

Rampart Defense, LLC



INDEPENDENT AUDITOR'S REPORT

Kandiyohi County Sheriff's Office Body-Worn Camera Program



AUGUST 1, 2022
RAMPART DEFENSE LLC
P.O. Box 23 Clearbrook, MN 56634

Audit Overview and Recommendations

Dear Kandiyohi County Board and Sheriff Holien:

We have audited the body-worn camera (BWC) program of the Kandiyohi County Sheriff's Office (KCSO) for the two-year period ended 2/28/2022. 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 Kandiyohi County Sheriff's Office. Our responsibility is to express an opinion on the operations of this program based on our audit.

On May 23, 2022, Rampart Defense LLC (Rampart) met with Sheriff Eric Holien, who provided information about KCSO'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 KCSO's recordkeeping.

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

KCSO 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."

Sheriff Holien provided documentation showing that the public notification, comment and meeting requirements had been satisfied prior to the implementation of KCSO's BWC program. Specifically, Sheriff Holien furnished a copy of a news release dated January 18, 2018, announcing the proposed implementation of a body-worn camera program and inviting the public to attend a hearing to discuss the program and KCSO's proposed BWC policies. Sheriff Holien also furnished copies of the agenda 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 KCSO, these terms may be used interchangeably in this report.

minutes of the February 6, 2018, Kandiyohi County Board meeting, documenting the presentation of KCSO's proposed body-worn camera system and policy, as well as the board's adoption of that policy. Copies of those documents have been retained in Rampart's audit files.

The Kandiyohi County Sheriff's Office's body-worn program was then implemented effective March 1, 2018.

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

In our opinion, the Kandiyohi County Sheriff's Office met the relevant statutory requirements prior to the implementation of its body-worn camera program.

KCSO BWC WRITTEN POLICY

As part of this audit, we reviewed KCSO'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.

In our opinion, the KCSO BWC policy is compliant with respect to clauses 2 – 6.

KCSO BWC Data Retention

KCSO's data retention policy states that "[a]ll BWC data shall be retained for a minimum period of 90 days. There are no exceptions for erroneously recorded or non-evidentiary data." The policy also includes an itemized list of retention periods for different categories of BWC data, with additional categories detailed in the Records Retention Schedule. These guidelines meet or exceed the requirements specified for each category of BWC data enumerated in §13.825 Subd. 3.

KCSO employs Watchguard body-worn cameras and manages BWC data retention on their own secure server through automated retention settings in the video management software. The retention period for each video is determined by the data classification assigned at the time of upload; however, this retention period can be adjusted as needed.

KCSO's BWC policy requires that each deputy transfer data from his or her body-worn camera to the appropriate server no later than the beginning of his or her next shift, and also requires that the deputy assign the appropriate label or labels to each file to identify the nature of the data. These labels then determine the appropriate retention period for each file.

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

KCSO BWC Data Destruction

Sheriff Holien advised us that KCSO BWC data are stored on a server located on-site. This server is then replicated on a second off-site server, thus creating an archive copy of all BWC data.

Data on the existing server 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 KCSO-owned physical hard drive used to store BWC data will have all data deleted prior to being destroyed by physical means, specifically crushing.

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

KCSO BWC Data Access

Any request for access to BWC data by data subjects or the media would be made to the Sheriff, who is responsible for reviewing each request in accordance with the provisions of §13.825 Subd. 4(b). Approved requests are fulfilled by KCSO IT staff.

KCSO BWC data is shared with other law enforcement agencies for evidentiary purposes only. All such requests must be made by email to Sheriff Holien by the requesting agency's chief law enforcement officer (CLEO) and are processed by KCSO IT staff once approved. Existing verbal agreements between KCSO and other area law enforcement agencies address data classification, destruction and security requirements, as specified in §13.825 Subd. 8(b). At the time of the audit, KCSO was in the process of obtaining a formal written acknowledgement from each requesting agency of its responsibilities under

§13.825 Subd. 7 and 8. The Rampart auditor reviewed the acknowledgements KCSO had received at that time. Access to KCSO BWC data for outside agencies is provided via email with an expiring link.

