



INDEPENDENT AUDITOR'S REPORT

Roseau County Sheriff's Office



NOVEMBER 25TH, 2025
RAMPART AUDIT LLC

Audit Overview and Recommendations

Dear Roseau County Board and Sheriff Gust:

We have audited the body-worn camera (BWC) program of the Roseau County Sheriff's Office (RCSO) for the two-year period ended 3/31/2025. Minnesota Statute §13.825 mandates that any law enforcement agency operating a portable recording system (PRS)¹ program obtain an independent, biennial audit of its program. This program and its associated data are the responsibility of the Roseau County Sheriff's Office. Our responsibility is to express an opinion on the operations of this program based on our audit.

On August 7, 2025, Rampart Audit, LLC (Rampart) met with Sgt. Logan Bender, who provided information about RCSO'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 RCSO's recordkeeping.

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

RCSO 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.

Rampart has previously audited RCSO's BWC program in 2021 and 2023. As part of the 2021 audit, we were advised that RCSO implemented its body-worn camera program in 2011, prior to the adoption of Minn. Stat. §626.8473. While RCSO's BWC policy was available on its website at the time of our 2021 audit, RCSO personnel indicated that the public comment requirements had most likely not been met. Because Minnesota Statute §626.8473 did not address pre-existing BWC programs, Rampart recommended RCSO suspend use of its BWC program until those requirements could be satisfied.

Prior to the issuance of our 2021 audit report, RCSO personnel submitted documentation to Rampart showing that RCSO had posted a public notice soliciting comments about its BWC program and policy, and that the Roseau County Board had provided an opportunity for public comment at its regularly

¹ 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 RCSO, these terms may be used interchangeably in this report.

scheduled meeting on May 25, 2021. The board then adopted the RCSO BWC program and policy at that same meeting. Once this was complete, RCSO re-implemented their BWC program.

Copies of these documents have been retained in Rampart's audit files. In our opinion, Roseau County Sheriff's Office is compliant with the requirements of §626.8473 Subd. 2.

Minn. Stat. §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."

The Rampart auditor verified that there was a working link to RCSO's BWC policy on the Sheriff's Office page of the Roseau County website at the time of the audit. In our opinion, RCSO is compliant with the requirements of §626.8473 Subd. 3(a).

RCSO BWC WRITTEN POLICY

As part of this audit, we reviewed RCSO'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 RCSO 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.

RCSO 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.

RCSO currently follows the General Records Retention Schedule for Minnesota Cities (GRRSMC), but also addresses the categories listed above separately within its BWC policy:

Part A of the Data Retention section of RCSO's BWC policy states: "All BWC data shall be retained for a minimum period of 90 days. There are no exceptions for erroneously recorded or non-evidentiary data," which satisfies the requirements of §13.825 Subd. 3(a).

Part B of the Data Retention section of RCSO's BWC policy specifies a minimum retention period of one year for "[d]ata documenting 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..." Part C of the Data Retention section of RCSO's BWC policy specifies a minimum retention period of six years for "[d]ata that documents the use of deadly force by a peace officer, or force of a sufficient type or degree to require a use of force report or supervisory review," as well as, "[d]ata documenting circumstances that have given rise to a formal complaint against an officer."

While Part C identifies "force of a sufficient type or degree to require a use of force report or supervisory review" as the threshold to prompt extended BWC retention rather than the "substantial bodily harm" threshold described in statute, it is our opinion that RCSO's BWC policy establishes a broader standard for retention that will result in additional BWC being subject to extended retention. In our opinion, the retention periods identified in Parts B and C of RCSO's BWC policy meet or exceed the requirements of §13.825 Subd. 3(b).

As stated in the preceding paragraphs, Part C of the Retention section of RCSO's BWC policy specifies a minimum retention period of six years for "[d]ata that documents the use of deadly force by a peace officer..." Because §13.825 Subd. 3(c) requires that such BWC data be retained indefinitely, RCSO's BWC policy is not compliant with this requirement.

Prior to the issuance of this report, RCSO submitted a revised BWC policy that states: "Evidentiary BWC media that documents a deputy's use of deadly force must be maintained indefinitely." A copy of the updated policy has been attached to this report as Appendix B.

