



# INDEPENDENT AIDITOR'S REPORT

---

Wyoming Police Department Body-Worn Camera Program



## **Audit Overview and Recommendations**

Dear Wyoming City Council and Chief Bauer:

We have audited the body-worn camera (BWC) program of the Wyoming Police Department (WPD) for the period of 10/09/2020 – 10/08/2022. Minnesota Statute §13.825 mandates that any law enforcement agency operating a portable recording system (PRS)<sup>1</sup> program obtain an independent, biennial audit of its program. This program and its associated data are the responsibility of the Wyoming Police Department. Our responsibility is to express an opinion on the operations of this program based on our audit.

On November 14, 2022, Rampart Defense LLC (Rampart) met with Property and Technology Technician/Crime Analyst Kallie Rezny, who provided information about WPD’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 WPD’s recordkeeping.

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

### **WPD 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.

Technician Rezny provided documentation showing that the public notification, comment and meeting requirements had been satisfied prior to the implementation of WPD’s BWC program on December 15, 2020. Specifically, Technician Rezny furnished the following:

1. A screenshot of the public notice posted on WPD’s website announcing their plan to implement a BWC program and inviting the public to provide comments electronically, by mail or in person at the November 4, 2020, meeting of the Wyoming City Council.

---

<sup>1</sup> 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 WPD, these terms may be used interchangeably in this report.

2. The minutes of the November 4, 2020, Wyoming City Council meeting, which noted that the council opened a public hearing to consider “a policy for Body Worn Portable Audio/Video Recording Device.” The minutes documented questions submitted by members of the public as well as city council members. After discussing these questions with the Public Safety Director, the city council voted unanimously to approve the proposed BWC policy.

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

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

Rampart staff verified that the Wyoming Police Department’s written BWC policy was accessible on their webpage at the time of our audit; however, locating the policy required entering a term such as “body worn camera” into a search box on the site. Prior to the issuance of this report, we verified that WPD had added a working link to the BWC policy on the Police Policies and Publications page.

#### **WPD BWC WRITTEN POLICY**

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

### **WPD BWC Data Retention**

Section 2.8-11 of WPD's BWC policy states that "[a]ll recordings shall be retained for a period consistent with the requirements of the organization's records retention schedule but in no event for a period of less than 180 days." The retention schedule also addresses the individual data categories identified in §13.825 Subd. 3 and specifies a retention period that meets or exceeds the statutory requirement for each.

WPD employs Axon body-worn cameras and manages BWC data retention on Evidence.com, Axon's secure, cloud-based data management system, 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.

WPD's BWC policy requires that each officer transfer data from his or her body-worn camera to the appropriate storage location 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.

We noted that Section 2.8-11 states: "If an individual captured in a recording submits a written request, the recording **may** be retained for an additional time period," while §13.825 Subd. 3 states: "...the law enforcement agency **shall** retain the recording for an additional time period..." [emphasis added]. Prior to completion of this report, WPD furnished an amended copy of the BWC policy that replaces "may" with "shall" to reflect the statutory language.

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

### **WPD BWC Data Destruction**

Technician Rezny advised us that WPD BWC data are stored on Axon's Evidence.com cloud service. Data are destroyed through automated deletion, based on a retention schedule assigned to each video. In addition, both Technician Rezny and the officer who created the video are notified via email prior to any deletion. Only Technician Rezny and a second administrator have the ability to schedule videos for manual deletion, and all such videos are queued for seven days to allow time for review prior to deletion.

Axon certifies that Evidence.com is compliant with the current FBI CJIS Security Policy, and notes that it has signed a CJIS Security Addendum with all 50 states. Axon specifically identifies Minnesota as one of the states with which it has worked to establish statewide CJIS-related vendor requirements.

FBI CJIS Security Policy specifies that digital media used to store CJIS data shall be overwritten at least three times or degaussed prior to disposal or release for reuse by unauthorized individuals, while inoperable digital media shall be destroyed through mechanical means, such as shredding.

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

### **WPD BWC Data Access**

Any request for access to BWC data by data subjects would be made in writing to Technician Rezny, who is the data practices designee. She is then responsible for reviewing and fulfilling each request in accordance with the provisions of §13.825 Subd. 4(b). Media requests for BWC data are directed to Chief Bauer.

