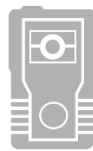




INDEPENDENT AUDITOR'S REPORT

Hubbard County Sheriff's Office



JANUARY 30TH, 2025
RAMPART AUDIT LLC

Audit Overview and Recommendations

Dear County Board of Commissioners and Sheriff Aukes:

We have audited the body-worn camera (BWC) program of the Hubbard County Sheriff's Office (HCSO) for the two-year period ended 10/31/2024. 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 HCSO. Our responsibility is to express an opinion on the operations of this program based on our audit.

On November 22, 2024, Rampart Audit LLC (Rampart) met with Sergeant Andrew Krey, who provided information about HCSO'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 HCSO's recordkeeping.

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

HCSO 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.

Sergeant Krey provided documentation showing these requirements had been met prior to the implementation of HCSO's BWC program. Specifically, Sergeant Krey provided copies of the meeting minutes and agendas of the Hubbard County Board of Commissioners Meetings dated February 15, 2022, which listed an agenda item number 2 described as "Public Input: No one was present to speak." Also listed was agenda item number 3 "PUBLIC COMMENT BODY WORN CAMERA POLICY: No one was present to speak." A copy of an affidavit of publication of the public notice was received by Rampart dated January 8, 2022 from the Park Rapids Enterprise newspaper. Also, Rampart found a public notice on the Hubbard County website noting that at a regularly scheduled meeting of 2/15/22 would be held

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

and the public could send comments electronically or come to the meeting in person with regards to the body worn camera program.

Copies of these documents have been retained in Rampart's audit files. In our opinion, HCSO met the public notice and comment requirements prior to the implementation of their BWC program on or about November 1, 2022.

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

Rampart verified that there was a working link to HCSO's BWC policy on the Police Department page of the Hubbard County Sheriff's Office website. In our opinion, HCSO is compliant with the requirements of §626.8473 Subd. 3(a).

HCSO BWC WRITTEN POLICY

As part of this audit, we reviewed HCSO'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) 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 HCSO 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.

HCSO BWC Data Retention

HCSO's BWC policy states that: "[a]ll recordings shall be retained for a period consistent with the County General Records Retention Schedule. Recordings will never be retained for a period of less than 90 days for inactive investigations. All other portable recording device data will be kept for no less than 1 year."

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. In our opinion, this portion of policy is compliant.

Minn. Stat. §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.

The HCSO's policy section 3(i) only notes: "All recordings shall be retained for a period consistent with the County General Records Retention Schedule. Recordings will never be retained for a period of less

than 90 days for inactive investigations. All other portable recording device data will be kept for no less than 1 year.”

The HCSO’s BWC policy does not meet the requirements for categories of BWC data described in §13.825 Subd. 3(b). Specifically, it does not meet the “indefinite” retention requirement for BWC data documenting deadly force incidents described in §13.825 Subd. 3(c). This requirement was created by the Minnesota State Legislature in 2023.

The HCSO Policy section 3(i) partly addresses the requirement contained in Minn. Stat. §13.825 Subd. 3(d) that an agency retain BWC recordings for an additional period when so requested in writing by a data subject, though it does not specify that such recordings be retained for up to 180 days as stated in statute. We recommend adding language to clarify the length of this additional retention period. The policy does not meet the requirements for specific one-year retention periods.

Prior to the issuance of this report, HCSO submitted a revised BWC policy that adds the required “indefinite” retention period for BWC data documenting deadly force incidents, the instances of one year retention mandates, as well as language clarifying that BWC recordings will be maintained for an additional period of 180 days when so requested by a data subject.

HCSO’s BWC policy does not address the prohibition on altering, erasing or destroying BWC data and metadata prior to its scheduled expiration date, as described in Clause 2 of the Policy section of this report. Such a prohibition is a mandatory element of BWC policies. Prior to the issuance of this report, HCSO submitted a revised BWC policy that adds this language.