Part F of the Data Retention section of RCSO's BWC policy states: "Upon written request by a BWC data subject, the agency shall retain a recording pertaining to that subject for an additional time period requested by the subject of up to 180 days..." This satisfies the requirements of §13.825 Subd. 3(d).

Part C of the Data Security Safeguards section of RCSO's BWC policy states: "[o]fficers shall not intentionally edit, alter, or erase any BWC recording unless otherwise expressly authorized by the Sheriff or the Sheriff's designee." As discussed in Clause 2 of the Policy section of this report, a BWC policy must prohibit altering, erasing or destroying any recording made with a peace officer's portable recording system, as well as associated data or metadata, prior to the expiration of the applicable retention period. In our opinion, the language described above does not satisfy this requirement.

Prior to the issuance of this report, RCSO submitted a revised BWC policy that addresses the retention issues noted in the preceding paragraph. We noted, however, that a conflict exists between the Retention of BWC Media section of the policy, which states unequivocally that: "Members shall not alter, erase, or destroy any BWC media, before the end of the applicable retention period," and the BWC Media section of the policy, which states: "Members shall not alter, copy, delete, release, or permit access to BWC media other than as permitted in this policy without the express consent of the Sheriff or the authorized designee." We recommend that RCSO remove this passage from their policy to avoid confusion.

RCSO employs Motorola body-worn cameras. BWC data are stored on WatchGuard's² Evidence Library Cloud-based storage service, with retention managed through automated settings in the CommandCentral 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. Sgt. Bender advised us that in the event a deputy fails to assign a category to a BWC recording, the default retention period is one year to avoid the accidental loss of data.

The Downloading and Labeling Data section of RCSO's BWC policy requires that each deputy "using a BWC is responsible for transferring or assuring the proper transfer of the data from his or her camera to the secure server by the end of that [deputy's] shift." As part of this process, the deputy assigns 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.

Sgt. Bender advised us that RCSO also has a legacy BWC server in the office containing old BWC data. In addition, some evidentiary BWC data was stored on their previous LETG RMS server with the corresponding case file.

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

RCSO BWC Data Destruction

As discussed above, RCSO's BWC data are stored on WatchGuard's cloud-based storage service, with data retention and deletion schedules managed automatically through the CommandCentral video management software based on the assigned data classification of each video.

WatchGuard 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, 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.

Sgt. Bender advised us that any RCSO in-house servers storing BWC data that are retired from service will be physically destroyed through mechanical means, specifically by grinding. We recommend noting these procedures in the written policy.

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

² Motorola Solutions, Inc. acquired WatchGuard, Inc. in 2019, and has been rebranding under the Motorola name since that time; however, many WatchGuard legacy products are still in use, and the Motorola and WatchGuard names are commonly used interchangeably.

RCSO BWC Data Access

The Access to BWC Data by non-employees subsection of the Administering Access to BWC Data section of RCSO's BWC policy states: "[o]fficers shall refer members of the media or public seeking access to BWC data to the County Coordinator and data practices responsible authority, who shall process the request in accordance with the MGDPA [Minnesota Government Data Practices Act] and other governing laws." Sgt. Bender confirmed this process during the audit, identifying the RCSO Administrative Support Specialist as the employee who receives and processes BWC data requests. All such requests are made in writing, using a Roseau County Sheriff's Office data request form. BWC data requests are fulfilled using physical media such as a DVD or USB memory device.

The Other authorized disclosures of data subsection of the Administering Access to BWC Data section of RCSO's BWC policy states: "BWC data may be shared with other law enforcement agencies only for legitimate law enforcement purposes that are documented in writing at the time of the request." All such requests must be submitted in writing to the Administrative Support Specialist. These requests are normally made via email, which creates an audit trail. Sheriff Gust or the Chief Deputy review and approve requests before processing. Requests are fulfilled via secure internet link from the Cloud storage service. Existing verbal agreements between RCSO and other area law enforcement agencies address data classification, destruction and security requirements, as specified in §13.825 Subd. 8(b).