WPD BWC data is shared with other law enforcement agencies for evidentiary purposes only. All such requests must be made by email to Technician Rezny or a second administrator. Existing verbal agreements between WPD and other area law enforcement agencies address data classification, destruction and security requirements, as specified in §13.825 Subd. 8(b). During the audit, WPD advised that they will evaluate adding a written acknowledgment of these requirements from requesting agencies.

Access to WPD BWC data for outside agencies is ordinarily provided via expiring email link. WPD identified one instance in which it was necessary to download a particularly large file to a USB memory stick.

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

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

### **WPD BWC Data Classification**

WPD 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.

### **WPD BWC Internal Compliance Verification**

The Agency Use of Data section of the WPD BWC policy states that "[s]upervisors and other assigned personnel may access portable audio/video recording device 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," while the Coordinator section notes that the coordinator shall establish "procedures for logging or auditing access."

Technician Rezny advised us that supervisors conduct random spot checks to monitor for compliance with the BWC policy; however, this is not stated in the policy. Minnesota Statute §626.8473 Subd.

3(b)(8) requires that a written BWC policy must include “procedures to ensure compliance and address violations of the policy, which must include, at a minimum, supervisory or internal audits and reviews...” In our opinion, while WPD is compliant with the review requirement in practice, they are not compliant with the requirement to document such procedures in the written BWC policy.

Prior to the issuance of this report, Wyoming PD furnished a revised BWC policy adding the following language: “The Chief or designee will conduct monthly supervisory and/or internal audits and reviews to ensure compliance with the BWC policy.”

We have attached a copy of the revised policy to this report as Appendix B.

The Access to Portable Audio/Video Recording Device Data states that “[a]gency personnel shall document their reasons for accessing stored portable audio/video recording device data... at the time of each access.” It prohibits accessing or sharing such data for non-law enforcement purposes and states that: “[a]ny Member of the Department who accesses or releases recordings without authorization may be subject to discipline.”

In our opinion, these sections of the revised policy are compliant with the applicable internal compliance and disciplinary requirements as of the date of this report.

### **WPD BWC Program and Inventory**

WPD currently possesses 10 Axon body-worn cameras.

The WPD 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.

The WPD BWC policy states that “[o]fficers shall check their issued portable audio/video recording devices at the beginning of each shift to make sure the devices are functioning properly...” Technician Rezny advised that this is accomplished through a device status check.

While WPD does not maintain a separate log of BWC deployment or use, Technician Rezny advised us that because each uniformed officer 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 WPD payroll records. In addition, non-uniformed personnel are issued and authorized but not required to wear or use body-worn cameras. Actual BWC use would be determined based on the creation of BWC data.

As of the date of the audit, WPD maintained 6,023 files of BWC data.

### **WPD BWC Physical, Technological and Procedural Safeguards**

WPD BWC data are initially recorded to an internal hard drive in each officer’s BWC. Those files are then transferred to Evidence.com through a docking station located at Wyoming Police Department.

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

As noted above, requests by other law enforcement agencies for WPD BWC data must be approved by Technician Rezny or a second administrator and are fulfilled via expiring email link. A similar method is employed to submit WPD BWC data to prosecutors.

### **Enhanced Surveillance Technology**

WPD 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.

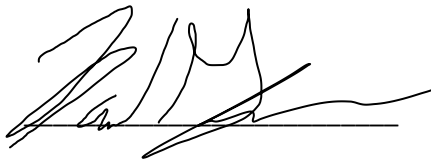
If WPD should obtain such enhanced technology in the future, Minnesota Statute §13.825 Subd. 10 requires notice to the Minnesota Bureau of Criminal Apprehension within 10 days. This notice must include a description of the technology and its surveillance capability and intended uses.

