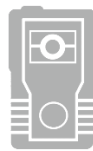




INDEPENDENT AUDITOR'S REPORT

Sherburne County Sheriff's Office



OCTOBER 6TH, 2026
RAMPART AUDIT LLC

Audit Overview and Recommendations

Dear Sherburne County Board and Sheriff Brott:

We have audited the body-worn camera (BWC) program of the Sherburne County Sheriff's Office (SCSO) for the two-year period ended 7/31/2026. 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 Sherburne County Sheriff's Office. Our responsibility is to express an opinion on the operations of this program based on our audit.

On August 28, 2026, Rampart Audit, LLC (Rampart) met with Chief Deputy Steve Doran, Captain Ryan Broich and Information Services Director Matt Albrecht, who provided information about SCSO'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 SCSO's recordkeeping.

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

SCSO 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 previously audited the Sherburne County Sheriff's Office's BWC program in 2022 and 2024. During our first audit, Chief Deputy Doran provided documentation showing that the public notification, comment and meeting requirements had been satisfied prior to the implementation of SCSO's BWC program on August 31, 2018. Specifically, Chief Deputy Doran furnished the following:

- A copy of the minutes of the May 1, 2018, Sherburne County Board meeting, which noted that a public hearing would be held on May 22, 2018, for the purpose of considering SCSO's new body-worn camera policy; and

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 SCSO, these terms may be used interchangeably in this report.

- A copy of the minutes for the May 22, 2018, Sherburne County Board meeting, which noted that a public hearing was opened for the purpose of obtaining public input and addressing any questions, issues, concerns or other items related to SCSO's proposed BWC policy.

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

In our opinion, the Sherburne County Sheriff's Office met the requirements of §626.8473 Subd. 2 prior to the implementation of its BWC program.

Minnesota Statute §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 staff noted that while there was a link to the Sherburne County Sheriff's Office's BWC policy on their webpage, it was nonfunctional at the time of our audit. The policy has been accessible during previous audits, and SCSO personnel advised us that the website was undergoing updates and the policy would be restored once the updates were complete. Prior to the completion of this report, SCSO personnel advised us that the updates had been completed. We verified that the policy was once again accessible on their website. In our opinion, the Sherburne County Sheriff's Office is compliant with the requirements of §626.8473 Subd. 3(a) as of the date of this report.

SCSO BWC WRITTEN POLICY

As part of this audit, we reviewed SCSO'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 SCSO 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 were added as a result of 2023 legislation and will also be discussed separately below.

SCSO 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.

The Sherburne County Sheriff's Office follows the General Records Retention Schedule for Minnesota Counties with respect to data having evidentiary value; however, SCSO's BWC policy also specifically addresses the itemized retention requirements listed in Minn. Stat. §13.825 Subd. 3.

Clause (a) of the Data Retention section of SCSO's BWC policy states that "BWC data shall be maintained for a minimum period of 90 days." This satisfies the 90-day minimum retention period established in Minn. Stat. §13.825 Subd. 3(a).

Clause (c) of the Data Retention section of SCSO's BWC policy specifies a minimum retention period of one year for data documenting a reportable firearms discharge, while Clause (d) specifies indefinite retention for data documenting "circumstances that have given rise to a formal complaint against a deputy," as well as data documenting "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." In our opinion, these retention periods meet or exceed the requirements of §13.825 Subd. 3(b) and (c).

Clause (e) of the Data Retention section of SCSO's BWC policy addresses the requirement contained in Minn. Stat. §13.825 Subd. 3(d) that an agency retain BWC recordings for an additional period of up to 180 days when so requested in writing by a data subject.

Clause (k) of the Data Retention section of SCSO's BWC policy states that:

All office members are prohibited from altering, erasing, or destroying any recording made with a deputy's portable recording system or data and metadata related to the recording prior to the expiration of the applicable retention period under section 13.825, subdivision 3, except that the full, unedited, and unredacted recording of a deputy using deadly force must be maintained indefinitely.

In our opinion, this satisfies the requirement described in Clause 2 of the Policy section of this report.

SCSO employs Motorola body-worn cameras and manages BWC data retention using a combination of their own secure servers and Motorola's cloud-based storage service through automated retention settings in the Motorola EL (Evidence Library) Cloud DEMS (digital evidence management system) 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.