We recommend such requests continue to be made via email or in other written form, and include a brief explanation of the law enforcement purpose for the request. A file of these requests should be maintained for audit purposes. We also recommend that RCSO obtain a written acknowledgement of the receiving agency's responsibilities under §13.825 Subd. 8(b).

The Other authorized disclosures of data subsection of the Administering Access to BWC Data section of RCSO's BWC policy states: "BWC data shall be made available to prosecutors, courts, and other criminal justice entities as provided by law." Sgt. Bender advised us that BWC disclosure requests from the Roseau County Attorney's Office follow the same process as is used by other law enforcement agencies.

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, RCSO's BWC policy did not address those requirements.

Prior to the issuance of this report, RCSO submitted a revised BWC policy that addresses the requirements discussed in the preceding paragraph. In our opinion, this revised BWC policy is compliant with respect to the applicable data access requirements.

RCSO BWC Data Classification

The Administering Access to Body Worn Camera Data section of RCSO's BWC policy states that "BWC recordings are classified as private data about the data subjects unless there is a specific law that provides differently," and identifies those circumstances in which BWC data are instead classified as either confidential or public.

As discussed in the preceding section of this report, RCSO's BWC policy does not address the requirements discussed in Clauses 5 and 6 of the Policy section of this report, which include the public classification of BWC data documenting an officer's use of deadly force.

Prior to the issuance of this report, RCSO submitted a revised BWC policy that addresses the requirements discussed in the preceding paragraph.

In our opinion, this revised policy is compliant with respect to the applicable data classification requirements.

RCSO BWC Internal Compliance Verification

The RCSO BWC Agency Use of Data section states that: "At least once a month, supervisors will randomly review BWC usage by each officer to ensure compliance with this policy..." The Compliance section of the policy further states that: "Supervisors shall monitor for compliance with this policy. The unauthorized access to or disclosure of BWC data may constitute misconduct and subject individuals to disciplinary action and criminal penalties pursuant to Minn. Stat. §13.09."

In our opinion, this fulfills the statutory requirements for supervisory review and employee discipline standards.

RCSO's BWC policy does not address the requirement that an RCSO deputy assigned a BWC wear and operate it in compliance with RCSO's BWC policy while performing law enforcement activities under the command control of another chief law enforcement officer or federal law enforcement official, as discussed in Clause 4 of the Policy section of this report.

Prior to the issuance of this report, RCSO submitted a revised BWC policy that addresses this requirement.

RCSO BWC Program and Inventory

RCSO currently possesses 13 Motorola body-worn cameras, including 11 V300 cameras and two V700 cameras. Each deputy is issued a BWC, with the remaining devices shared by jail staff.

The RCSO 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.

While RCSO does not maintain a separate log of BWC deployment or use, because each deputy wears a BWC while on duty, the number of BWC units deployed each shift can be determined based on a review of RCSO payroll records.

As of 8/07/2025, RCSO maintained 6,627 BWC videos.

RCSO BWC Physical, Technological and Procedural Safeguards

RCSO BWC data are initially recorded to a storage unit in each officer's body worn camera. Those data are then transferred via either a wireless connection or through a physical docking station to the WatchGuard Cloud service.

Deputies have view-only access to all BWC data for report writing, trial preparation and other legitimate law enforcement purposes. All such access is logged and can be reviewed by RCSO supervisors.

As discussed above, RCSO's BWC data are stored on WatchGuard's cloud-based service, with data retention and deletion schedules managed automatically through the Evidence Library video management software based on the assigned data classification of each video.

As noted above, requests by other law enforcement agencies for RCSO BWC data must be approved by Sheriff Gust or the Chief Deputy.

RCSO's BWC policy does not address the requirement described in Clause 3 of the Policy section of this report, which mandates that a BWC policy specify that a BWC be worn at or above the mid-line of the waist. Prior to the submission of this report, RCSO furnished a revised BWC policy that satisfies this requirement.