### **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 WPD records.

### **Audit Conclusions**

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



Daniel E. Gazelka

Rampart Defense LLC

03/20/2023

## Appendix A:

Police Department Date 12/01/2020 Number 2-8 Retention Permanent Type Policy To: ALL POLICE DIVISION PERSONNEL Subject: PORTABLE AUDIO/VIDEO RECORDING DEVICES INDEX 2-8.01 DEFINITIONS 2-8.02 DEPARTMENTAL PRIVACY EXPECTATION 2-8.03 USE AND DOCUMENTATION 2-8.04ACTIVATION OF THE PORTABLE AUDIO/VIDEO RECORDING DEVICES 2-8.05SPECIAL GUIDELINES FOR RECORDING 2-8.06EXPLOSIVE DEVICE 2-8.07 IDENTIFICATION AND PRESERVATION OF RECORDINGS 2-8.08ACCESS TO PORTABLE AUDIO/VIDEO RECORDING DEVICE DATA 2-8.09AGENCY USE OF DATA 2-8.10 COORDINATOR 2-8-11 DATA RETENTION POLICY The Wyoming Police Department may provide members with access to portable audio/video recording devices for the use during the performance of their duties. The use of recorders is intended to enhance the mission of the Department by accurately capturing contacts between members of the Department and the public. PURPOSE This policy is to provide guidelines for the use of portable audio/video recording devices by members of the Wyoming Police Department while in performance of their duties (Minn. Stat. § 626.8473 and 13.825) Compliance with this policy will provide for an exacting detailed record of contacts the members of the Department have with the public. While showing accountability and transparency to the public with the balance of keeping the privacy concerns of those being recorded a priority. SCOPE This policy governs the use of portable audio/video recording devices and data pertained by those devices in the course of official duties and applies to all members of the Wyoming Police Department. It does not apply to the use surreptitious recording devices in undercover operations, surveillance videos, wiretaps or eavesdropping (concealed listening devices), or the use of squad-based (dash-cam) video recorders. The Chief or Chief's designee may supersede this policy by providing specific instructions for the use of portable audio/video recording devices to individual officers, or providing specific instructions for the use of portable audio/video recording devices pertaining to certain events or classes of events, including but not limited to political rallies and demonstrations. 2-8.01 DEFINITIONS A. Portable audio/video recording devices– A device worn by a member that is capable of both video and audio recording of the member's activities and interactions with others or collecting digital multimedia evidence as part of an investigation and as provided in Minn. Stat. § 13.825. B. Official Duties – For purposes of this policy, official duties means that the officer is on-duty and performing authorized law enforcement services on behalf of the Wyoming Police Department. C. Law Enforcement Related Information – means information captured or available for capture by use of a portable audio/video recording devices 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/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 their 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 portable audio/video recording device, 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 restrooms, locker rooms, 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.

**2-8.02 DEPARTMENTAL PRIVACY EXPECTATION** All recordings made by members on any department-issued device at any time or while acting in an official capacity of this department, regardless of ownership of the device, shall remain the property of the Department. Members shall have no expectation of privacy or ownership interest in the content of these recordings.

**2-8.03 USE AND DOCUMENTATION**

A. Officers may use only department-issued portable audio/video recording devices while on-duty or in the performance of their official duties for the Wyoming Police Department or when otherwise performing authorized law enforcement services as an employee of this department. B. Officers who have been issued portable audio/video recording devices shall operate and use them consistent with this policy. Officers shall check their issued portable audio/video recording devices 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 and obtain a functioning device as soon as reasonably practicable. C. Officers should wear their issued portable audio/video recording devices at the location on their body and in the manner specified in training. D. Officers must document portable audio/video recording devices use and nonuse as follows: a. Whenever an officer makes a recording, the existence of the recording shall be documented in their report or other official record of the contact. b. In any instance where the device malfunctions, Officers shall document the malfunction in their report or other official record of the contact. c. In any instance where the officer deemed privacy to outweigh law enforcement interest and the audio or video was intentionally blocked, the officer must document the circumstances and reasons for why the function was intentionally blocked in their report or other official record of the contact. d. Whenever an officer fails to record an activity that is required to be recorded under this policy or captures only part of the activity, the officer must document the circumstances and reasons for not recording in their report or other official record of the contact. Supervisors shall review these reports and initiate any corrective action deemed necessary.

