IDEPENDENT AUDITOR'S REPORT

ATWATER POLICE DEPARTMENT BODY-WORN CAMERA PROGRAM

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

Audit Overview and Recommendations

Dear Atwater City Council and Chief Johnson:

We have audited the body-worn camera (BWC) program of the Atwater Police Department (APD) for the two-year period ended 5/17/2022. 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 Atwater Police Department. 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 Chief Ross Johnson, who provided information about APD'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 APD's recordkeeping.

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

APD 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 Johnson provided documentation showing that the public notification, comment and meeting requirements had been satisfied prior to the implementation of APD's BWC program on May 18, 2020. Specifically, Chief Johnson furnished a copy of the minutes of the December 4, 2019, Atwater City Council meeting, at which he requested that the council schedule a public hearing to "invite public questions regarding a policy on body cameras" for the Atwater Police Department. The minutes noted

[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 APD, these terms may be used interchangeably in this report.

that the hearing would be held as part of the January 6, 2020, City Council meeting. Chief Johnson also furnished a copy of the minutes from the January 6, 2020, Atwater City Council meeting, which noted that a public hearing was called during the meeting to receive questions from the public regarding the proposed body camera policy. There were no questions or comments. After the public hearing was closed, the city council voted to authorize the purchase of a body-worn camera for APD. Copies of these documents have been retained in Rampart's audit files.

Chief Johnson advised us that, as of the audit date, Atwater Police Department is in the process of building a website, but the site is not yet operational. The Rampart auditor reviewed with Chief Johnson the requirement to include a link to the written BWC policy once the APD website is active.

APD BWC WRITTEN POLICY

As part of this audit, we reviewed APD'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 APD BWC policy is compliant with respect to clauses 2 – 6.

APD BWC Data Retention

APD'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. These guidelines meet or exceed the requirements specified for each category of BWC data enumerated in §13.825 Subd. 3.

APD employs a single Watchguard body-worn camera and contracts with the Kandiyohi County Sheriff's Office for BWC data management. Rampart has previously audited the Kandiyohi County Sheriff's Office BWC program. That agency manages BWC data retention on their own secure server through automated retention settings in the Watchguard 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.

APD's BWC policy requires that each officer transfer data from his or her body-worn camera to the appropriate server by the end of each shift, and also requires that the officer 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, APD's written BWC policy is compliant with respect to applicable data retention requirements.

APD BWC Data Destruction

As discussed above, Chief Johnson advised us that APD contracts with the Kandiyohi County Sheriff's Office for BWC data management services. BWC data are stored on a server located at the sheriff's office. This server is then backed up via a replica process to a second off-site server, thus creating an archive copy of all BWC data.

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

APD BWC Data Access

Any request for access to BWC data by data subjects or the media would be made to Chief Johnson, who is responsible for reviewing and fulfilling each request in accordance with the provisions of §13.825 Subd. 4(b).

APD BWC data is shared with other law enforcement agencies for evidentiary purposes only. All such requests must be made by email to Chief Johnson by the requesting agency's chief law enforcement officer (CLEO) and are processed by KCSO IT staff once approved. Existing verbal agreements between APD 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, APD 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 APD had received at that time. Access to APD BWC data for outside agencies is provided via email with an expiring link.

We recommend that APD continue to obtain a written acknowledgement from any outside law enforcement agency that any BWC data obtained from APD 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, APD's written BWC policy is compliant with respect to the applicable data access requirements.

APD BWC Data Classification

APD 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.

APD BWC Internal Compliance Verification

APD's BWC policy states that "[a]t least once a month, supervisors will randomly review BWC usage by each officer 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.

APD'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."

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

APD BWC Program and Inventory

APD currently possesses one Watchguard body-worn camera.

The APD BWC policy identifies those circumstances in which officers 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 APD does not maintain a separate log of BWC deployment or use, Chief Johnson advised us that because there is only one camera, deployment can be determined based on a review of APD payroll records. Actual BWC use would be determined based on the creation of BWC data.