HCSO currently possess 30 Motorola V300 body-worn cameras: 27 are in regular use and 3 are used as backups. HCSO utilizes Motorola’s Evidence Library (EL) Cloud Service storage and manages BWC data retention through automated retention settings in the EL video management software. The retention period for each video is determined by the data classification assigned at the time of upload; however, this retention period can be adjusted by supervisors and the office manager as needed. The preset classification auto assigns a minimum of 1 year. So, if a deputy fails to assign a data classification, the default retention period is one year. If the video is labeled “test” or “default,” the retention period is 90 days. Sergeant Krey noted that there are other labels that set retention anywhere from 1-5 years but in no case less than 90 days.

Sergeant Krey advised that the Motorola body-worn cameras utilize physical docking stations located at the HCSO, and that deputies are responsible for docking their BWC for upload to the cloud at the end of their shift.

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

HCSO BWC Data Destruction

As discussed above, HCSO utilizes Motorola’s Evidence Library for storage, with retention periods determined based on the classification assigned to BWC data. Motorola certifies that its Cloud Service is compliant with the Federal Bureau of Investigation’s Criminal Justice Information System Security Division Policy as required by Minnesota Statute §13.825 Subd. 11(b). Data destruction is achieved

through automated deletion and overwriting, with storage devices sanitized (overwritten three or more times or degaussed) or physically destroyed upon being removed from service.

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

HCSO BWC Data Access

Sergeant Krey advised us that that all requests for BWC data from the public or media are made in writing using a paper request form or an email request which goes to records management staff, which is finally submitted to the Sheriff for approval. Once approved, a DVD (redacted as necessary) is produced for the person making the request. Requests from other law enforcement agencies or prosecutor's office or probation are submitted via email to records management staff, and released through EL Cloud link. Rampart located an option for a paper mailed copy of a general government data request form as well as an email form on the Hubbard County MN website. We recommend stating the location for the public to access the data form or summarizing it within their BWC policy.

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, HCSO had not revised its BWC policy to address these requirements.

Rampart notes that many departments/offices incorporate statutory language to their policy which state that *"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. In addition, BWC data shall be made available to prosecutors, courts, and other criminal justice entities as provided by law."* Rampart recommends adding similar language to policy due to the statutory mandate to create "written procedures."

Sergeant Krey indicated that HCSO maintains verbal acknowledgments of any receiving agency's obligations under §13.825 Subd. 7 and Subd. 8, which include a requirement to maintain BWC data security. Rampart recommends obtaining written acknowledgements.

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, BPD had not addressed these new requirements. Prior to the issuance of this report, BPD submitted a revised BWC policy that added language to meet these requirements.

HCSO BWC Data Classification

HCSO's BWC Policy states that "Except as provided by MN Statute 13.825 sub. 2, audio and video recordings are considered private or non-public data. Any person captured in a recording may have access to the recording." At the time of the audit this does not meet the data classifications mandated by statute. As noted in the preceding section, prior to the issuance of this report, HCSO submitted a revised BWC policy that addresses the changes the Minnesota State Legislature made in 2023 regarding BWC data documenting incidents involving the use of deadly force. In our opinion, this revised policy is compliant with respect to the applicable data classification requirements.

HCSO BWC Internal Compliance Verification

The HCSO BWC section 3(H) states that "[H]ubbard County Sergeants will review a minimum of three random deputies body worn camera recordings each month through out calendar year," a practice that Sergeant Krey confirmed. All such reviews are logged in the EL software. Sergeant Krey advised us that EL software has an audit trail feature that allows for tracking all access.

The Policy section of HCSO's BWC policy states that "[t]he Hubbard County Sheriff's Office has implemented the use of portable recording devices, and may issue one of these devices to officers for use during the performance of their official duties." The Procedures 3(B) section states that "[d]evices shall be activated anytime it would be appropriate or valuable to record an interaction, and anytime there is personal interaction with a member of the public during a call for service."

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. HCSO's BWC policy does not address this new statutory requirement.

HCSO's written BWC policy partially addresses consequences associated with violations of the policy, to include disciplinary action. Rampart recommends adding verbiage regarding potential criminal penalties.