Enhanced Surveillance Technology

RCSO 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 RCSO 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

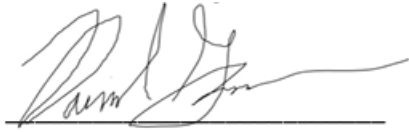
Rampart selected a random sample of 132 calls for service from which to review any available BWC recordings. It should be noted that not every call will result in an officer activating his or her BWC. For example, an officer who responds to a driving complaint but is unable to locate the suspect vehicle 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 auditors reviewed the retained BWC videos to verify that this data was accurately documented in RCSO records.

The Rampart auditor noted that while BWC recordings in our sample were retained properly, labeling was inconsistent. We recommend that RCSO administrators review labeling practices and expectations with RCSO deputies.

Rampart Audit, LLC

Audit Conclusions

In our opinion, the Roseau County Sheriff's Office's Body-Worn Camera Program is substantially compliant with Minnesota Statute §13.825.

A handwritten signature in black ink, appearing to read "Paul J. [unclear]", is written over a solid horizontal line.

Rampart Audit, LLC

11/25/2025

APPENDIX A:

Policy **424**

Roseau County Sheriff's Office

Roseau County SO Policy Manual 2025

Body-Worn Cameras

424.1 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).

424.1.1 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.

424.2 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.

424.3 RESPONSIBILITIES

424.3.1 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 Roseau 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 Roseau 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 nonpublic data by RSCO 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 Civil Process Clerk 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 Roseau County Sheriff's Office that expands the type or scope of surveillance capabilities of the office's portable recorders.

424.3.2 MEMBER RESPONSIBILITIES

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

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

424.4 BWC USE

The following guidelines apply to the use of BWCs:

- (a) Only office-issued BWCs should be used without the express consent of the Sheriff or the authorized designee (Minn. Stat. § 13.825).
- (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.

424.4.1 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.

424.5 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.

424.5.1 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.

424.5.2 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.

424.5.3 LIVESTREAMING

Livestreaming enables authorized individuals to remotely view the audio and video captured by a member's BWC in real time. Only supervisors and [dispatcher]s 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.

424.5.4 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.

424.6 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.

424.6.1 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.

424.7 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 without the express consent of the Sheriff or the authorized designee.

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

424.7.1 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 Sheriff is permitted to access and view BWC media for training purposes.
 - 1. The Sheriff 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 Sheriff may use BWC media for training purposes with the approval of the Sheriff or the authorized designee. The Sheriff 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 Civil Process Clerk may access BWC media when necessary to conduct officer-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 (see the Standards of Conduct and the Protected Information policies for additional guidance) (Minn. Stat. § 626.8473).

424.7.2 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 Civil Process Clerk should review BWC media before public release.

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.

424.8 RETENTION OF BWC MEDIA

Non-evidentiary 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 shall be retained for an additional time period. The BWC coordinator should be responsible for notifying the individual prior to destruction of the BWC media (Minn. Stat. § 13.825).

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

424.8.1 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).

424.9 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.

APPENDIX B:

Policy
424

Roseau County Sheriffs Office

Roseau County SO Policy Manual 2025

Body-Worn Cameras

424.1 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).

424.1.1 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.

424.2 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.

424.3 RESPONSIBILITIES

424.3.1 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 Roseau 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 Roseau 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 RCSO members and members of other governmental entities and agencies for a legitimate, specified law enforcement purpose (Minn. Stat. § 13.825, Subd. 7; Minn. Stat. § 13.825, Subd. 8).
- (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) (Minn. Stat. § 626.8473, Subd. 3).
 - 2. Gain insight into community expectations regarding BWC use.
- (i) Coordinating with the Civil Process Clerk 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) (Minn. Stat. § 13.825, Subd. 3).
 - 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.).
- U) Coordinating with the Evidence Room to develop procedures for the transfer, storage, and backup of evidentiary BWC media (see the Evidence Room Policy).
- (k) Completing an annual administrative review of the BWC program and providing it to the Sheriff for review.
- (l) Preparing the biennial audit required by Minn. Stat. § 13.825, Subd. 9.
- (m) Notifying the Bureau of Criminal Apprehension (BCA) in a timely manner when new equipment is obtained by the Roseau County Sheriff's Office that expands the type or scope of surveillance capabilities of the office's portable recorders (Minn. Stat. § 13.825, Subd. 10).

