

Rampart Defense, LLC



INDEPENDANT AUDITOR'S REPORT

Roseau County Sheriff's Office Body-Worn Camera Program



JUNE 18, 2021

RAMPART DEFENSE LLC
P.O. BOX 23 Clearbrook, MN 56634

Appendix A: What Follows is the Roseau County Sheriff's Office Body Camera Policy as presented to Rampart Defense LLC for compliance auditing check. After that Policy you will find our audit overview and recommendations.

Body-Worn Cameras

PURPOSE

The primary purpose of using BWCs is to capture evidence arising from police-citizen encounters.

While this technology allows for the collection of valuable information, it opens up many questions

about how to balance public demands for accountability and transparency with the privacy concerns of those being recorded. In deciding what to record, this policy also reflects a balance between the desire to establish exacting and detailed requirements and the reality that officers must attend to their primary duties and the safety of all concerned, often in circumstances that are

tense, uncertain, and rapidly evolving.

POLICY

It is the policy of the Roseau County Sheriff's Office to authorize and require the use of department-issued BWCs as set forth below.

SCOPE

This policy governs the use of BWCs in the course of official duties. It does not apply to the use of surreptitious recording devices in undercover operations or the use of squad-based (dash-cam) video recorders. The Sheriff or Sheriff's designee may supersede this policy by providing specific instructions for the use of BWCs to individual officers, or providing specific instructions for the use of BWCs pertaining to certain events or classes of events, including but not limited to political rallies and demonstrations. The Sheriff or Sheriff's designee may also provide specific instructions or standard operating procedures for BWC use to officers assigned to specialized details, such as carrying out duties in courts or guarding prisoners or patients in hospitals and mental health facilities.

DEFINITIONS

The following phrases have special meanings as 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 means 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 means that 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 officer.

General citizen contact means 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 means a law enforcement encounter with a person that becomes confrontational,

158

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

Official duties, for purposes of this policy, means that the officer is on duty and performing authorized law enforcement services on behalf of this agency.

USE AND DOCUMENTATION

Officers 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 department.

Officers who have been issued BWCs shall operate and use them consistent with this policy. Officers shall check their issued BWCs at the beginning of each shift to make sure the devices are functioning properly and shall promptly report any malfunctions to the officer's supervisor. Officers should wear their issued BWCs at the location on their body and in the manner specified in training.

Officers must document BWC use and nonuse as follows:

1. Whenever an officer makes a recording, the existence of the recording shall be documented in an incident report.
2. Whenever an officer fails to record an activity that is required to be recorded under this policy or captures only a part of the activity, the officer must document the circumstances and reasons for not recording in an incident report. Supervisors shall review these reports and initiate any corrective action deemed necessary.

GENERAL GUIDELINES FOR RECORDING

A. Officers 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 (D)(2) (above).

B. Officers have discretion to record or not record general citizen contacts.

C. Officers have no affirmative duty to inform people that a BWC is being operated or that they 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

159

information having evidentiary value. The officer having charge of a scene shall likewise direct the discontinuance of recording when further recording is unlikely to capture additional information having evidentiary value. Officers shall state the reasons for ceasing the recording on camera before deactivating their BWC. If circumstances change, officers shall reactivate their cameras as required by this policy to capture

information having evidentiary value.

E. Officers shall not intentionally block the BWC's audio or visual recording functionality to defeat the purposes of this policy.

F. Notwithstanding any other provision in this policy, officers 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. Officers shall not intentionally edit, alter, or erase any BWC recording unless otherwise expressly authorized by the Sheriff or the Sheriff's designee.

SPECIAL GUIDELINES FOR RECORDING

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

A. To use their BWC 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 BWC to take recorded statements from persons believed to be victims and witnesses of crimes, and persons suspected of committing crimes, considering the needs of the investigation and the circumstances pertaining to the victim, witness, or suspect.

In addition,

C. Officers need not record persons being provided medical care unless there is reason to believe the recording would document information having evidentiary value.

Officers may activate their BWCs when dealing with individuals believed to be experiencing a mental health crisis or event. BWCs shall be activated as necessary to document any use of force and the basis therefor 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.

D. Officers may use their BWC's and squad based audio/video systems 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, but otherwise should not record 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.

DOWNLOADING AND LABELING DATA

A. Each officer using a BWC is responsible for transferring or assuring the proper transfer of the data from his or her camera to *[specify data storage location]* by the end of that

160

officer's shift. However, if the officer is involved in a shooting, in-custody death, or other law enforcement activity resulting in death or great bodily harm, the Sheriff or Sheriff's designee shall take custody of the officer's BWC and assume responsibility for transferring the data from it.

1. Evidence---criminal: The information has evidentiary value with respect to an actual or suspected criminal incident or charging decision.

2. Evidence--force: Whether or not enforcement action was taken or an arrest resulted, the event involved the application of force by a law enforcement officer of this or another agency.

3. Evidence--property: Whether or not enforcement action was taken or an arrest resulted, an officer seized property from an individual or directed an individual to dispossess property.