Prior to the issuance of this report, HCSO submitted a revised version of their BWC policy adding the language described in the preceding paragraphs. A copy of the revised policy is attached to this report as Appendix B.

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

HCSO BWC Program and Inventory

HCSO currently possesses 30 Motorola V300 body-worn cameras.

The HCSO BWC policy identifies those circumstances in which deputies are expected to activate their body-worn cameras, as well as circumstances in which they are prohibited from activating their body-

worn cameras. The policy also provides guidance for those circumstances in which BWC activation is deemed discretionary.

The Procedures 3(A) section of HCSO's BWC policy states that "[p]ortable recording devices should be worn in a conspicuous manner, or the persons being recorded should be notified whenever reasonably practicable." but does not identify that location. As discussed in Clause 3 of the Policy section of this report, the 2023 legislative changes require that an agency's BWC policy must specify that a BWC be worn at or above the mid-line of the waist. Prior to the issuance of this report, HCSO submitted a revised BWC policy that includes this requirement.

Sergeant Krey advised us that he is able to determine the number of BWCs deployed by reviewing the software and/or shift schedule.

As of the audit date, November 22, 2024, HCSO maintained 30,744 BWC data files.

HCSO BWC Physical, Technological and Procedural Safeguards

HCSO BWC data are initially recorded to a hard drive in each deputy's BWC. Data from each BWC is then uploaded to EL's Cloud Service via a physical docking station located at the Sheriff's Office. In the event a deputy fails to label the video, the default retention period is one year to avoid the accidental loss of data.

Administrators and two designated Sergeants have the ability to delete and change labels. Deputies have view only powers of their videos. All BWC data access is logged automatically and available for audit purposes.

Enhanced Surveillance Technology

HCSO currently employs BWCs with only standard audio/video recording capabilities. HCSO has 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. Their Procedure 3(G) section states "[n]otifying the MN BCA within a reasonable time period when new equipment is obtained that expands the type or scope of surveillance capabilities of the Office's portable recording device."

If HCSO 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. HCSO specifically notes that this task should fall under the responsibility of the Sheriff's Office designated coordinator.

Data Sampling

Rampart selected a random sample of 132 calls for service (CFS) 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 auditor reviewed the retained BWC videos to verify that this data was accurately documented in HCSO records.

Audit Conclusions

In our opinion, the HCSO's Body-Worn Camera Program is substantially compliant with Minnesota Statutes §13.825 and §626.8473.

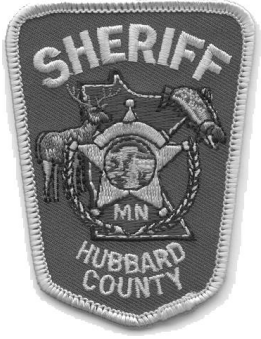
A handwritten signature in black ink, appearing to read "Rampart Audit LLC", is written over a horizontal line.

Rampart Audit LLC

1/30/2025

APPENDIX A:

Hubbard County Sheriff's Office

Subject: Portable Audio/Video Recording Devices		
Policy #: 02-036	Issue Date: 02/01/2022	
Effective Date: 02/01/2022	Revision Date:	
Issued By: Sheriff Cory Aukes		
Purpose: To provide guidelines for the use of portable audio/video recording devices by members of this Office while in performance of their duties.		

I. Policy, Rules, Procedure:

1) POLICY

The Hubbard County Sheriff's Office has implemented the use of portable recording devices, and may issue one of these devices to officers for use during the performance of their official duties.

2) DEFINITIONS

Portable Recording Device: A device that is capable of audio and video recording, that is possessed by an officer, intended to accurately record interactions with members of the public.

3) PROCEDURES

- A. At the beginning of each shift, uniformed officers and officers assigned to investigations are responsible for making sure that their portable recording device is functioning properly. Supervisor notification shall take place as soon as possible if the device is not working properly, or if a malfunction occurs. A properly functioning device shall be obtained as soon as reasonably practicable.