We recommend that KCSO continue to obtain a written acknowledgement from any outside law enforcement agency that any BWC data obtained from KCSO will be managed by the requesting agency in compliance with the requirements of §13.825 Subd. 7 and 8. A copy of each written acknowledgment should be maintained on file.

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

KCSO BWC Data Classification

KCSO follows the BWC data classifications set forth in Minnesota Statute §13.825, and the written BWC policy incorporates the statutory language extensively. In our opinion, this section of the policy is compliant with respect to the applicable data classification requirements.

KCSO BWC Internal Compliance Verification

KCSO's 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 and to identify any performance areas in which additional training or guidance is required." The policy further addresses the use of BWC video in response to complaints or concerns about misconduct or performance.

KCSO's BWC policy also 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."

Sheriff Holien confirmed that sergeants also monitor to ensure deputies are performing function tests of the body-worn cameras as required by policy.

In our opinion, KCSO's BWC policy meets the compliance and disciplinary requirements specified in §626.8473 Subd. 8.

KCSO BWC Program and Inventory

KCSO currently possesses 23 Watchguard body-worn cameras.

The KCSO 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 KCSO does not maintain a separate log of BWC deployment or use, Sheriff Holien advised us that because each uniformed deputy wears a BWC while on duty, the number of BWC units deployed with

uniformed personnel each shift can be determined based on a review of KCSO payroll records. Actual BWC use would be determined based on the creation of BWC data.

As of 5/23/2022, KCSO maintained 12,372 BWC data files (videos).

KCSO BWC Physical, Technological and Procedural Safeguards

KCSO BWC data are initially recorded to an internal hard drive in each deputy's BWC. Those files are then transferred to a dedicated server at the KCSO office via wireless upload either from the deputy's squad car or from the squad room at the sheriff's office. In addition, there is a manual upload option if the automated upload process fails. The server is secured behind multiple locked doors. As noted earlier in this report, KCSO BWC data is also replicated on a second county-owned server in a separate secure facility.

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

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

Enhanced Surveillance Technology

KCSO 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 KCSO 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 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 auditor reviewed the retained BWC videos to verify that this data was accurately documented in KCSO records.

Prior Period Examination

As part of this audit, Rampart learned that KCSO had not obtained an independent audit for the first two years of its BWC program’s operation, covering the period from 3/1/2018 – 2/29/2020. After consulting with Sheriff Holien, Rampart agreed to expand its scope of work to review this additional period.

With the exception of the recently-adopted practice of obtaining written acknowledgments from other agencies of their §13.825 Subd. 7 and 8 responsibilities pertaining to BWC data security, Rampart determined that the policies, practices and procedures of KCSO’s BWC program during this prior period were substantially identical to those in place during the audit period.

Rampart also selected a random sample of ICRs from this prior period for which to review any available BWC recordings. The auditor reviewed the retained BWC videos to verify that this data was accurately documented in KCSO records.

Audit Conclusions

In our opinion, the Kandiyohi County Sheriff’s Office’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 "Daniel E. Gazelka", is written over a horizontal line. The signature is stylized and extends to the right of the line.

Daniel E. Gazelka

Rampart Defense LLC

8/01/2022

APPENDIX A:

Policy 421 Kandiyohi County Sheriff's Office Kandiyohi County SO Policy Manual Copyright Lexipol, LLC 2021/12/30, All Rights Reserved. Published with permission by Kandiyohi County Sheriff's Office