SCSO's BWC policy requires that each deputy transfer data from his or her body-worn camera to the 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. BWCs can be docked either in the deputy's squad or in a docking station at the Sheriff's Office.

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

SCSO BWC Data Destruction

As noted above, SCSO personnel advised us that SCSO BWC data are stored on both in-house servers and Motorola's cloud-based storage service. Chief Deputy Doran advised us that since March 7, 2026, all new BWC data has been stored exclusively to the cloud. BWC data created prior to that date are currently stored on the in-house servers; however, that legacy data will be migrated to cloud-based storage later this year.

Data are destroyed through automated deletion and overwriting, based on a retention schedule assigned to each video. In addition, at the time it is retired from service, any SCSO-owned physical hard drive used to store BWC data will have all data deleted prior to being destroyed by physical means with a hard drive punch.

Motorola describes its Evidence Library cloud service as CJIS compliant and notes that the service is routinely and automatically updated to maintain compliance.

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, SCSO's written BWC policy is compliant with respect to the applicable data destruction requirements.

SCSO BWC Data Access

All requests for access to BWC data by data subjects or the media are made in writing to the SCSO Records Management Department, using SCSO's data disclosure form. The chief deputy reviews each request and, if approved, Records staff are then responsible for fulfilling the request in accordance with the provisions of §13.825 Subd. 4(b).

The Administering Access to BWC Data section of SCSO'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 disclosure." The same section also states that: "BWC data shall be made available to prosecutors, courts, and other criminal justice entities as provided by law."

BWC data requests from other law enforcement agencies are submitted to the SCSO Records Management Department via email. These requests are reviewed by the chief deputy and, if approved, are processed by Records staff. Data are then shared through secure internet link via DEMS. As part of the audit, Chief Deputy Doran provided a copy of the written reminder SCSO includes each time it shares BWC data with another law enforcement agency of that receiving agency's responsibilities under Minn. Stat. §13.825 Subd. 7. Rampart recommends this practice.

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. SCSO has addressed these requirements in Clause (c) of the Access to BWC Data by Non-Employees section of its BWC policy.

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

SCSO BWC Data Classification

The Administering Access to BWC Data section of SCSO's BWC policy defines data subjects and notes that "BWC data is presumptively private." The policy also identifies types of BWC data that are confidential, as well as types that are public. As noted in the preceding section of this report, SCSO has added language to address the changes the Minnesota State Legislature made in 2023 regarding BWC data documenting incidents involving the use of deadly force.

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

SCSO BWC Internal Compliance Verification

The Compliance section of the SCSO BWC policy states that "[s]upervisors 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." The Agency Use of Data section of the SCSO BWC policy states that "[a]t least once a month, supervisors will randomly review BWC usage by each deputy to ensure compliance with this policy." Chief Deputy Doran confirmed that each supervisor reviews a random selection of three (3) BWC videos for each of his or her direct reports every month to verify compliance. This includes a review of the sergeants' BWC usage by the captain. All access is also logged in the BWC data management software, and supervisors maintain an Excel log as well for easy verification. The Agency Use of Data section further notes that:

Each time a BWC video is reviewed within the WatchGuard² [system], the employee shall note the reason why for auditing purposes. Until the WatchGuard system is updated to include a data field for this purpose, employees shall document the reason for viewing in the comment section of the call in ProPhoenix RMS.

The Policy section of SCSO's BWC policy states that "[i]t is the policy of this office to authorize and require the use of department-issued BWCs as set forth below, and to administer BWC data as provided by law." The Use and Documentation section states that "[d]eputies may use only department-issued BWCs in the performance of official duties for this agency or when otherwise performing authorized law enforcement services as an employee of this office."

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. SCSO addresses this requirement in Clause (h) of the General Guidelines for Recording section of its BWC policy.

As noted above, SCSO's BWC policy addresses consequences associated with violations of the policy, to include both disciplinary action and potential criminal penalties.

² Motorola acquired Watchguard in 2019. While rebranding under the Motorola name appears largely complete, the names are still used interchangeably at times.

In our opinion, SCSO's BWC policy is compliant with respect to the compliance and disciplinary requirements contained in §626.8473 Subd. 3(b)(8).