424.3.2 MEMBER RESPONSIBILITIES

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

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

424.4 BWC USE

The following guidelines apply to the use of BWCs:

- (a) Only office-issued BWCs should be used (Minn. Stat. § 13.825, Subd. 6).
- (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.

424.4.1 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.

424.5 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.

424.5.1 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.

424.5.2 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.

424.5.3 LIVESTREAMING

Livestreaming enables authorized individuals to remotely view the audio and video captured by a member's BWC in real time. Only supervisors and [dispatcher)s 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.

424.5.4 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.

424.6 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.

424.6.1 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.

424.7 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 without the express consent of the Sheriff or the authorized designee.

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

424.7.1 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 Sheriff is permitted to access and view BWC media for training purposes.
 - 1. The Sheriff 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 Sheriff may use BWC media for training purposes with the approval of the Sheriff or the authorized designee. The Sheriff 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 Civil Process Clerk 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 (see the Standards of Conduct and the Protected Information policies for additional guidance) (Minn. Stat. § 626.8473, Subd. 3).
- U) Members may be subject to criminal penalties for the misuse of BWC media pursuant to Minn. Stat. § 13.09 (Minn. Stat. § 626.8473, Subd. 3).

424.7.2 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; Minn. Stat. § 13.825, Subd. 4).
- (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.

424.7.3 ACCESS BY OTHER LAW ENFORCEMENT AGENCIES AND GOVERNMENT ENTITIES

Other law enforcement agencies and government entities (e.g., prosecutors, criminal justice agencies) may obtain access to not public BWC media for a legitimate, specified law enforcement purpose upon written authorization from the Sheriff or the authorized designee and pursuant to office protocols (Minn. Stat. § 13.825, Subd. 8).

424.7.4 ACCESS BY PERSONS CAPTURED ON BWC MEDIA

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 unless otherwise provided by law. 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).

424.7.5 ACCESS TO BWC MEDIA USED IN COLLISION INVESTIGATIONS

Individuals shall be provided with unredacted BWC media used in a collision investigation if the individual (Minn. Stat. § 13.825, Subd. 4):

- (a) Is entitled to a collision report under Minn. Stat. § 169.09
- (b) Submits a written request accompanied by the related collision report

The Office may deny access to unredacted data as provided in Minn. Stat. § 13.825, Subd. 4.

424.7.6 BWC MEDIA REGARDING USE OF FORCE INCIDENTS RESULTING IN DEATH

When a person dies as a result of the use of force by a deputy, the Office shall (Minn. Stat. §

13.825, Subd. 2; Minn. Stat. § 626.8473, Subd. 3):

- (a) Allow certain individuals as identified in Minn. Stat. § 13.825, upon request, to inspect all portable recording system data that documents the incident within five days of the request pursuant to the provisions of Minn. Stat. § 13.825.
- (b) Release all portable recording system data that documents the incident within 14 days of the incident pursuant to the provisions of Minn. Stat. § 13.825.

424.7.7 DENIALS, REDACTIONS, AND NOTICES

Requests for the release of BWC media shall be processed in accordance with the Records Maintenance and Release Policy. The Civil Process Clerk should review BWC media before public release.

The Sheriff should work with the Custodian of Records when redactions, denials, or notices (e.g., reason for denial, potential penalties for misuse, seeking court relief) are necessary (Minn. Stat.

§ 13.825, Subd. 2; Minn. Stat. § 13.825, Subd. 4; Minn. Stat. § 626.8473, Subd. 3).

424.8 RETENTION OF BWC MEDIA

Non-evidentiary 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 shall be retained for an additional time period up to 180 days. The BWC coordinator should be responsible for notifying the individual that the BWC media will then be destroyed unless a new request is made (Minn. Stat. § 13.825, Subd. 3).

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

424.8.1 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).

424.8.2 EVIDENTIARY RETENTION REQUIREMENTS

BWC media documenting the following incidents must be retained for a minimum of one year and destroyed according to the office's records retention schedule (Minn. Stat. § 13.825, Subd.

3):

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

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

424.9 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.