responsibilities under §13.825 Subd. 7 and 8. A copy of each written acknowledgment is maintained on file.

Requests from prosecutors and other law enforcement agencies are fulfilled via an emailed internet link through the VideoManager EL software.

While CCSO is already following this process in practice, we recommend adding language to the BWC policy stating that BWC data will be shared with other agencies only for legitimate law enforcement purposes that are disclosed in writing at the time of the request. Prior to the issuance of this report, CCSO submitted a revised BWC policy that adds this language.

As discussed in Clauses 5 and 6 of the Policy section of this report, the Minnesota State Legislature in 2023 added specific access requirements related to BWC data that document deadly force incidents, and specified that these requirements must be included in the agency's BWC policy. At the time of our audit, CCSO had not addressed these new requirements. Prior to the issuance of this report, CCSO submitted a revised BWC policy that added language to meet these requirements.

In our opinion, CCSO's revised BWC policy is compliant with respect to the applicable data access requirements.

### **CCSO BWC Data Classification**

CCSO's BWC policy identifies all BWC data as private or nonpublic, "[e]xcept as provided in Minn. Stat. §13.825 Subd. 2." In our opinion, incorporating by reference the exceptions identified in §13.825 Subd.

2 satisfies the applicable data classification requirements. Rampart recommends, however, that CCSO add language to its BWC policy to specifically note that BWC data documenting an officer's use of deadly force is statutorily classified as public. Prior to the issuance of this report, CCSO submitted a revised BWC policy that addresses the "public classification" of such data.

### **CCSO BWC Internal Compliance Verification**

The Review of Recorded Media Files section of the CCSO BWC policy authorizes supervisors to "review relevant recordings any time they are investigating alleged misconduct or reports or meritorious conduct or whenever such recordings would be beneficial in reviewing the member's performance." The policy also notes that BWC recordings may be reviewed "[b]y a supervisor as part of internal audits and reviews as required by Minn. Stat. §626.8473.

Chief Deputy Danielson advised us that, "Our office reviews deputy body worn camera footage after every use of force and / or significant matter or call. In addition, we review body worn camera footage during the investigation of all deputy complaints as well as random checks of random deputies at intermittent times.

We recommend that CCSO adopt additional language to clarify that supervisors shall conduct internal audits and reviews, as well as to provide guidance with respect to the appropriate procedures and frequency for such audits and reviews. Prior to the issuance of this report, CCSO submitted a revised policy that addresses this issue by requiring supervisors to conduct reviews to determine both overall compliance with the policy, as well as to specifically review that deputies are properly uploading and labeling BWC recordings.

As discussed in Clause 4 of the Policy section of this report, the 2023 legislative changes require that an agency's BWC policy must require that an officer assigned a BWC wear and operate the system in compliance with the agency's BWC policy while performing law enforcement activities under the command and control of another chief law enforcement officer or federal law enforcement official.

CCSO's BWC policy does not address the requirements discussed in the preceding paragraph. Prior to the issuance of this report, CCSO submitted a revised BWC policy that states: "Members shall comply with this policy's provisions while performing law enforcement activities under the command and control of another law enforcement agency."

**Auditor's Note:** The Carlton County Sheriff's Office participates in two federal task forces: The U.S. Marshals Service (USMS) Fugitive Task Force, and the Drug Enforcement Agency (DEA) Task Force. CCSO's BWC policy directs any deputy working on an assignment approved by either task force to follow the BWC policy adopted by the corresponding task force. We note that this appears to contradict the Minn. Stat. §626.8473 Subd. 3(b)(3) requirement that "officers assigned a portable recording system wear and operate the system in compliance with the agency's policy adopted under this section while performing law enforcement activities under the command and control of... [a] federal law enforcement official." It is not clear whether the legislative intent behind this requirement was to address ad hoc circumstances, such as when multiple agencies respond to a protest, natural disaster or other isolated incident, or if the requirement was intended to apply to recurring circumstances, such as task force operations, though we note that it appears to be common practice for such task forces to adopt their

own BWC policy. In the present case, Rampart has not reviewed or audited the associated task force programs, policies or procedures and we do not express an opinion as to their compliance with Minn. Stat. §13.825 or §626.8473.