**2-8.04 ACTIVATION OF THE PORTABLE AUDIO/VIDEO RECORDING DEVICES** This policy is not intended to describe every possible situation which the recorder should be used, although there are many situations where its use is appropriate. Officers shall activate the recorder any time the officer believes it would be appropriate or valuable to record an incident. The recorder shall be activated in any of the following situations: A. Officers shall activate their portable audio/video recording devices when responding to all calls or 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 their 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)(d) (above). B. Officers have discretion to record or not record general citizen contacts. C. Officers have no affirmative duty to inform people that a portable audio/video recording devices is being operated or that they are being recorded. D. Once activated, the portable audio/video recording devices 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. Officers shall state the reasons for ceasing the recording on camera before deactivating their portable audio/video recording devices. 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 portable audio/video recording devices audio or visual recording functionality to defeat the purpose of this policy, unless privacy outweighs law enforcement interest. If a concern regarding privacy occurs only one function (either audio or video) may be blocked at a time. F. Notwithstanding any other provisions in this policy, officers shall not use their portable audio/video recording devices to record other agency personnel during non-enforcement related activities, such as during pre- and post-shift time, 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 portable audio/video recording devices recording unless otherwise expressly authorized by the Chief or Chief's designee.

**2-8.05 SPECIAL GUIDELINES FOR RECORDING** Officers may, in the exercise of sound discretion, determine: A. To use their portable audio/video recording devices 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 portable audio/video recording devices 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. C. Officers shall use their portable audio/video recording devices to record their transportation and the physical transfer of persons in their custody.

**2-8.06 EXPLOSIVE DEVICE** Many portable recorders, including body-worn cameras and audio/video transmitters, emit radio waves that could trigger an explosive device. Therefore, these devices should not be used where an Officer reasonably believes an explosive device to be present.

**2-8.07 IDENTIFICATION AND PRESERVATION OF RECORDINGS** A. Each officer using a portable audio/video recording device is responsible for transferring or assuring the proper transfer of the data from their device to the specified data storage location by the end of that officer's shift. However, if the officer is involved in a shooting, an in-custody death, or other law enforcement activity resulting in death or great bodily harm, a supervisor shall take custody of the officer's portable audio/video recording device and assume responsibility for transferring the data from it. B. Officers shall label the portable audio/video recording device 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. Officers should assign as many labels as are applicable to each file. An Officer should label recordings when he/she reasonably believes: a) The recording contains evidence relevant to potential criminal, civil or administrative matters. b) A complainant, victim or witness has requested non-disclosure. c) A complainant, victim or witness has not requested non-disclosure but the disclosure of the recording may endanger the person and/or their property. d) Disclosure may be an unreasonable violation of someone's privacy. e) Medical or mental health information is contained. f) Disclosure may compromise

an under-cover officer or confidential informant. Any time an officer reasonably believes a recorded contact may be beneficial in a non-criminal matter (example: a hostile contact), the officer should promptly notify a supervisor of the existence of the recording. C. In addition, officers shall label each file as appropriate to indicate that it contains information about data subjects who may have rights under the Minnesota Government Data Practices Act (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. D. Labeling designations may be corrected or amended based on additional information.

2-8.08 ACCESS TO PORTABLE AUDIO/VIDEO RECORDING DEVICE DATA SPECIFY DATA SAFEGUARDS TO BE USED A. Personally owned devices, including but not limited to computers and mobile devices, shall not be programmed or used to access or view portable audio/video recording device data. B. Officers may access and view stored portable audio/video recording device data only when there is a business need for doing so, including the need to defend against an allegation of misconduct or substandard performance. Except as provided in the critical incident response policy, 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. C. Officers may display portions of portable audio/video recording device 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. D. Agency personnel shall document their reasons for accessing stored portable audio/video recording device data as specified in training at the time of each access. Agency personnel are prohibited from accessing portable audio/video recording device data for non-business reasons and from sharing the data for non-law enforcement related purposes, including but not limited to uploading portable audio/video recording device data recorded or maintained by this agency onto public and social media websites, unless otherwise expressly authorized by the Chief or the Chief's designee. Any Member of the Department who accesses or releases recordings without authorization may be subject to discipline. (Minn. Stat. § 626.8473) E. Officers shall refer members of the media or public seeking access to portable audio/video recording device data to the data practices designee, who will process the request in accordance with the MGDPA and other governing laws. Employees seeking access to portable audio/video recording device data for non-business reasons may make a request for it in the same manner as any member of the public, reference section 2-8.11. F. Portable audio/video recording device data shall be made available to prosecutors, courts, and other criminal justice entities as provided by law.