Portable recording devices should be worn in a conspicuous manner,

or the persons being recorded should be notified whenever reasonably practicable. This procedure does not apply to non-uniformed officers who are conducting a recording of a lawful undercover operation.

Policy and Procedures Manual

Oral communications may be inconspicuously recorded as long as one individual involved in the conversation has knowledge that the conversation is being recorded, and has given prior consent to the recording.

When a portable recording device is used, the officer's name, badge number, date/time at the beginning of use and date/time at the end of use shall be recorded. This information can be recorded manually or by the device and software program that is utilized.

The existence of a recording should be documented in a report or other official record. Any instances where the recording device malfunctioned or was deactivated should also be documented in the report, along with the reason for the deactivation.

- B. This policy does not describe every possible situation where a portable recording device should be used. Devices shall be activated anytime it would be appropriate or valuable to record an interaction, and anytime there is personal interaction with a member of the public during a call for service. The device should be activated in any of the following situations:
 - a. Traffic stops including motorist assists
 - b. Self-initiated activity when Dispatch would normally be notified
 - c. Any other enforcement or investigative interactions
 - d. Any other contact that becomes adversarial when recording would not normally be required
- C. Dignity of individuals being recorded should be taken into consideration. Recording should be discontinued whenever it reasonably appears that an individual's privacy outweighs any legitimate law enforcement interest in recording. This same procedure should be considered if a member of the public requests the recording to be stopped. Recording should resume when the privacy concerns are no longer an issue unless the situation no longer fits the requirements for recording.
- D. Officer safety should never be jeopardized in order for a portable recording device to be activated. The device should be activated in these situations as soon as reasonably practicable.

- E. Once activated, the portable recording device should continue recording until it is reasonably believed that direct participation in an event has concluded, or the situation no longer fits the requirements

for recording. The recording may be stopped during extended periods of inactivity or during breaks from direct participation in an event.

F. The following actions involving portable recording devices are prohibited:

- a. Utilizing County issued devices for personal use
- b. Making personal copies of recordings created while on-duty or while acting in an official capacity
- c. Personally retaining possession of recordings of on-duty activities or information obtained, created while on-duty or while acting in an official capacity. This procedure applies to recordings made with County issued and personal devices. Any such recordings shall not be duplicated or distributed except for legitimate business purposes. Any such recordings shall be retained at the Sheriff's Office.
- d. Utilizing personal recording devices while on-duty without receiving prior supervisor approval. Any recordings made with a personal device are subject to the provisions of this policy.
- e. For the purpose of a criminal or administrative investigation, utilizing portable recording devices to inconspicuously record communications with co-workers or supervisors without a Court Order or lawful authorization of the Sheriff or Sheriff's designee.
- f. Utilizing recordings for the purpose of embarrassment, harassment or ridicule.
- g. Activating a portable recording device in an area that may contain an explosive device. This does not apply to authorized use of recording devices by members of the Emergency Response Unit who may be utilizing authorized distraction devices.

G. The Sheriff, or designee, should designate a Coordinator who is responsible for the following:

- a. Establishing procedures for the security, storage and maintenance of data and recordings. These procedures should be in compliance with the Minnesota Government Data Practices Act and any other applicable laws.
- b. Establishing procedures for accessing data and recordings.
- c. Establishing procedures for logging or auditing access.
- d. Establishing procedures for transferring, downloading, tagging or marking events.
- e. Establishing an inventory of portable recording devices to include:
 - i. Total number of devices owned or maintained by the Office.
 - ii. Daily record of the total number deployed and used in the field.

- iii. Total amount of recorded audio and video data collected and maintained by the Office.
- iv. Preparing the biennial audit required by Minnesota Statute 13.825 sub. 9.
- v. Notifying the MN BCA within a reasonable time period when new equipment is obtained that expands the type or scope of surveillance capabilities of the Office's portable recording device.

H. Hubbard County Sergeants will review a minimum of three random Deputies body worn camera recordings each month throughout calendar year.