In our opinion, CCSO's revised BWC policy satisfies the requirements of Clause 4, except with respect to CCSO's task force operations, for which we do not express an opinion.

The Accountability section of CCSO's BWC policy states that "[a]ny member who accesses or releases recordings without authorization may be subject to discipline." Because certain violations of Minn. Stat. Chapter 13 can be charged as misdemeanors, we recommend that CCSO add language noting that violations of the BWC policy may also result in prosecution. Prior to the issuance of this report, CCSO submitted a revised BWC policy that adds this language.

In our opinion, CCSO's revised BWC policy are compliant with the applicable internal compliance and disciplinary requirements contained in §626.8473 Subd. 3(b)(8).

### **CCSO BWC Program and Inventory**

CCSO currently possesses 33 Motorola body-worn cameras, including multiple spares.

The CCSO BWC policy identifies those circumstances in which deputies are expected to activate their body-worn cameras, as well as circumstances in which they are prohibited from activating their body-worn cameras. The policy also provides guidance for those circumstances in which BWC activation is deemed discretionary.

The Prohibited Use of Audio/Video Recorders section of the CCSO BWC policy states that "[p]rior to going into service, each uniformed member will be responsible for making sure that he/she is equipped with a portable recorder issued by the Office, and that the recorder is in good working order." Chief Deputy Danielson advised that this is accomplished through a function check to ensure the recorder is operating correctly. This section of the policy also states that "[m]embers are prohibited from using personally owned recording devices while on duty."

While CCSO does not maintain a separate log of BWC deployment or use, Chief Deputy Danielson advised us that because each uniformed deputy wears a BWC while on duty, the number of BWC units deployed with uniformed personnel each shift can be determined based on a review of CCSO payroll records. In addition, non-uniformed personnel are issued and authorized but not required to wear or use body-worn cameras. Actual BWC use would be determined based on the creation of BWC data.

As of 10/30/2024, CCSO maintained 23,206 files of BWC data, totaling approximately 19.58 TB.

### **CCSO BWC Physical, Technological and Procedural Safeguards**

CCSO BWC data are initially recorded to an internal hard drive in each deputy's BWC. Those files are then transferred to a Motorola's cloud service via wireless data uplink.



Deputies have view-only access to their own data for report writing, trial preparation, data administration, investigatory purposes and other legitimate law enforcement purposes through Motorola's VideoManager EL software.

CCSO's BWC policy states that: "Members are prohibited from using office-issued recorders and recording media for personal use and are prohibited from making personal copies of recordings created while on-duty or while acting in their official capacity." In addition: "Members are also prohibited from retaining recordings of activities or information obtained while on duty..." We noted that while CCSO previously removed language authorizing the use of personally-owned recording devices, there is a reference in this passage to "personally owned recorders," which appears to be an artifact from the previous version of the BWC policy. Because §13.825 Subd. 6 states unequivocally that "[w]hile on duty, a peace officer may only use a portable recording system issued and maintained by the officer's agency in documenting the officer's activities," we recommend removing this reference to personally owned recorders.

As noted above, requests by other law enforcement agencies for CCSO BWC data must be approved by Deputy Chief Danielson and are fulfilled via expiring email link. A similar method is employed to submit CCSO BWC data to the Carlton County Attorney's Office.

The Member Responsibilities section of CCSO's BWC policy states: "Uniformed members shall wear the recorder in a conspicuous manner at or above the mid-line of the waist and notify persons that they are being recorded, whenever reasonably practicable." This section of the policy also states that: "Unless conducting a lawful recording in an authorized undercover capacity, non-uniformed members should wear the recorder in a conspicuous manner when in use or otherwise notify persons that they are being recorded, whenever reasonably practicable." As discussed in Clause 3 of the Policy section of this report, the 2023 legislative changes require that an agency's BWC policy must specify that a BWC be worn at or above the mid-line of the waist. Because Minn. Stat. §626.8473 Subd. 3(b)(2) does not indicate that this requirement applies only to uniformed personnel, Rampart recommends that CCSO modify the second passage quoted above to clarify that non-uniformed personnel must also wear their BWC at or above the mid-line of the waist, except when acting in an authorized undercover capacity.