SCSO BWC Program and Inventory

SCSO currently possesses 234 Motorola V700 body-worn cameras, of which 94 are assigned to licensed staff and the remaining 140 are assigned to jail staff³.

The SCSO 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.

Clause (g) of the General Guidelines for Recording section of SCSO's BWC policy states: "BWC's must be worn at or above the mid-line between the waist and the neck in a position that maximizes the recording system's capacity to record video footage of the deputy's activities," as discussed in Clause 3 of the Policy section of this report.

Chief Deputy Doran 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 in real time based on the Motorola GPS function, while a count can be determined after the fact based on a review of SCSO 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 the date of the audit, SCSO maintained 94.6293 TB of BWC data recorded by deputies.

SCSO BWC Physical, Technological and Procedural Safeguards

SCSO BWC data are initially recorded to an internal hard drive in each deputy's BWC. Those files are then uploaded to Motorola's cloud-based storage service once the BWC is docked either in the deputy's squad, or in a docking station located at the SCSO office.

Deputies have view-only access to their own data for report writing, trial preparation, data administration, investigatory purposes and other legitimate law enforcement purposes.

As noted above, requests by other law enforcement agencies for SCSO BWC data must be submitted to the Records Department and are fulfilled via secure internet link. A similar method is employed to submit SCSO BWC data to prosecutors.

³ Minn. Stat. §13.825 Subd. 1(b)(1) defines Portable Recording System as "a device worn by a peace officer..." Because Sherburne County jail staff are not licensed peace officers, their policies, procedures and data are not addressed in this audit.

Enhanced Surveillance Technology

SCSO 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 SCSO 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 (CFS) from which to review any available BWC recordings created by sworn personnel. 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 SCSO records.

Audit Conclusions

In our opinion, the Sherburne County Sheriff's Office's Body-Worn Camera Program is compliant with Minnesota Statutes §13.825 and §626.8473.

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

Rampart Audit, LLC

10/06/2026

APPENDIX A:

[Auditor note: logo did not transfer]	SHERBURNE COUNTY SHERIFF'S OFFICE <i>SHERIFF'S OFFICE POLICY AND PROCEDURE MANUAL</i>	703
		Revised: 08/14/2026
Title: USE OF BODY-WORN CAMERAS		Pages: 8

703.1 PURPOSE AND SCOPE

The primary purpose of using body-worn-cameras (BWCs) is to capture evidence arising from police- citizen encounters. This policy sets forth guidelines governing the use of BWCs and administering the resulting data. Compliance with these guidelines is mandatory, but it is recognized that deputies must also attend to other primary duties and the safety of all concerned, sometimes in circumstances that are tense, uncertain, and rapidly evolving.

This policy governs the use of BWCs in the course of official duties. It does not apply to the use of squad-based (dash-cam) recording systems. The sheriff or sheriff's designee may supersede this policy by providing specific instructions for BWC use to individual deputies, or providing specific instructions pertaining to particular events or classes of events, including but not limited to political rallies and demonstrations. The sheriff or designee may also provide specific instructions or standard operating procedures for BWC use to deputies assigned to specialized details, such as carrying out duties in courts, guarding prisoners or patients in hospitals and mental health facilities, or in the performance of undercover operations or while working with confidential informants and/or persons providing confidential information, and in the performance of tactical operations.

703.2 POLICY

It is the policy of this office to authorize and require the use of department-issued BWCs as set forth below, and to administer BWC data as provided by law.

703.3 DEFINITIONS OF PHRASES USED IN THIS POLICY

MGDPA or Data Practices Act - Refers to the Minnesota Government Data Practices Act, Minn. Stat.

§ 13.01, et seq.

Records Retention Schedule - Refers to the General Records Retention Schedule for Minnesota Counties.

Law Enforcement-Related Information - Information captured or available for capture by use of a BWC that has evidentiary value because it documents events with respect to a stop, arrest, search, citation, or charging decision.

Evidentiary Value - The information may be useful as proof in a criminal prosecution, related civil or administrative proceeding, further investigation of an actual or suspected criminal act, or in considering an allegation against a law enforcement agency or deputy.

General Citizen Contact - An informal encounter with a citizen that is not and does not become law enforcement-related or adversarial, and a recording of the event would not yield information relevant to an ongoing investigation. Examples include, but are not limited to, assisting a motorist with directions, summoning a wrecker, or receiving generalized concerns from a citizen about crime trends in his or her neighborhood.