BODY-WORN CAMERAS - 340 BODY-WORN CAMERAS 421.1 PURPOSE 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 data that results. 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. 421.2 **POLICY** It is the policy of this office to authorize and require the use of office-issued BWCs as set forth below, and to administer BWC data as provided by law. 421.3 **SCOPE** 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 or guarding prisoners or patients in hospitals and mental health facilities. 421.4 **DEFINITIONS** The following phrases have special meanings as used in this policy: A. MGDPA or Data Practices Act refers to the Minnesota Government Data Practices Act, Minn. Stat. § 13.01, et seq. B. Records Retention Schedule refers to the General Records Retention Schedule for Kandiyohi County Sheriff's Office. C. 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. D. 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 deputy. E. 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, Kandiyohi County Sheriff's Office Kandiyohi County SO Policy Manual BODY-WORN CAMERAS Copyright Lexipol, LLC 2021/12/30, All Rights Reserved. Published with permission by Kandiyohi County Sheriff's Office BODY-WORN CAMERAS - 341 or receiving generalized concerns from a citizen about crime trends in his or her neighborhood. F. Adversarial means 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. G. Unintentionally recorded footage is a video recording that results from a deputy's inadvertence or neglect in operating the deputy'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. H. Official

duties, for purposes of this policy, means that the deputy is on duty and performing authorized law enforcement services on behalf of this agency. 421.5 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 conduct a function test of their issued BWCs at the beginning of each shift to make sure the devices are operating properly. Deputies noting a malfunction during testing or at any other time shall promptly report the malfunction to the deputy's supervisor and shall document the report in writing. Supervisors and the reporting deputy shall take prompt action to address malfunctions and document the steps taken in writing. C. Deputies should wear their issued BWCs at the location on their body and in the manner specified in training and that will serve the purpose of the BWC. D. Deputies must document BWC use and non-use as follows: 1. Whenever an deputy makes a recording, the existence of the recording shall be documented in an incident report or in the current records management system. 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 an incident report or the current records management system. Supervisors shall review these reports and initiate any corrective action deemed necessary. E. The 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; Kandiyohi County Sheriff's Office Kandiyohi County SO Policy Manual BODY-WORN CAMERAS Copyright Lexipol, LLC 2021/12/30, All Rights Reserved. Published with permission by Kandiyohi County Sheriff's Office BODY-WORN CAMERAS - 342 2. A daily record of the total number of BWCs actually deployed and used by deputies and, if applicable, the precincts in which they were used; 3. The total amount of recorded BWC data collected and maintained; and 4. This policy, together with the Records Retention Schedule. 421.6 GENERAL GUIDELINES FOR RECORDING A. Deputies shall activate their BWCs when anticipating that they will be involved in, become involved in, or witness other deputies 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, deputies 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. 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 and document in a report per sec 446.5 D(2). If circumstances change, deputies shall reactivate their cameras as required by this policy to capture information having evidentiary value. E. Deputies 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, 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. 421.7 SPECIAL GUIDELINES FOR RECORDINGS

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. Kandiyohi County Sheriff's Office Kandiyohi County SO Policy Manual BODY-WORN CAMERAS Copyright Lexipol, LLC 2021/12/30, All Rights Reserved. Published with permission by Kandiyohi County Sheriff's Office BODY-WORN CAMERAS - 343 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. 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. D. Deputies may use their BWCs 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 deputy anticipates witnessing a criminal event or being involved in or witnessing an adversarial encounter or use-of-force incident. 421.8 DOWNLOADING AND LABELING DATA A. Each deputy using a BWC is responsible for transferring or assuring the proper transfer of the data from his or her camera to designated location at the Kandiyohi County Law Enforcement Center by the end of that deputy's shift or at the beginning of the next shift. However, all BWC must be uploaded prior to going on days off or vacation. However, if the deputy is involved in a shooting, in-custody death, or other law enforcement activity resulting in death or great bodily harm, a supervisor or investigator shall take custody of the deputy's BWC and assume responsibility for transferring the data from it. Deputies involved in those critical incidents shall not review the BWC video unless cleared to do so by the Sheriff. B. Deputies shall label the BWC data files at the time of video capture or transfer to storage, and should consult with a supervisor if in doubt as to the appropriate labeling. [Include any technology-specific instructions for this process; if metadata is not being stored, then the information could be documented in a video log or other record.] Deputies should assign as many of the following labels as are applicable to each file: 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, a deputy seized property from an individual or directed an individual to dispossess property. 4. Evidence—other: The recording has potential evidentiary value for reasons identified by the deputy at the time of labeling. 5. Training: The event was such that it may have value for training. Kandiyohi County Sheriff's Office Kandiyohi County SO Policy Manual BODY-WORN CAMERAS Copyright Lexipol, LLC 2021/12/30, All Rights Reserved. Published with permission by Kandiyohi County Sheriff's Office BODY-WORN CAMERAS - 344 6. 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 and unintentionally recorded footage are not evidence. C. In addition, deputies shall flag each file as appropriate to indicate that it contains information about data subjects who may have rights under the MGDPA limiting disclosure of information about them. These individuals include: 1. Victims