4. Evidence--administrative: The incident involved an adversarial encounter.

5. Evidence---other: The recording has potential evidentiary value for reasons identified by the officer at the time of labeling.

6. Training: The event was such that it may have value for training.

7. Unintentionally recorded footage: See Definitions, part G. Officers labeling a file as such shall document the events or subject matter that was accidentally recorded on a form or in a manner specified by the department.

8. Not evidence: The recording does not contain any of the foregoing categories of information and has no apparent evidentiary value. Recordings of general citizen contacts are not evidence.

B. In addition, officers shall flag each file as appropriate to indicate that it contains information about data subjects who may have rights under the MGDPA limiting public disclosure of information about them. These individuals include:

1. Victims and alleged victims of criminal sexual conduct.

2. Victims of child abuse or neglect.

3. Vulnerable adults who are victims of maltreatment.

4. Undercover officers.

5. Informants.

6. When the video is clearly offensive to common sensitivities.

7. Victims of and witnesses to crimes, if the victim or witness has requested not to be identified publicly.

8. Individuals who called 911, and services subscribers whose lines were used to place a call to the 911 system.

9. Mandated reporters.

10. Juvenile witnesses, if the nature of the event or activity justifies protecting the identity of the witness.

11. Juveniles who are or may be delinquent or engaged in criminal acts.

12. Individuals who make complaints about violations with respect to the use of real property.

13. Officers and employees who are the subject of a complaint related to the events captured on video.

14. Other individuals whose identities the officer believes may be legally protected from public disclosure.

C. Labeling and flagging designations may be corrected or amended based on additional information.

ACCESS TO BWC DATA

161

A. Authorized designee responsible for up loading and disseminating all video to department Officers as requested. In addition:

B. Personally owned devices, including but not limited to computers and mobile devices, shall not be programmed or used to access or view BWC data.

C. Officers 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.

D. Officers 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. Officers should limit these displays to protect against the incidental disclosure of individuals whose identities are not public.

E. 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 onto public and social media websites.

F. Officers shall refer members of the media or public seeking access to BWC data to the Sheriff or Sheriff's designee who will process the request in accordance with the MGDPA and other governing laws. Employees seeking access to BWC data for nonbusiness reasons may make a request for it in the same manner as any member of the public.

G. BWC data shall be made available to prosecutors, courts, and other criminal justice entities as provided by law.

AGENCY USE OF DATA

A. 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 officer misconduct or performance.

B. Nothing in this policy limits or prohibits the use of BWC data as evidence of misconduct or as a basis for discipline.

DATA RETENTION AND SECURITY

A. Evidentiary data shall be retained for the period specified in the General Records Retention Schedule for Minnesota Counties. When a particular recording is subject to multiple retention periods, it shall be maintained for the longest applicable retention period.

B. Unintentionally recorded footage shall not be retained.

C. BWC footage that is classified as non-evidentiary, or becomes classified as nonevidentiary, shall be retained for a minimum of 30 days following the date of capture. If information comes to light indicating that non-evidentiary data has evidentiary value or value for training, it may be reclassified and retained for a longer period.

D. The department shall maintain an inventory of BWC recordings.

162

E. Officers shall not intentionally edit, alter, or erase any BWC recording unless otherwise expressly authorized by the Sheriff or the Sheriff's designee.

F. As required by Minn. Stat. § 13.825, subd. 9, as may be amended from time to time, this agency shall obtain an independent biennial audit of its BWC program.

G. 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.

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.

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 3/31/2021. 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 April 22, 2021, Rampart Defense, LLC (Rampart) met with Chief Deputy Tobi Eidsmoe, who provided information about RCSO's BWC program policies, procedures and operations. As part of the audit, 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.

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."

Chief Deputy Eidsmoe advised us that RCSO implemented its body-worn camera program in 2011. This predates Minnesota Statute §13.825, which was enacted by the state legislature in 2016. Minnesota Statute §626.8473 establishes requirements for any law enforcement agency implementing a BWC program, including the following:

- The agency must provide an opportunity for public comment prior to purchasing or implementing a BWC program. The agency must, at a minimum, accept public comments submitted electronically or by mail. In addition, the governing body with jurisdiction over the agency's budget must provide an opportunity for public comment at a regularly scheduled meeting.

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.

- The chief officer of any state or local agency that uses or proposes to use a BWC must establish and enforce a written policy governing its use.
- In developing and adopting the policy, the agency must provide for public comment and input in the same manner as noted above.
- The policy must be posted on the agency's Website, if the agency has a Website.

While RCSO's BWC policy is available on its website, Chief Deputy Eidsmoe was unable to locate documentation showing that the public notification, comment and meeting requirements had been satisfied either before or after the adoption of §13.825, and indicated that he believed these requirements had not been met. Because Minnesota Statute §626.8473 does not contain language grandfathering existing BWC programs, Rampart strongly recommended RCSO suspend use of its BWC program until those requirements could be satisfied.

Prior to the issuance of this report, Chief Deputy Eidsmoe 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 scheduled meeting on April 27, 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. Rampart has seen and retained photographic and PDF copies of the council meeting minutes, resolution and public notification to this effect.