2-8.09 AGENCY USE OF DATA A. Supervisors and other assigned personnel may access portable audio/video recording device 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 portable audio/video recording device data as evidence of misconduct or as a basis for discipline. C. This agency will conduct a

biennial audit to check for the occurrence of unauthorized access to portable audio/video recording device data as required by Minn. Stat. § 13.825, Subd. 9. D. Officers should contact their supervisors to discuss retaining and using portable audio/video recording device 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 portable audio/video recording device data with trainees for the purpose of providing coaching and feedback on the trainee's performance as authorized by a supervisor.

2-8.10 COORDINATOR The Chief of Police or the authorized designee should designate a coordinator responsible for:

- A. Establishing procedures for the security, storage and maintenance of data and recordings.
  - a. The coordinator will work to ensure that procedures comply with requirements of the MGDPA and other applicable laws (Minn. Stat. § 13.01 et seq.) (See the protected Information and the Records Maintenance and Release Appendix section 2-8.11).
- B. Establishing procedures for accessing data and recording.
  - a. These procedures should include the process to obtain written authorization for access to non-public data by Wyoming PD members and members of other governmental entities and agencies.
- C. Establishing procedures for logging or auditing access.
- D. Establishing procedures for transferring, downloading, tagging or marking events.
- E. Establishing an inventory of portable recorders including:
  - a. Total number of devices owned or maintained by Wyoming Police Department.
  - b. Daily record of the total number deployed and used by members.
  - c. Total amount of recorded audio and video data collected by the devices and maintained by the Wyoming Police Department.
- F. Preparing the biennial audit required by Minn. Stat. § 13.825 Subd. 9.
- G. Notifying the Bureau of Criminal Apprehension (BCA) in a timely manner when new equipment is obtained by the Wyoming Police Department that expands the type or scope of surveillance capabilities of the department's portable recorders.

2.8-11 DATA RETENTION

- A. All recordings shall be retained for a period consistent with the requirements of the organization's records retention schedule but in no event for a period less than 180 days.
- B. If an individual captured in a recording submits a written request, the recording may be retained for an additional time period. The coordinator should be responsible for notifying the individual prior to destruction of the recording (Minn. Stat. § 13.825).
- C. Requests for the release of audio/video recordings shall be processed in accordance with the Records Maintenance and Release Appendix.
- D. Except as provided by Minn. Stat. § 13.825, Subd. 2, audio/video recordings are considered private or nonpublic data. Any person captured in a recording may have access to the recording. If the individual requests a copy of the recording and does not have the consent of other non-law enforcement individuals captured on the recording, the identity of those individuals must be blurred or obscured sufficiently to render the subject unidentifiable prior to release. The identity of on-duty peace officers may not be obscured unless their identity is protected under Minn. Stat. § 13.82, Subd. 17.
- E. Records Maintenance and Release Appendix.

NAME RETENTION DURATION CATEGORY RESTRICTIONS

|                           |                        |              |
|---------------------------|------------------------|--------------|
| Uncategorized             | Until Manually Deleted | Unrestricted |
| Accident                  | 3 Years                | Unrestricted |
| Citation                  | 3 Years                | Unrestricted |
| DUI                       | 7 Years                | Unrestricted |
| Emergency Response        | 180 Days               | Unrestricted |
| Evidence - Criminal       | 7 Years                | Unrestricted |
| Evidence - Force          | 7 Years                | Unrestricted |
| Evidence - Other          | 3 Years                | Unrestricted |
| Evidence - Property       | 1 Year                 | Unrestricted |
| Evidence - Administrative | 1 Year                 | Unrestricted |
| Health Info               | 180 Days               | Unrestricted |
| Homicide                  | Until Manually Deleted | Unrestricted |
| Investigation             | 180 Days               | Unrestricted |
| Non Disclosure Flag       | 180 Days               | Restricted   |
| Not Evidence              | 180 Days               | Unrestricted |
| Officer Injury            | 7 Years                | Unrestricted |
| Officer Involved Shoot    | 20 Years               | Restricted   |
| Pending Review            | Until Manually Deleted | Unrestricted |
| Pursuit                   | 7 Years                | Unrestricted |
| Traffic Stop              | 180 Days               | Unrestricted |
| Training Demo             | 180 Days               | Unrestricted |
| Use of Force              | 7 Years                | Unrestricted |