Prior to the issuance of this report, BPD submitted a revised BWC policy that clarifies that all members must wear their BWC at or above the mid-line of the waist. In our opinion, this revised BWC policy satisfies this requirement.

### **Enhanced Surveillance Technology**

CCSO currently employs BWCs with only standard audio/video recording capabilities. They have no plans at this time to add enhanced BWC surveillance capabilities, such as thermal or night vision, or to otherwise expand the type or scope of their BWC technology.

If CCSO should obtain such enhanced technology in the future, Minnesota Statute §13.825 Subd. 10 requires notice to the Minnesota Bureau of Criminal Apprehension within 10 days. This notice must include a description of the technology and its surveillance capability and intended uses.

### **Data Sampling**

Rampart selected a random sample of 132 calls for service from which to review any available BWC recordings. It should be noted that not every call will result in a deputy activating his or her BWC. For example, a deputy who responds to a driving complaint but is unable to locate the suspect vehicle would be unlikely to activate his or her BWC. It should also be noted that because the audit covers a period of two years, while most BWC data is only required to be retained for 90 days, there is a significant likelihood that the sample population will include calls for which BWC data was created, but which has since been deleted due to the expiration of the retention period. The auditor reviewed the retained BWC videos to verify that this data was accurately documented in CCSO records.

### **Audit Conclusions**

In our opinion, as of the date of this report the Carlton County Sheriff's Office's Body-Worn Camera Program is substantially compliant with Minnesota Statutes §13.825 and §626.8473, except with respect to task force assignments, for which Rampart does not express an opinion.

A handwritten signature in black ink, appearing to read "Rampart Audit LLC", is written over a horizontal line.

Rampart Audit LLC

2/25/2025

# APPENDIX A:

Policy

422

## Carlton County Sheriff's Office

Carlton Cnty SO Policy Manual

## Portable Audio/Video Recorders

### 422.1 PURPOSE AND SCOPE

This policy provides guidelines for the use of portable audio/video recording devices by members of this office while in the performance of their duties (Minn. Stat. § 626.8473). Portable audio/video recording devices include all recording systems whether body-worn, hand-held, or integrated into portable equipment.

This policy does not apply to mobile audio/video recordings, interviews, or interrogations conducted at any Carlton County Sheriff's Office facility, undercover operations, wiretaps, or eavesdropping (concealed listening devices).

#### 422.1.1 DEFINITIONS

Definitions related to this policy include:

**Portable recording system** - A device worn by a member that is capable of both video and audio recording of the member's activities and interactions with others or collecting digital multimedia evidence as part of an investigation and as provided in Minn. Stat. § 13.825.

### 422.2 POLICY

The Carlton County Sheriff's Office may provide members with access to portable recorders for use during the performance of their duties. The use of recorders is intended to enhance the mission of the Office by accurately capturing contacts between members of the Office and the public.

### 422.3 COORDINATOR

The Sheriff or the authorized designee should designate a coordinator responsible for (Minn. Stat.

§ 626.8473; Minn. Stat. § 13.825):

- (a) Establishing procedures for the security, storage, and maintenance of data and recordings.
  - 1. The coordinator should work with the Custodian of Records and the member assigned to coordinate the use, access, and release of protected information to ensure that procedures comply with requirements of the Minnesota Government

Data Practices Act (MGDPA) and other applicable laws (Minn. Stat. § 13.01 et seq.) (see the Protected Information and the Records Maintenance and Release policies).