Adversarial - A law enforcement encounter with a person that becomes confrontational, during which at least one person expresses anger, resentment, or hostility toward the other, or at least one person

directs toward the other verbal conduct consisting of arguing, threatening, challenging, swearing, yelling, or shouting. Encounters in which a citizen demands to be recorded or initiates recording on his or her own are deemed adversarial.

Unintentionally Recorded Footage - A video recording resulting from a deputy's inadvertence or neglect in operating the officer's BWC, provided that no portion of the resulting recording has evidentiary value. Examples of unintentionally recorded footage include, but are not limited to, recordings made in station house locker rooms, restrooms, and recordings made while deputies were engaged in conversations of a non-business, personal nature with the expectation that the conversation

was not being recorded.

Test Recording Footage - A momentarily check of the BWC system conducted by a deputy to ensure the system is functioning correctly.

Official Duties - For purposes of this policy, means that the deputy is on duty and performing authorized law enforcement services on behalf of this office.

703.4 USE AND DOCUMENTATION

- (a) Deputies may use only department-issued BWCs in the performance of official duties for this agency or when otherwise performing authorized law enforcement services as an employee of this office.
- (b) Deputies who have been issued BWCs shall operate and use them consistent with this policy. Deputies shall make sure their BWC is working properly at the beginning of each shift. Deputies noting a malfunction shall promptly report the malfunction to the deputy's supervisor and shall document the malfunction with an ICR. Supervisors shall take prompt action to address malfunctions and document the steps taken in the ICR.
- (c) Deputies must document BWC use and non-use as follows:
 - 1. Whenever a deputy makes a recording, the existence of the recording shall be documented in an incident report if a case is generated or in the CAD notes if only a call is generated.
 - 2. Whenever a deputy fails to record an activity that is required to be recorded under this policy or captures only a part of the activity, the deputy must document the circumstances and reasons for not recording in a supplement report to the original ICR if a case is generated, or in the CAD notes if only a call is generated. Supervisors shall review these reports and initiate any corrective action deemed necessary.
- (d) The sheriff's office will maintain the following records and documents relating to BWC use, which are classified as public data:
 - 1. The total number of BWCs owned or maintained by the agency;
 - 2. A daily record of the total number of BWCs actually deployed and used by deputies;
 - 3. The total amount of recorded BWC data collected and maintained; and
 - 4. This policy, together with the Records Retention Schedule.

703.5 GENERAL GUIDELINES FOR RECORDING

- (a) Deputies shall activate their BWCs when anticipating that they will be involved in, become involved in, or witness other officers of this agency involved in a pursuit, *Terry* stop of a motorist or pedestrian, search, seizure, arrest, use of force, adversarial contact, and during other activities likely to yield information having evidentiary value. However, officers need not activate their cameras when it would be unsafe, impossible, or impractical to do so, but such instances of not recording when otherwise required must be documented as specified in the Use and Documentation guidelines, part 703.4(d)(2).
- (b) Deputies have discretion to record or not record general citizen contacts.
- (c) Deputies have no affirmative duty to inform people that a BWC is being operated or that the individuals are being recorded.

- (d) Once activated, the BWC should continue recording until the conclusion of the incident or encounter, or until it becomes apparent that additional recording is unlikely to capture information having evidentiary value. The deputy having charge of a scene shall likewise direct the discontinuance of recording when further recording is unlikely to capture additional information having evidentiary value. If the recording is discontinued while an investigation, response, or incident is ongoing, deputies shall state the reasons for ceasing the recording on camera before deactivating their BWC. If circumstances change, deputies shall reactivate their cameras as required by this policy to capture information having evidentiary value. A statement on camera such as, "Everything has settled down and the action appears to be over" should often suffice as a statement of reasons for stopping to record.
- (e) Deputies shall not intentionally block the BWC's audio or visual recording functionality to defeat the purposes of this policy, except as allowed in 703.6 (c).
- (f) Notwithstanding any other provision in this policy, deputies shall not use their BWCs to record other agency personnel during non-enforcement related activities, such as during pre- and post-shift time in locker rooms, during meal breaks, or during other private conversations, unless recording is authorized as part of an administrative or criminal investigation.
- (g) BWC's must be worn at or above the mid-line between the waist and the neck in a position that maximizes the recording system's capacity to record video footage of the deputy's activities;
- (h) Deputies must wear and operate the system in compliance with this policy while performing law enforcement activities under the command and control of another chief law enforcement officer or federal law enforcement official.