I. All recordings shall be retained for a period consistent with the County General Records Retention Schedule. Recordings will never be retained for a period of less than 90 days for inactive investigations. All other portable recording device data will be kept for no less than 1 year.


Recordings may be kept for an additional period of time if a written request is received from an individual who is captured in a recording. The Coordinator should notify the individual of these requests prior to destroying the recording.

J. Except as provided by MN Statute 13.825 sub. 2, audio and video recordings are considered private or non-public data. Any person captured in a recording may have access to the recording. If the individual captured requests a copy of the recording, the identity of other non-law enforcement individuals captured in the recording must be sufficiently obscured to protect their identity prior to release. The identity of on-duty peace officers may not be obscured unless their identity is protected under MN Statute 13.82 sub. 17.

K. Any employee who accesses or releases recordings without authorization may be subject to discipline up to and including termination.

APPENDIX B:

Hubbard County Sheriff's Office

Subject: Portable Audio/Video Recording Devices		
Policy #: 02-036	Issue Date: 02/01/2022	
Effective Date: 02/01/2022	Revision Date: 03/04/2024	
Issued By: Sheriff Cory Aukes		
Purpose: To provide guidelines for the use of portable audio/video recording devices by members of this Office while in performance of their duties.		

Policy, Rules, Procedure:

1) POLICY

The Hubbard County Sheriff's Office has implemented the use of portable recording devices, and may issue one of these devices to officers for use during the performance of their official duties.

2) DEFINITIONS

Portable Recording Device: A device that is capable of audio and video recording, that is possessed by an officer, intended to accurately record interactions with members of the public.

3) PROCEDURES

- A. At the beginning of each shift, uniformed officers and officers assigned to investigations are responsible for making sure that their portable recording device is functioning properly. Supervisor notification shall take place as soon as possible if the device is not working properly, or if a malfunction occurs. A properly functioning device shall be obtained as soon as reasonably practicable.

Portable recording devices should be worn in a conspicuous manner, above the mid-line of the waist in a position that maximizes the recording system capacity to record officer's activities. The persons being recorded should be notified whenever reasonably practicable. This procedure does not apply to non-uniformed officers who are conducting a recording of a lawful undercover operation.

Oral communications may be inconspicuously recorded as long as one individual involved in the conversation has knowledge that the conversation is being recorded, and has given prior consent to the recording.

When a portable recording device is used, the officer's name, badge number, date/time at the beginning of use and date/time at the end of use shall be recorded. This information can be recorded manually or by the device and software program that is utilized.

The existence of a recording should be documented in a report or other official record. Any instances where the recording device malfunctioned or was deactivated should also be documented in the report, along with the reason for the deactivation.

- B. This policy does not describe every possible situation where a portable recording device should be used. Devices shall be activated anytime it would be appropriate or valuable to record an interaction, and anytime there is personal interaction with a member of the public during a call for service. The device should be activated in any of the following situations:

- a. Traffic stops including motorist assists
 - b. Self-initiated activity when Dispatch would normally be notified
 - c. Any other enforcement or investigative interactions
 - d. Any other contact that becomes adversarial when recording would not normally be required
- C. Dignity of individuals being recorded should be taken into consideration. Recording should be discontinued whenever it reasonably appears that an individual's privacy outweighs any legitimate law enforcement interest in recording. This same procedure should be considered if a member of the public requests the recording to be stopped. Recording should resume when the privacy concerns are no longer an issue unless the situation no longer fits the requirements for recording.
- D. Officer safety should never be jeopardized in order for a portable recording device to be activated. The device should be activated in these situations as soon as reasonably practicable.
- E. Officers assigned a portable recording system must 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;
- F. Once activated, the portable recording device should continue recording until it is reasonably believed that direct participation in an event has concluded, or the situation no longer fits the requirements for recording. The recording may be stopped during extended periods of inactivity or during breaks from direct participation in an event.
- G. The following actions involving portable recording devices are prohibited:
 - a. Utilizing County issued devices for personal use
 - b. Making personal copies of recordings created while on-duty or while acting in an official capacity
 - c. Personally retaining possession of recordings of on-duty activities or information obtained, created while on-duty or while acting in an official capacity. This procedure applies to recordings made with County issued and personal devices. Any such recordings shall not be duplicated or distributed except for legitimate business purposes. Any such recordings shall be retained at the Sheriff's Office.