2. The coordinator should work with the Custodian of Records to identify recordings that must be retained for a specific time frame under Minnesota law (e.g., firearm discharges, certain use of force incidents, formal complaints).
- (b) Establishing procedures for accessing data and recordings.
    1. These procedures should include the process to obtain written authorization for access to non-public data by CCSO members and members of other governmental entities and agencies.
  - (c) Establishing procedures for logging or auditing access.
  - (d) Establishing procedures for transferring, downloading, tagging, or marking events.
  - (e) Establishing an inventory of portable recorders including:
    1. Total number of devices owned or maintained by the Carlton County Sheriff's Office.
    2. Daily record of the total number deployed and used by members and, if applicable, the precinct or district in which the devices were used.
    3. Total amount of recorded audio and video data collected by the devices and maintained by the Carlton County Sheriff's Office.
  - (f) Preparing the biennial audit required by Minn. Stat. § 13.825, Subd. 9.
  - (g) Notifying the Bureau of Criminal Apprehension (BCA) in a timely manner when new equipment is obtained by the Carlton County Sheriff's Office that expands the type or scope of surveillance capabilities of the office's portable recorders.
  - (h) Ensuring that this Portable Audio/Video Recorders Policy is posted on the Office website.

#### **422.4 MEMBER PRIVACY EXPECTATION**

All recordings made by members on any office-issued device at any time or while acting in an official capacity of this office, regardless of ownership of the device, shall remain the property of the Office. Members shall have no expectation of privacy or ownership interest in the content of these recordings.

#### **422.5 MEMBER RESPONSIBILITIES**

Prior to going into service, uniformed members will be responsible for making sure that they are equipped with a portable recorder issued by the Office, and that the recorder is in good working order (Minn. Stat. § 13.825). If the recorder is not in working order or the member becomes aware of a malfunction at any time, the member shall promptly report the failure to their supervisor and obtain a functioning device as soon as reasonably practicable. Uniformed members should wear the recorder in a conspicuous manner at or above the mid-line of the waist

and notify persons that they are being recorded, whenever reasonably practicable (Minn. Stat. § 626.8473).

Any member assigned to a non-uniformed position may carry an approved portable recorder at any time the member believes that such a device may be useful. Unless conducting a lawful recording in an authorized undercover capacity, non-uniformed members should wear the recorder in a conspicuous manner when in use or otherwise notify persons that they are being recorded, whenever reasonably practicable.

When using a portable recorder, the assigned member shall record their name, employee number, and the current date and time at the beginning and the end of the shift or other period of use, regardless of whether any activity was recorded. This procedure is not required when the recording device and related software captures the user's unique identification and the date and time of each recording.

Members should document the existence of a recording in any report or other official record of the contact, including any instance where the recorder malfunctioned or the member deactivated the recording (Minn. Stat. § 626.8473). Members should include the reason for deactivation.

#### **422.6 ACTIVATION OF THE AUDIO/VIDEO RECORDER**

This policy is not intended to describe every possible situation in which the recorder should be used, although there are many situations where its use is appropriate. Members should activate the recorder any time the member believes it would be appropriate or valuable to record an incident.

The recorder should be activated in any of the following situations:

- (a) All enforcement and investigative contacts including stops and field interview (FI) situations
- (b) Traffic stops including, but not limited to, traffic violations, stranded motorist assistance and all crime interdiction stops
- (c) Self-initiated activity in which a member would normally notify 9-1-1 Communications
- (d) Any other contact that becomes adversarial after the initial contact in a situation that would not otherwise require recording

Members should remain sensitive to the dignity of all individuals being recorded and exercise sound discretion to respect privacy by discontinuing recording whenever it reasonably appears to the member that such privacy may outweigh any legitimate law enforcement interest in recording. Requests by members of the public to stop recording should be considered using this same criterion. Recording should resume when privacy is no longer at issue unless the circumstances no longer fit the criteria for recording.

At no time is a member expected to jeopardize his/her safety in order to activate a portable recorder or change the recording media. However, the recorder should be activated in situations

described above as soon as reasonably practicable.

#### 422.6.1 CESSATION OF RECORDING

Once activated, the portable recorder should remain on continuously until the member reasonably believes that his/her direct participation in the incident is complete or the situation no longer fits the criteria for activation. Recording may be stopped during significant periods of inactivity such as report writing or other breaks from direct participation in the incident.

#### 422.6.2 SURREPTITIOUS RECORDINGS

Minnesota law permits an individual to surreptitiously record any conversation in which one party to the conversation has given his/her permission (Minn. Stat. § 626A.02).