703.6 SPECIAL GUIDELINES FOR RECORDING

Deputies may, in the exercise of sound discretion, determine:

- (a) To use their BWCs to record any police-citizen encounter if there is reason to believe the recording would potentially yield information having evidentiary value, unless such recording is otherwise expressly prohibited.
- (b) To use their BWCs to take recorded statements from persons believed to be victims of and witnesses to crimes, and persons suspected of committing crimes, considering the needs of the investigation and the circumstances pertaining to the victim, witness, or suspect.
- (c) To momentarily mute the BWC microphone for the purpose of strategic consultation amongst deputies.

In addition:

- (a) Deputies need not record persons being provided medical care unless there is reason to believe the recording would document information having evidentiary value. When responding to an apparent mental health crisis or event, BWCs shall be activated as necessary to document any use of force and the basis for it, and any other information having evidentiary value, but need not be activated when doing so would serve only to record symptoms or behaviors believed to be attributable to the mental health issue.
- (b) Deputies need not use their BWC to record their transportation and the physical transfer of persons in their custody to hospitals, detox and mental health care facilities, juvenile detention centers, and jails. In-squad cameras will suffice for these types of transports. Deputies should not record with BWC's in these facilities unless the officer anticipates witnessing a criminal event or being involved in or witnessing an adversarial encounter or use-of-force incident. Deputies may want to restart BWC at the time subject is removed from the car and transferred to the custody of another.
- (c) Deputies assigned BWCs should not record interactions involving undercover officers, confidential informants, or persons providing confidential information.
- (d) Deputies assigned to specialized units, to include but not limited to the Criminal Investigation Division, Drug Task Force, Mobile Field Force and Emergency Response Unit, are not required to record the entirety of a search warrant and/or further search of a property, or when conducting field

interviews or interrogations when working in this capacity. General citizen contacts which entail follow up investigations do not require the use of BWC unless deemed to be necessary to comply with section 703.S(a) of this policy.

- (e) Deputies assigned to the Emergency Response Unit are not required to record the entirety of their deployment when unsafe, impossible or impractical to do so. Examples include but are not limited to deployment as a sniper unit on a perimeter of a scene or deployed inside of an armored vehicle at a scene.
- (f) Emergency Response Operators deploying with a sniper or in a sniper capacity are not required to wear a BWC.

In addition, for Transport/Court Security functions:

- (a) Deputies shall activate their BWCs when responding to an assigned call for service or when handling a self-initiated call for service such as a traffic stop, walk-in complaint, or any other self-discovered activity requiring involvement or interaction.
- (b) Deputies shall not activate their BWCs within any correctional or secure detention facility.
- (c) Deputies shall not activate their BWCs in an active courtroom unless responding to a disturbance within the courtroom or taking someone into custody.
- (d) Deputies shall not activate their BWCs during the course of scheduled inmate or detainee medical appointments or medical guard details unless there is an active disturbance or hostile conduct involving the inmate or detainee.

703.7 DOWNLOADING AND LABELING DATA

- (a) Each deputy using a BWC is responsible for assuring the proper transfer of the data from his or her BWC system during his or her shift without incurring overtime. The intent is to prevent an excessive buildup of data on the BWC DVR. However, if the BWC DVR contains data that is likely to be needed immediately for an ongoing criminal investigation or is of a serious nature, the deputy shall download the data prior to the end of his or her shift.
- (b) Deputies shall categorize the BWC data files by choosing the category that best describes the event within the provided menu options at the time of video capture.
- (c) Upon a data request, Records shall forward notification of the request to the investigating deputies. Deputies shall then make an attempt to identify those persons whose image may have been captured in the BWC video footage. The identity of these persons is important in order to comply with MGDPA requirements related to data subjects. This data should be documented and added to a narrative report or CAD notes. At times it will be impractical to identify every individual at a scene, but special attention should be given to identifying the following: Victims, undercover deputies, informants, mandated reporters, juvenile witnesses (if the nature of the event or activity justifies protecting their identity) and juvenile delinquents, and individual complainants.
- (d) School Resource Officers should transfer data each week or before end of shift if data is likely to be needed immediately for an investigation or is of a serious nature.