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. Procedures for testing the portable recording system to ensure adequate functioning;
3. 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;
4. Circumstances where recording is mandatory, prohibited, or at the discretion of the officer using the system;
5. Circumstances under which a data subject must be given notice of a recording;
6. Circumstances under which a recording may be ended while an investigation, response, or incident is ongoing;
7. Procedures for the secure storage of portable recording system data and the creation of backup copies of the data; and
8. 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.

Due to their complexity and interrelatedness, clauses 1 and 7 are discussed separately below. Clause 8 is also discussed separately.

While the RCSO policy is comprehensive and thorough with respect to clauses 4 – 6, we noted that it does not address procedures for testing the BWC to ensure adequate functioning (clause 2) or procedures to address a system malfunction or failure (clause 3). We strongly recommend adding language to include these required elements.

We recommend including a directive in the BWC policy that personnel check their issued BWC at the start of their shift, or prior to placing the BWC in service. In the event of a device failure, either at the start of their shift or in the field, personnel should notify a supervisor of the failure and obtain a replacement BWC as soon as reasonably practicable.

RCSO BWC Data Retention

In reviewing RCSO's body-worn camera policy, we noted that it specifies a minimum retention period of 30 days for BWC data. Minnesota Statute §13.825 Subd. 3 mandates a minimum retention period of 90 days for all BWC data. Chief Deputy Eidsmoe advised us that BWC data are, in fact, retained for a minimum of 90 days, and that the written policy will be updated to reflect this statutory requirement.

We also noted that the RCSO written policy states that "[u]nintentionally recorded footage shall not be retained." Because there is no exception in the statute for accidental or unintentional recordings, they also fall under the 90-day minimum retention requirement discussed above. We strongly recommend eliminating this section of the policy.

RCSO does not create any copies of BWC data on optical discs (CD/DVD) or other removable media.

RCSO BWC Data Destruction

RCSO BWC data stored on servers is destroyed through manual deletion and overwriting. In addition, any hard drive retired from service will be physically destroyed through mechanical means.

We recommend noting these procedures in the written policy.

RCSO BWC Data Access

Any requests for access to BWC data by data subjects would be facilitated by Chief Deputy Eidsmoe in accordance with the provisions of §13.825 Subd. 4(b).

RCSO BWC data is shared with other law enforcement agencies for evidentiary purposes only. All such requests must be made to Sheriff Gust or Chief Deputy Eidsmoe by the requesting agency's chief law enforcement officer (CLEO). 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 be made in writing and include a brief explanation of the law enforcement purpose for the request. This could be accomplished through email. A file of these requests should be maintained for audit purposes.

RCSO BWC Data Classification

Chief Deputy Eidsmoe advised us that RCSO follows the BWC data classifications set forth in Minnesota Statute §13.825; however, this is not explicitly stated in the RCSO BWC policy. We recommend incorporating this information by reference in RCSO's BWC policy.

RCSO BWC Internal Compliance Verification

The RCSO BWC Compliance section 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.

Chief Deputy Eidsmoe advised us that supervisory staff perform internal audits of BWC data and that these data are used for deputy performance reviews.

RCSO BWC Program and Inventory

RCSO currently possesses three (3) Watchguard body-worn cameras, and seven (7) VIEVU body-worn cameras. Chief Deputy Eidsmoe advised us that VIEVU is a legacy system and the camera models RCSO owns are no longer sold. As the VIEVU cameras age out of service, they are replaced with Watchguard units.

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, Chief Deputy Eidsmoe advised us that because each patrol 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. In addition, the sheriff and chief deputy have access to cameras but do not ordinarily wear them unless responding to a call for which activation is anticipated. BWC use would be determined based on the creation of BWC data.

As of 4/22/2021, RCSO maintained 185 GB of BWC data.

RCSO BWC Physical, Technological and Procedural Safeguards

RCSO BWC data are uploaded from each device at the end of each shift. RCSO employs an automated upload process in which data are buffered in temporary files on a desktop computer, then copied to a secure server. Once the upload to the server is complete, the temporary files located on the desktop computer are deleted automatically. The server is password-protected and is located behind locked doors, where it is accessible only by the sheriff, chief deputy and the head of IT. This server is backed-up to a second server located in a separate secure location.

BWC data associated with criminal cases are copied to the LETG case management software as needed. These video files are then accessible to the Roseau County Attorney's Office for prosecutorial purposes.

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 80 ICRs 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 ICRs 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.

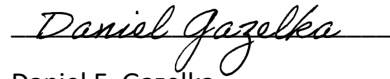
Audit Conclusions

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

- All BWC data, including unintentional or test recordings, must be retained for a minimum of 90 days.
- The BWC policy must include procedures for testing the BWC to ensure adequate functioning.
- The BWC policy must include 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.

Rampart Defense, LLC

We recommend RCSO immediately amend their policy to address the areas of non-compliance identified above.



Daniel E. Gazelka

Rampart Defense LLC

6/18/2021