Members of the Office may surreptitiously record any conversation during the course of a criminal investigation in which the member reasonably believes that such a recording will be lawful and beneficial to the investigation.

Members shall not surreptitiously record another office member without a court order unless lawfully authorized by the Sheriff or the authorized designee.

#### 422.6.3 EXPLOSIVE DEVICE

Many portable recorders, including body-worn cameras and audio/video transmitters, emit radio waves that could trigger an explosive device. Therefore, these devices should not be used where an explosive device may be present.

### 422.7 PROHIBITED USE OF AUDIO/VIDEO RECORDERS

Members are prohibited from using office-issued portable recorders and recording media for personal use and are prohibited from making personal copies of recordings created while on-duty or while acting in their official capacity.

Members are also prohibited from retaining recordings of activities or information obtained while on-duty, whether the recording was created with office-issued or personally owned recorders. Members shall not duplicate or distribute such recordings, except for authorized legitimate office business purposes. All such recordings shall be retained at the Office.

Members are prohibited from using personally owned recording devices while on-duty.

Members may only use a portable recording system issued and maintained by the Carlton County Sheriff's Office in documenting the members activities.

Recordings shall not be used by any member for the purpose of embarrassment, harassment or ridicule.

Members are prohibited from altering, erasing or destroying media captured by portable recorders prior to the expiration of the applicable retention period.

### 422.8 IDENTIFICATION AND PRESERVATION OF RECORDINGS

To assist with identifying and preserving data and recordings, members should download, tag

or mark the recordings in accordance with procedure and document the existence of the recording in any related case report.

A member should transfer, tag or mark recordings when the member reasonably believes:

- (a) The recording contains evidence relevant to potential criminal, civil or administrative matters.
- (b) A complainant, victim or witness has requested non-disclosure.
- (c) A complainant, victim or witness has not requested non-disclosure but the disclosure of the recording may endanger the person.
- (d) Disclosure may be an unreasonable violation of someone's privacy.
- (e) Medical or mental health information is contained.
- (f) Disclosure may compromise an under-cover officer or confidential informant.
  
- (g) The recording or portions of the recording may be protected under the Minnesota Data Practices Act.

Any time a member reasonably believes a recorded contact may be beneficial in a non-criminal matter (e.g., a hostile contact), the member should promptly notify a supervisor of the existence of the recording.

#### **422.9 ACCOUNTABILITY**

Any member who accesses or releases recordings without authorization may be subject to discipline (see the Standards of Conduct and the Protected Information policies) (Minn. Stat. § 626.8473).

#### **422.10 REVIEW OF RECORDED MEDIA FILES**

When preparing written reports, members should review their recordings as a resource (see the Officer-Involved Shootings and Deaths Policy for guidance in those cases). However, members shall not retain personal copies of recordings. Members should not use the fact that a recording was made as a reason to write a less detailed report.

Supervisors are authorized to review relevant recordings any time they are investigating alleged misconduct or reports of meritorious conduct or whenever such recordings would be beneficial in reviewing the member's performance.

Recorded files may also be reviewed:

- (a) By a supervisor as part of internal audits and reviews as required by Minn. Stat. § 626.8473.
- (b) Upon approval by a supervisor, by any member of the Office who is participating in an official investigation, such as a personnel complaint, administrative investigation, or criminal investigation.
- (c) Pursuant to lawful process or by court personnel who are otherwise authorized to review

evidence in a related case.

- (d) By media personnel with permission of the Sheriff or the authorized designee.
- (e) In compliance with the Minnesota Data Practices Act request, if permitted or required by the Act, including pursuant to Minn. Stat. § 13.82, Subd. 15, and in accordance with the Records Maintenance and Release Policy.

All recordings should be reviewed by the Custodian of Records prior to public release (see the Records Maintenance and Release Policy). Recordings that are clearly offensive to common sensibilities should not be publicly released unless disclosure is required by law or order of the court (Minn. Stat. § 13.82, Subd. 7; Minn. Stat. § 13.825, Subd. 2).

#### **422.11 RETENTION OF RECORDINGS**

All recordings shall be retained for a period consistent with the requirements of the organizations records retention schedule but in no event for a period of less than 180 days.