and alleged victims of criminal sexual conduct and sex trafficking. 2. Victims of child abuse or neglect. 3. Vulnerable adults who are victims of maltreatment. 4. Undercover deputies. 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. Deputies and employees who are the subject of a complaint related to the events captured on video. 14. Other individuals whose identities the deputy believes may be legally protected from public disclosure. D. Labeling and flagging designations may be corrected or amended based on additional information. 421.9 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. Kandiyohi County Sheriff's Office Kandiyohi County SO Policy Manual BODY-WORN CAMERAS Copyright Lexipol, LLC 2021/12/30, All Rights Reserved. Published with permission by Kandiyohi County Sheriff's Office BODY-WORN CAMERAS - 345 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. 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. 2. Data that documents the use of force by a peace officer that results 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 (a) 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. E. Access to BWC data by non-employees. Deputies shall refer members of the media or public seeking access to BWC data to the Sheriff, who shall process the request in accordance with the MGDPA and other governing laws. In particular: 1. 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: (a) If the data was collected or created as part of an active investigation. (b) 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. 2. 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: Kandiyohi County Sheriff's Office Kandiyohi County SO Policy Manual BODY-WORN CAMERAS Copyright

Lexipol, LLC 2021/12/30, All Rights Reserved. Published with permission by Kandiyohi County Sheriff's Office BODY-WORN CAMERAS - 346 (a) Data on other individuals in the recording who do not consent to the release must be redacted. (b) Data that would identify undercover deputies must be redacted. (c) 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. F. Access by peace officer and law enforcement employees. No employee may have access to the department's BWC data except for legitimate law enforcement or data administration purposes: 1. Agency personnel shall document their reasons for accessing stored BWC data at the time of each access. 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. G. 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, 1. 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. 2. BWC data shall be made available to prosecutors, courts, and other criminal justice entities as provided by law. 421.10 DATA SECURITY SAFEGUARD A. Password protected hard drive. The agency is unable to make backup copies of data. B. 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. C. Deputies shall not intentionally edit, alter, or erase any BWC recording unless otherwise expressly authorized by the sheriff or the sheriff's designee. D. 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. 421.11 AGENCY USE OF DATA A. At least once a month, supervisors will randomly review BWC usage by each deputy to ensure compliance with this policy and to identify any performance areas in which additional training or guidance is required. Kandiyohi County Sheriff's Office Kandiyohi County SO Policy Manual BODY-WORN CAMERAS Copyright Lexipol, LLC 2021/12/30, All Rights Reserved. Published with permission by Kandiyohi County Sheriff's Office BODY-WORN CAMERAS - 347 B. 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. D. 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 officers may utilize BWC data with trainees for the purpose of providing coaching and feedback on the trainees' performance. 421.12 DATA RETENTION A. All BWC data shall be retained for a minimum period of 90 days. There are no exceptions for erroneously recorded or non-evidentiary data. B. 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. C. Certain kinds of BWC data must be retained for six years: 1. Data that documents the use of deadly force by a deputy that causes great or substantial bodily injury as defined in Minnesota state statutes. 2. Data documenting circumstances that have given rise to a formal complaint against a deputy. D. Other data having evidentiary value shall be retained for the period specified in the Records

Retention Schedule. When a particular recording is subject to multiple retention periods, it shall be maintained for the longest applicable period. E. 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. F. 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. G. This office shall maintain an inventory of BWC recordings having evidentiary value. H. This office will post this policy, together with [a link to] its Records Retention Schedule, on its website. 421.13 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.