- d. Utilization of personal BWC devices is strictly prohibited, only department issued and maintained devices will be used.
 - e. For the purpose of a criminal or administrative investigation, utilizing portable recording devices to inconspicuously record communications with co-workers or supervisors without a Court Order or lawful authorization of the Sheriff or Sheriff's designee.
 - f. Utilizing recordings for the purpose of embarrassment, harassment or ridicule.
 - g. Activating a portable recording device in an area that may contain an explosive device. This does not apply to authorized use of recording devices by members of the Emergency Response Unit who may be utilizing authorized distraction devices.
 - h. 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 (b) unredacted recording of a peace officer using deadly force must be maintained indefinitely;
- H. The Sheriff, or designee, should designate a Coordinator who is responsible for the following:
 - a. Establishing procedures for the security, storage and maintenance of data and recordings. These procedures should be in compliance with the Minnesota Government Data Practices Act and any other applicable laws.
 - b. Establishing procedures for accessing data and recordings.
 - c. Establishing procedures for logging or auditing access.
 - d. Establishing procedures for transferring, downloading, tagging or marking events.
 - e. Establishing an inventory of portable recording devices to include:
 - i. Total number of devices owned or maintained by the Office.
 - ii. Daily record of the total number deployed and used in the field.
 - iii. Total amount of recorded audio and video data collected and maintained by the Office.
 - iv. Preparing the biennial audit required by Minnesota Statute 13.825 sub. 9.
 - v. Notifying the MN BCA within a reasonable time period when new equipment is obtained that expands the type or scope of surveillance capabilities of the Office's portable recording device.
- I. Hubbard County Sergeants will review a minimum of three random Deputies body worn camera recordings each month throughout calendar year.

- J. Portable recording system data must be maintained for at least one year and destroyed according to the agency's records retention schedule approved pursuant to section 138.17 if:
- (1) *The data document (i) the discharge of a firearm by a peace officer in the course of duty if a notice is required under section 626.553, subdivision 2, or (ii) the use of force by a peace officer that results in substantial bodily harm; or*
 - (2) *A formal complaint is made against a peace officer related to the incident.*
- .
- K. (a) Except as provided by MN Statute 13.825 sub. 2, audio and video recordings are considered private or non-public data. Any person captured in a recording may have access to the recording. If the individual captured requests a copy of the recording, the identity of other non-law enforcement individuals captured in the recording must be sufficiently obscured to protect their identity prior to release. The identity of on-duty peace officers may not be obscured unless their identity is protected under MN Statute 13.82 sub. 17.
- (b) Citizens requesting BWC data must submit a request to records staff, the request is then handled by records management and forwarded to the Sheriff or Chief Deputy for approval. All law enforcement/court/probation entities with access to electronic websites that allow the sharing of BWC can send requests to and be approved through records staff by the appropriate electronic websites. Every email link sent with BWC to another entity will have a disclaimer at the bottom stating, *"By receiving this data you acknowledge your data practices responsibilities as outlined in MN 13.825 sub 7 & 8 and the data classification, safety and destruction requirements therein"*. Data access procedures can be found on the Hubbard County website.
- (c) 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 agency will notify the requestor at the time of the request that the data will then be destroyed unless a new written request is received.
- (d) *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. In addition, BWC data shall be made available to prosecutors, courts, and other criminal justice entities as provided by law.*
- L. It is mandatory, notwithstanding any law to the contrary, when an individual dies as a result of a use of force by a peace officer in Hubbard County, 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:

Hubbard County may deny a request if it is determined that there is a compelling reason that inspection would interfere with an active investigation. If Hubbard County 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;

M. It is mandatory 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;

N. Any employee who accesses or releases recordings without authorization may be subject to discipline up to and including termination as well as potential criminal charges.