Recordings documenting the discharge of a firearm by a peace officer in the course of duty if notice is required under section 626.553, subd. 2, or, the use of force by a peace officer that results in substantial bodily harm; or, if a formal complaint is made against a peace officer related to the incident shall be maintained for at least one year.

If an individual captured in a recording submits a written request, the recording shall be retained for an additional period of time. The coordinator should be responsible for notifying the individual prior to destruction of the recording (Minn. Stat. § 13.825).#

##### **422.11.1 RELEASE OF AUDIO/ VIDEO RECORDINGS**

Requests for the release of audio/ video recordings shall be processed in accordance with office policy.

##### **422.11.2 ACCESS TO RECORDINGS**

Except as provided by Minn Stat. § 13.825, Subd. 2, audio/ video recordings are considered private or non public data.

Any person captured in a recording may have access to the recording. If the individual requests a copy of the recording and does not have the consent of other non-law enforcement individuals captured on the recording, the identity of those individuals must be blurred or obscured sufficiently to render the the subject unidentifiable prior to release. The identity of on-duty peace officers may not be obscured unless their identity is protected under Minn. Stat. § 13.82, Subd. 17.

#### **422.12 US MARSHAL FUGITIVE TASK FORCE MEMBERS**

The Carlton County Sheriff's Office may have employees working as members of the US Marshal Service (USMS) Fugitive Task Force. Any employee deputized as a US Marshal working on a task force approved assignment must follow USMS rules related to the use of portable recording systems.



#### **422.13** DRUG ENFORCEMENT AGENCY TASK FORCE MEMBERS

The Carlton County Sheriff's Office may have employees working as members of the Drug Enforcement Agency (DEA) Task Force. Any employee deputized as a DEA task force member working on a task force approved assignment must follow DEA rules related to the use of portable recording systems.

# APPENDIX B:

Policy

**433**

## Carlton County Sheriff's Office

Carlton Cnty SO Policy Manual

---

### Body-Worn Cameras

#### 433.1 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 office and for the access, use, and retention of office BWC media (Minn. Stat.

§ 626.8473).

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).

##### 433.1.1 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 office BWCs and the associated metadata.

**BWC media systems** - Any software, including web-based programs and mobile applications, used by the Office 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.

#### **433.2 POLICY**

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

#### **433.3 RESPONSIBILITIES**

##### **433.3.1 BWC COORDINATOR RESPONSIBILITIES**

The Sheriff or the authorized designee should delegate certain responsibilities to a BWC coordinator (Minn. Stat. § 13.825; Minn. Stat. § 626.8473).

The responsibilities of the coordinator include:

- (a) Serving as a liaison between the Office and the BWC manufacturer/distributor and any third-party media storage vendor.
- (b) Developing inventory and documentation procedures for issuing and tracking BWC equipment, including properly marking BWCs as property of the Office, recording the date each BWC is placed into or taken out of service, and maintaining the following information:
  - 1. The total number of devices owned or maintained by the Carlton County Sheriff's Office
  - 2. The daily record of the total number deployed and used by members and, if applicable, the precinct or district in which the devices were used
  - 3. The total amount of recorded audio and video data collected by the BWC media systems and maintained by the Carlton County Sheriff's Office
- (c) 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.
- (d) 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 office duties.
  - 2. Security requirements, such as two-factor authentication and appropriate password parameters, are in place for user credentials.
  - 3. Procedures include a process to obtain written authorization for access to non-public data by CCSO members and members of other governmental entities and agencies.
- (e) Configuring BWC media systems, or developing manual procedures, so that media is appropriately categorized and retained according to the event type tagged by members.