As of 5/23/2022, APD maintained 101 BWC data files (videos).

APD BWC Physical, Technological and Procedural Safeguards

APD BWC data are initially recorded to an internal hard drive in each officer's BWC. Those files are then transferred to a dedicated server at the Kandiyohi County Sheriff's Office via wireless upload either from the officer's squad car or from the squad room at the police department. The KCSO server is secured behind multiple locked doors. As noted earlier in this report, all BWC data stored on the primary KCSO server is also replicated to 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 APD BWC data must be approved by Chief Johnson and are fulfilled via expiring email link. A similar method is employed to submit APD BWC data to the Kandiyohi County Attorney's Office.

Enhanced Surveillance Technology

APD currently employs a BWC 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 APD 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 APD records.

Audit Conclusions

In our opinion, the Atwater Police Department's Body-Worn Camera Program is substantially compliant with Minnesota Statutes §13.825 and §626.8473:

_____

Daniel E. Gazelka

Rampart Defense LLC

7/28/2022

APPENDIX A:

City of Atwater Minnesota
Use of Body-Worn Cameras Policy

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 officers must also attend to other primary duties and the safety of all concerned, sometimes in circumstances that are tense, uncertain, and rapidly evolving.

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

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 chief or chief's designee may supersede this policy by providing specific instructions for BWC use to individual officers, or providing specific instructions pertaining to particular events or classes of events, including but not limited to political rallies and demonstrations. The chief or 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:

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 Minnesota Cities.

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 officer.

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, 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 an officer's inadvertence or neglect in operating the officer's B WC, 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 officers 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 officer is on duty and performing authorized law enforcement services on behalf of this agency.

Use and Documentation

A. 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.

B. Officers who have been issued BWCs shall operate and use them consistent with this policy. Officers shall conduct a function test of their issued BWCs at the beginning of each shift to make sure the devices are operating properly according to manufacture guidelines. Officers noting a malfunction during testing or at any other time shall promptly report the malfunction to the officer's supervisor and shall document the report in writing on the mobile computer under file and an email sent to the Chief of Police.(malfunctions) Officers of the BWC will notify the Chief of Police when the malfunction occurs or when practical. Supervisors shall take prompt action to address malfunctions and document the steps taken in writing.

C. Officers should wear their issued BWCs at the location on their body and in the manner specified in training.

D. Officers must document BWC use and non-use as follows:

1. Whenever an officer makes a recording, the existence of the recording shall be documented in an incident report or [CAD record/other documentation of [the event].

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 or [CAD record/other documentation of the event]. Supervisors shall review these reports and initiate any corrective action deemed necessary.

E. The department will maintain the following records and documents relating to BWC use, which are classified as public data:

1. The total number of BWCs owned or maintained by the agency;
2. A daily record of the total number of BWCs actually deployed and used by officers 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.

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 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 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. If the recording is discontinued while an investigation, response, or incident is ongoing, 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 Atwater Police Department 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.

Special Guidelines for Recording

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

A. To use their BWCs to record any police-citizen encounter if there is reason to believe the recording would potentially yield information having evidentiary value, unless such recording is otherwise expressly prohibited.

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

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. 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. Officers should use their BWC to record their transportation and the physical transfer of persons in their custody to hospitals, detox and mental health care facilities, juvenile detention centers, and jails, 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

Each officer using a BWC is responsible for transferring or assuring the proper transfer of the data from his or her camera to the Mobile Computer BWC incidents file by the end of that 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, a supervisor or investigator shall take custody of the officer's BWC and assume responsibility for transferring the data from it.

Officers 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. Shall label the file with the Incident

Number or call for service number if a Incident number is not created. As well at labeling the nature of the creation of the media file IE (Evidence—Criminal)

A. Officers should assign as many of the following labels as are applicable to each file:

l. **Evidence—criminal**: The information has evidentiary value with respect to an actual or suspected criminal incident or charging decision.

The Records Retention Schedule for Minnesota Cities provides that retention periods for cases that have been charged are based on the status of court proceedings.) For uncharged offenses, retention is seven years or permanent in the case of homicide.