# Appendix B:

Wyoming Police Department Manual Wyoming Police Department Policy: 109 1 of 9 Original Date: 03/14/2023 Updated Date: 03/16/2023 Policy Number: 109 Retention: Permanent To: All Police Division Personnel Subject: Body Worn Camera Policy Index

|   |   |
|---|---|
| Policy.....   | 2 |
| Purpose   | 2 |
| .....   | 2 |
| Scope.....  | 2 |
| 2   |   |
| Definitions.....                                      | 2 |
| Adversarial .....                                     | 2 |
| Body Worn Camera(s) aka BWC.....                      | 2 |
| Brady-Giglio Impaired .....                           | 2 |
| Critical Incident.....                                | 3 |
| Evidentiary Value .....                               | 3 |
| Incidental Citizen Contact.....                       | 3 |
| Law Enforcement-Related Information .....             | 3 |
| MGDPA or Data Practices Act.....                      | 3 |
| Records Retention Schedule.....                       | 3 |
| Official Duties/Capacity .....                        | 3 |
| Unintentionally Recorded Footage.....                 | 3 |
| Use and Documentation                                 |   |
| .....   | 4 |
| 4 Activation of the Body Worn Camera Devices.....     | 4 |
| 4 Identification and Preservation of Recordings ..... | 5 |
| 5 Access to BWC Device Data .....                     | 6 |
| 6 Agency Use of Data.....                             | 7 |
| 7   |   |
| Coordinator.....                                      | 7 |
| Data Retention.....                                   | 8 |
| 8   |   |
| Categories and Retention Schedule.....                | 9 |
| 9   |   |

Wyoming Police Department Manual Wyoming Police Department Policy: 109 2 of 9 Policy It is the policy of this department to authorize and/or require the use of department-issued BWCs as set forth below as required by M.S. section 626.8473, subd.3. Purpose This policy is to provide guidelines for the use of BWC by members of the Wyoming Police Department while in performance of their duties (Minn. Stat. § 626.8473 and 13.825) Compliance with this policy will provide for a detailed record of contacts

the members of the Department have with the public, while showing accountability and transparency to the public with the balance of keeping the privacy concerns of those being recorded a priority. 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, if available. The chief or chief's designee may modify 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 chief or chief'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. Officers deemed to be Brady-Giglio impaired must wear and utilize their BWC in all public contacts while serving in their official capacity. Definitions The following phrases have special meanings as used in this policy:

**Adversarial** A law enforcement encounter 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 their own are deemed adversarial.

**Body Worn Camera(s) aka BWC** Refers to a portable recording system as defined in M.S. 13.825, sub 1(b)(1) as a device worn by a peace officer that is capable of both video and audio recording of the officer's activities and interactions with others or collecting digital multimedia evidence as part of an investigation.

**Brady-Giglio Impaired** Wyoming Police Department Manual Wyoming Police Department Policy: 109 3 of 9 Brady-Giglio impaired means that a police officer has engaged in certain qualifying conduct established by the Chisago County Attorney that may necessitate disclosure as part of the prosecution or defense of a criminal defendant (see Policy 612). A police officer deemed to have a Brady impairment shall have additional BWC use expectations as identified within this policy.

**Critical Incident** Refers to an encounter between a police officer and community member(s) that results in great bodily harm or death to a community member. A critical incident could include an officer use of force or deadly force encounter between a police officer and a member of the community. A critical incident may also include an in-custody death of a person under the care, custody, or control of an officer.

**Evidentiary Value** Information that 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 department or officer. Note: "[R]elated civil or administrative proceeding" refers, for example, to implied consent or forfeiture actions arising from an arrest or prosecution. Nothing in this policy obligates the department to collect or maintain BWC data solely for use in third party tort litigation.

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

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

**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 retention schedule adopted by the Wyoming Police Department.

**Official Duties/Capacity** For purposes of this policy, means that the officer is on duty and/ or performing authorized law enforcement services on behalf of this department or while in