- (f) 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 office policy.
- (g) Developing and updating BWC training for members who are assigned a BWC or given access to BWC media systems.
- (h) Coordinating with the community relations coordinator to (see the Community Relations Policy):
  - 1. Provide the public with notice of the office's use of BWCs (e.g., posting on the office website or social media pages).
  - 2. Gain insight into community expectations regarding BWC use.
- (i) Coordinating with the Records Manager to (see the Records Section, Records Maintenance and Release, and Protected Information policies):
  - 1. Determine and apply proper retention periods to BWC media (e.g., firearm discharges, certain use of force incidents, formal complaints).
  - 2. Develop procedures for the appropriate release of BWC media.
  - 3. Ensure procedures comply with the requirements of the Minnesota Government Data Practices Act and other applicable laws (Minn. Stat. § 13.01 et seq.).
- (j) Coordinating with the Evidence Room to develop procedures for the transfer, storage, and backup of evidentiary BWC media (see the Evidence Room Policy).
- (k) Preparing the biennial audit required by Minn. Stat. § 13.825, Subd. 9.
- (l) Notifying the Bureau of Criminal Apprehension (BCA) in a timely manner when new equipment is obtained by the Carlton County Sheriff's Office that expands the type or scope of surveillance capabilities of the office's portable recorders.

#### 433.3.2 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 (Minn. Stat. § 13.825; Minn. Stat. § 626.8473).

Members should wear their assigned BWC on their outermost garment positioned at or above the mid-line of the waist (Minn. Stat. § 626.8473). 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 (Minn. Stat. §

626.8473).

Members shall comply with this policy's provisions while performing law enforcement activities under the command and control of another law enforcement agency (Minn. Stat. § 626.8473).

#### **433.4 BWC USE**

The following guidelines apply to the use of BWCs:

- (a) Only office-issued BWCs should be used.
- (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 office-issued BWCs shall be strictly limited to office-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 Sheriff.

##### **433.4.1 PROHIBITIONS**

BWCs should not be used to record:

- (a) Routine administrative activities of the Office that do not involve interactions with the public. Care should be taken to avoid incidentally recording confidential documents that the Office has a duty to keep secure (i.e., criminal justice information).
- (b) Areas within the office 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.
- (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 deputies or confidential informants.
- (g) Strip searches.

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

#### **433.5 ACTIVATION OF BWC**

Members should activate their BWC during all calls for service and the performance of law enforcement-related functions. 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.

#### 433.5.1 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.

#### 433.5.2 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 office interest in recording the event. Members may also mute or deactivate their BWC:

- (a) To protect the privacy of a victim or witness.
- (b) When an individual wishes to provide information anonymously.
- (c) To avoid recording a confidential informant or undercover deputy.
- (d) When discussing case tactics or strategy.
- (e) During private conversations with other members or emergency responders.

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 office'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.

#### 433.5.3 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 Sheriff 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.

#### 433.5.4 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.

#### **433.6 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 Office.

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.

##### 433.6.1 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.

#### **433.7 BWC MEDIA**

All BWC media is the sole property of the Office. 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 Office and shall not be used by the vendor for any purpose without explicit approval of the Sheriff or the authorized designee.

Members shall not alter, copy, delete, release, or permit access to BWC media other than as permitted in this policy.

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

##### **433.7.1 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 office-related purposes in accordance with the following guidelines:

- (a) BWC media tagged as restricted should only be accessible by those designated by the Sheriff or the authorized designee.
- (b) Members may review their own BWC media for office-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 office-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 office 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 (Minn. Stat. § 626.8473).

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 Lieutenant is permitted to access and view BWC media for training purposes.
1. The Lieutenant should conduct a quarterly review of a random sampling of BWC media to evaluate office 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 Lieutenant may use BWC media for training purposes with the approval of the Sheriff or the authorized designee. The Lieutenant 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 office-related duties.
- (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.
- (i) Any member who accesses or releases BWC media without authorization may be subject to discipline and/or criminal prosecution (see the Standards of Conduct and the Protected Information policies for additional guidance) (Minn. Stat. § 626.8473).

#### 433.7.2 PUBLIC ACCESS

Unless disclosure is required by law or a court order, BWC media should not be released to the public if:

- (a) It is clearly offensive to common sensibilities (Minn. Stat. § 13.82, Subd. 7; Minn. Stat. § 13.825, Subd. 2).
- (b) It unreasonably violates a person's privacy or depicts the interior of:
  1. A private residence.
  2. A facility that offers health care, mental health or substance abuse treatment, or social services.
  3. A school building.
  4. Any other building in which public access is restricted or which implicates heightened security concerns.