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.

These recordings must be maintained for six years regardless of the disposition of any related criminal case.

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.

Evidence/property logs are subject to a one-year minimal retention period

4. **Evidence—administrative:** The incident involved an adversarial encounter or resulted in a complaint against the officer.

The definition of "adversarial encounter " is intended to trigger the recording of interactions thought likely to result in complaints against an officer or the agency, Video that turns out to have evidentiary value in any internal investigation is subject to a six-year retention period. (Code POL 05880.).

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. **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.

Data not identified as having evidentiary value is subject to a 90-day retention period under Minn. Stat. 13.825, subd. 3(a).

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 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 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.

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 officer who collected the data.

   3. Any other officer whose voice or image is documented in the data, regardless of whether that officer is or can be identified by the recording.

B. **BWC data is presumptively private**. BWC recordings are classified as private data about the data subjects unless there is a specific law that provides differently. As a result:

   1. BWC data pertaining to people is presumed private, as is BWC data pertaining to businesses or other entities.

   2. Some BWC data is classified as confidential (see C. below).

   3. Some BWC data is classified as public (see D. below).

C. **Confidential data.** BWC data that is collected or created as part of an active criminal investigation is confidential. This classification takes precedence over the "private" classification listed above and the "public" classifications listed below.

D. **Public data**. The following BWC data is public:

   1. 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 officers must be redacted.

   4. Data that documents the final disposition of a disciplinary action against a public employee.

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

E. **Access to BWC data by non-employees.** Officers shall refer members of the media or public seeking access to BWC data to the Chief of Police, 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.

3. 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:

   a. Data on other individuals in the recording who do not consent to the release must be redacted.

   b. Data that would identify undercover officers must be redacted.

   c. Data on other officers 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 officers and law enforcement employees.** No employee may have access to the department's BWC data except for legitimate law enforcement or data administration purposes:

l. 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.

2. Agency personnel shall document their reasons for accessing stored BWC data in the file located on the mobile computer (Officer BWC requests form and emailed to the Chief of Police 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.

3. Employees seeking access to BWC data for non-business reasons may make a request for it in the same manner as any member of the public.

G. **Other authorized disclosures of data.** 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 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,

l. 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.

Data Security Safeguards

A. Backup copies made of the BWC media will be filed by year on the mobile computer as well as on an external hard drive with a lock password for both devices with the backup external hard drives being stored in evidence.

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

D. 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.

Agency Use of Data

A. At least once a month, supervisors will randomly review BWC usage by each officer to ensure compliance with this policy and to identify any performance areas in which addition training or guidance is required.

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 officer 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. Officers should contact their supervisors to discuss retaining and using BWC footage for training purposes. Officer 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.

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:

l. Data that documents the use of deadly force by a peace officer, or force of a sufficient type or degree to require a use of force report or supervisory review.

2. Data documenting circumstances that have given rise to a formal complaint against an officer.

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, all other B WC footage that is classified as non-evidentiary, becomes classified as non-evidentiary, or is not maintained for training shall be destroyed after 90 days.

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.

F. The department shall maintain an inventory of BWC recordings having evidentiary value.

G. The department will post this policy, together with its Records Retention Schedule, on its website.

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.

Use, availability, logistics and discretion

It will be at the discretion of the Chief to allow officers to decide whether to wear, use or activate the BWC during a shift. Due to various logistical restrictions a BWC may not always be available for use during a shift. It will not be considered a policy violation if an officer chooses not to utilize the BWC during a shift if approved by the chief or if a BWC is not available for use due to logistical restrictions or mechanical and or technological failure. The Chief may choose not to utilize a BWC.

Storage agreement

The Atwater Police Department will enter into a digital data storage agreement with the Kandiyohi County Sheriff's Office. The city of Atwater will purchase the BWC. The digital data will be uploaded, stored and maintained by the Kandiyohi County Sheriff's Office

NOTHING FOLLOWS