703.8 ADMINISTERING ACCESS TO BWC DATA

- (a) **Data subjects.** Under Minnesota law, the following are considered data subjects for purposes of administering access to BWC data:
 - 1. Any person or entity whose image or voice is documented in the data.
 - 2. The deputy who collected the data.
 - 3. Any other deputy whose voice or image is documented in the data, regardless of whether that deputy is or can be identified by the recording.
- (b) **BWC data is presumptively private.** BWC recordings are classified as private data about the data subjects unless there is a specific law that provides differently. As a result:

1. BWC data pertaining to people is presumed private, as is BWC data pertaining to businesses or other entities.
 2. Some BWC data is classified as confidential (see c. below).
 3. Some BWC data is classified as public (see d. below).
- (c) **Confidential data.** BWC data that is collected or created as part of an active criminal investigation is confidential. This classification takes precedence over the "private" classification listed above and the "public" classifications listed below.
- (d) **Public data.** The following BWC data is public:
1. After an investigation is complete, BWC data are public if they document the discharge of a firearm by a peace officer in the course of duty, other than for training or the killing of an animal that is sick, injured, or dangerous.
 2. After an investigation is complete, BWC data are public if they document the use of force by a peace officer that result in substantial bodily harm.
 3. Data that a data subject requests to be made accessible to the public, subject to redaction. Data on any data subject (other than a peace officer) who has not consented to the public release must be redacted *[if practicable]*. In addition, any data on undercover deputies must be redacted.
 4. Data that documents the final disposition of a disciplinary action against a public employee.

However, if another provision of the Data Practices Act classifies data as private or otherwise not public, the data retains that other classification. For instance, data that reveals protected identities under Minn. Stat. § 13.82, subd. 17 (e.g., certain victims, witnesses, and others) should not be released even if it would otherwise fit into one of the public categories listed above.

703.8.1 ACCESS TO BWC DATA BY NON-EMPLOYEES

Deputies shall refer members of the media or public seeking access to BWC data to the records supervisor who shall process the request in accordance with the MGDPA and other governing laws. In particular:

- (a) An individual shall be allowed to review recorded BWC data about him- or herself and other data subjects in the recording, but access shall not be granted:
1. If the data was collected or created as part of an active investigation.
 2. To portions of the data that the agency would otherwise be prohibited by law from disclosing to the person seeking access, such as portions that would reveal identities protected by Minn. Stat. § 13.82, subd. 17.
- (b) Unless the data is part of an active investigation, an individual data subject shall be provided with a copy of the recording upon request, but subject to the following guidelines on redaction:
1. Data on other individuals in the recording who do not consent to the release must be redacted.
 2. Data that would identify undercover deputies must be redacted.
 3. Data on other deputies who are not undercover, and who are on duty and engaged in the performance of official duties, may not be redacted.
 4. Data that would identify confidential informants or persons providing confidential information must be redacted.
- (c) Access when death by use of force
1. Notwithstanding any law to the contrary, when an individual dies as a result of a use of force by a deputy, the SCSO must allow the following individuals, 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, except as otherwise provided in this section (1) and (2):
 - i. The deceased individual's next of kin;
 - ii. The legal representative of the deceased individual's next of kin; and
 - iii. The other parent of the deceased individual's child.

2. When an individual dies as a result of a use of force by a deputy, the SCSO shall release all portable recording system data, redacted no more than what is 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 case the data remain classified by section 13.82, subdivision 7.

703.8.2 ACCESS BY PEACE OFFICERS AND LAW ENFORCEMENT EMPLOYEES

No employee may have access to the department's BWC data except for legitimate law enforcement or data administration purposes:

- (a) Deputies may access and view stored BWC video only when there is a business need for doing so, including the need to defend against an allegation of misconduct or substandard performance. Officers may review video footage of an incident in which they were involved prior to preparing a report, giving a statement, or providing testimony about the incident.
- (b) Agency personnel are prohibited from accessing BWC data for non-business reasons and from sharing the data for non-law enforcement related purposes, including but not limited to uploading BWC data recorded or maintained by this agency to public and social media websites.
- (c) Employees seeking access to BWC data for non-business reasons may make a request for it in the same manner as any member of the public.