Except as provided by Minn. Stat. § 13.825, Subd. 2 or pursuant to Minn. Stat. § 13.82, Subd. 15, BWC media is considered private or nonpublic data.

Any person captured on BWC media may have access to the BWC media. If the individual requests a copy of the BWC media and does not have the consent of other non-law enforcement individuals captured on the BWC media, the identity of those individuals must be blurred or

obscured sufficiently to render the person unidentifiable prior to release. The identity of on-duty peace officers may not be obscured unless their identity is protected under Minn. Stat. § 13.82, Subd. 17 (Minn. Stat. § 13.825, Subd. 4).

Requests for the release of BWC media shall be processed in accordance with the Records Maintenance and Release Policy. The Records Manager should review BWC media before public release. BWC media may be released to other law enforcement agencies only for legitimate law enforcement purposes that are documented in writing at the time of request, prior to disclosure. The law enforcement agency receiving the data shall acknowledge their intent to comply with all data classification, destruction, and security requirements of Minn Stat § 13.825. BWC media shall be made available to prosecutors, courts, and other criminal justice entities as provided by law.

When an individual dies as a result of a use-of-force by a Carlton County Sheriff's Deputy, the Carlton County Sheriff's Office shall release all portable recording systems data, redacted no more than required by law, documenting the incident no later than 14 days after the incident, unless the Sheriff asserts in writing that the public classification would interfere with an ongoing investigation, in which the case data remain classified by § 12.82 subd. 7. Notwithstanding any law to the contrary, when an individual dies as a result of a use of force by a peace officer, the Carlton County Sheriff's Office must 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, upon their request, to inspect all portable recording system data, redacted no more than what is required by law, documenting the incident within five days of the request, with the following exception:

- (a) The Carlton County Sheriff's Office may deny a request if the Sheriff's Office determines that there is a compelling reason that inspection would interfere with an active investigation. If the agency denies access, the Sheriff must provide a prompt, written denial to the individual who requested the data with a short description of the compelling reason access was denied and must provide notice that relief may be sought from the district court pursuant to § 13.82 Subd. 7.

See the Officer-Involved Shootings and Deaths Policy regarding BWC media requests pursuant to Minn. Stat. § 13.825 relating to deaths by use of force.

#### **433.8 RETENTION OF BWC MEDIA**

All BWC media should be retained in accordance with state records retention laws but in no event for a period less than 90 days (Minn. Stat. § 13.825).

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 Sheriff or the authorized designee.

If an individual captured on BWC media submits a written request, the BWC media pertaining to that subject shall be retained for an additional time period requested by the subject of up to 180 days. The Sheriff's Office will notify the requestor at the time of the request that the data will then be

destroyed unless a new written request is received. The BWC coordinator should be responsible for notifying the individual prior to destruction of the BWC media (Minn. Stat. § 13.825).

The following categories of BWC data shall be retained for a minimum period of one year:

- (a) any reportable firearms discharge;
- (b) any use-of-force by a deputy that results in substantial bodily harm;
- (c) any incident that results in a formal complaint against a deputy.

Members shall not alter, erase, or destroy any BWC media, before the end of the applicable retention period (Minn. Stat. § 626.8473).

#### **433.8.1 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 office 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 Evidence Room Policy).

Evidentiary BWC media that documents a deputy's use of deadly force must be maintained indefinitely (Minn. Stat. § 13.825; Minn. Stat. § 626.8473).

### **433.9 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.

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.

#### **433.10 US MARSHAL FUGITIVE TASK FORCE MEMBERS**

The Carlton County Sheriff's Office may have employees working as members of the US Marshal Service (USMS) Fugitive Task Force. Any employee deputized as a US Marshal working on a task force approved assignment must follow the USMS rules related to the use of portable recording systems.

#### **433.11 DRUG ENFORCEMENT AGENCY TASK FORCE MEMBERS**

The Carlton County Sheriff's Office may have employees working as members of the Drug Enforcement Agency (DEA) Task Force. Any employee deputized as a DEA task force member

working on a task force approved assignment must follow the DEA rules related to the use of portable recording systems.