703.8.3 OTHER AUTHORIZED DISCLOSURES OF DATA

Deputies may display portions of BWC footage to witnesses as necessary for purposes of investigation as allowed by Minn. Stat. § 13.82, subd. 15, as may be amended from time to time. Deputies should generally limit these displays in order to protect against the incidental disclosure of individuals whose identities are not public. Protecting against incidental disclosure could involve, for instance, showing only a portion of the video, showing only screen shots, muting the audio, or playing the audio but not displaying video.

In addition:

- (a) 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 disclosure.
- (b) BWC data shall be made available to prosecutors, courts, and other criminal justice entities as provided by law.

703.9 DATA SECURITY SAFEGUARDS

The Sherburne County Sheriff's Office IS will provide storage designed to back up all recordings.

- (a) Personally owned devices, including but not limited to computers and mobile devices, shall not be programmed or used to access or view agency BWC data.
- (b) Deputies shall not intentionally edit, copy, alter, or erase any BWC recording unless otherwise expressly authorized by the sheriff or the sheriff's designee.
- (c) As required by Minn. Stat. § 13.825, subd. 9, as may be amended from time to time, this office shall obtain an independent biennial audit of its BWC program.
- (d) Server destruction is accomplished via a Formax FD87H Hard Drive Punch.

703.10 AGENCY USE OF DATA

- (a) Each time a BWC video is reviewed within the WatchGuard, the employee shall note the reason why for auditing purposes. Until the WatchGuard system is updated to include a data field for this purpose, employees shall document the reason for viewing in the comment section of the call in ProPhoenix RMS (e.g. "Viewed BWC for monthly audit," "Viewed BWC for report writing purposes," etc). If a case has more than one BWC video file, employees shall identify each video file reviewed and list a reason for viewing them.

- (b) At least once a month, supervisors will randomly review BWC usage by each deputy to ensure compliance with this policy.
- (c) In addition, supervisors and other assigned personnel may access BWC data for the purposes of reviewing or investigating a specific incident that has given rise to a complaint or concern about deputy misconduct or performance.
- (c) Nothing in this policy limits or prohibits the use of BWC data as evidence of misconduct or as a basis for discipline.
- (e) Deputies should contact their supervisors to discuss retaining and using BWC footage for training purposes. Deputy objections to preserving or using certain footage for training will be considered on a case-by-case basis. Field training deputies may utilize BWC data with trainees for the purpose of providing coaching and feedback on the trainees' performance.

703.11 DATA RETENTION

- (a) BWC data shall be retained for a minimum period of 90 days.
- (b) BWC data documenting or labeled as arrest, criminal investigation, death, or warrant must be maintained for a minimum period of 180 days.
- (c) Data 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, must be maintained for a minimum period of one year.
- (d) Certain kinds of BWC data must be retained for indefinitely:
 - 1. Data 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.
 - 2. Data documenting circumstances that have given rise to a formal complaint against a deputy.
- (e) When a particular recording is subject to multiple retention periods, it shall be maintained for the longest applicable period.
- (f) Subject to Part f. (below), all other BWC footage that is classified as non-evidentiary, becomes classified as non-evidentiary, or is not maintained for training shall be destroyed after 90 days.
- (g) 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. The 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.
- (h) The office shall maintain an inventory of BWC recordings having evidentiary value.
- (i) The inventory will be kept in the BWC management system.
- U) The office will post this policy, together with its Records Retention Schedule, on its website.
- (k) All office members are prohibited altering, erasing, or destroying any recording made with a deputy's portable recording system or data and metadata related to the recording prior to the expiration of the applicable retention period under section 13.825, subdivision 3, except that the full, unedited, and unredacted recording of a deputy using deadly force must be maintained indefinitely.

703.12 COMPLIANCE

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.

703.13 POST BOARD AUTHORITY

The POST board has authority to inspect SCSO policies to ensure compliance with Minn.

Stat. 626.8473. The board may conduct this inspection based upon a complaint it receives about a particular agency or through a random selection process. The board may impose licensing sanctions and seek injunctive relief under section 214.11 for failure to comply with the statute.