uniform. Unintentionally Recorded Footage 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 Wyoming Police Department Manual Wyoming Police Department Policy: 109 4 of 9 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. Use and Documentation Officers may use only department-issued BWCs in the performance of official duties for this department or when otherwise performing authorized law enforcement services as an employee of this department. Note: This provision prohibits officers from using personally owned BWCs, or those provided by private entities that may be contracting for services, while performing department authorized law enforcement activities. The use of non-department equipment is inconsistent with the department's obligation to administer resulting video footage as government data. Officers who have been issued BWC devices shall operate and use them consistent with this policy. Officers shall check their issued BWC devices 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 and obtain a functioning device as soon as reasonably practicable. Officers shall wear their issued BWCs at the location on their body and in the manner specified in training or which maximizes viewable video images. Officers must document BWC devices use and nonuse as follows: A. Whenever an officer makes a recording, the existence of the recording shall be documented in their report or other official record of the contact. B. In any instance where the device malfunctions, Officers shall document the malfunction in their report or other official record of the contact. C. In any instance where the officer deemed privacy to outweigh law enforcement interest and the audio or video was intentionally blocked, the officer must document the circumstances and reasons for why the function was intentionally blocked in their report or other official record of the contact. D. Whenever an officer fails to record an activity that is required to be recorded under this policy or captures only part of the activity, the officer must document the circumstances and reasons for not recording in their report or other official record of the contact. Activation of the Body Worn Camera Devices This policy is not intended to describe every possible situation which the recorder should be used, although there are many situations where its use is appropriate. Officers shall activate the BWC any time the officer believes it would be appropriate or valuable to record an incident. The BWC shall be activated in any of the following situations: A. Officers shall activate their BWC devices when responding to calls or 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 their activities likely to yield information having evidentiary value. However, Wyoming Police Department Manual Wyoming Police Department Policy: 109 5 of 9 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. 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 recording devices 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. Officers are strongly encouraged to state the reasons for ceasing the recording on camera before deactivating their BWC

devices. If circumstances change, officers shall reactivate their cameras as required by this policy to capture information having evidentiary value. E. Officers should remain sensitive to the dignity of all individuals being recorded and exercise sound discretion to respect privacy by discontinuing recording whenever it reasonably appears to the officer that such privacy may outweigh any legitimate law enforcement interest in recording. Requests by members of the public to stop recording should be considered using this same criterion. Recording should resume when privacy is no longer at issue unless the circumstances no longer fit the criteria for recording. F. Notwithstanding any other provisions in this policy, officers shall not use their BWC devices to record other agency personnel during non-enforcement related activities, such as during pre and post-shift time, 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 Chief or Chief's designee. H. Officers assigned to a plain clothes, investigative assignment, undercover assignment, or uniformed administrative role shall not be required to wear a BWC during their day-to-day work unless working in a uniformed call response capacity or are otherwise required by this policy or a command-level directive. Command staff members shall have discretion to not wear a BWC.

**Identification and Preservation of Recordings** Each officer using a BWC device is responsible for transferring or assuring the proper transfer of the data from their device to the specified data storage location by the end of that officer's shift. However, if the officer is involved in a shooting, an in-custody death, or other law enforcement activity resulting in death or great bodily harm, a supervisor shall take custody of the officer's BWC device and assume responsibility for transferring the data from it. Officers shall label the BWC device 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. Officers should assign as many labels as are applicable to each file. An officer should label recordings when they reasonably believe:

- A. The recording contains evidence relevant to potential criminal, civil or administrative matters.
- B. A complainant, victim, or witness has requested non-disclosure. Wyoming Police Department Manual Wyoming Police Department Policy: 109 6 of 9
- C. A complainant, victim, or witness has not requested non-disclosure but the disclosure of the recording may endanger the person and/or their property.
- D. Disclosure may be an unreasonable violation of someone's privacy.
- E. Medical or mental health information is contained.
- F. Disclosure may compromise an under-cover officer or confidential informant.

Any time an officer reasonably believes a recorded contact may be beneficial in a non-criminal matter (example: a hostile contact), the officer should promptly notify a supervisor of the existence of the recording. In addition, officers shall label each file as appropriate to indicate that it contains information about data subjects who may have rights under the Minnesota Government Data Practices Act (MGDPA) limiting public disclosure of information about them. These individuals include:

- A. Victims and alleged victims of Criminal Sexual Conduct;
- B. Victims of child abuse or neglect;
- C. Vulnerable adults who are victims of maltreatment;
- D. Undercover officers;
- E. Informants;
- F. When the video is clearly offensive to common sensitivities;
- G. Victims of and witnesses to crimes, if the victim or witness has requested not to be identified publicly;
- H. Individuals who called 911, and services subscribers whose lines were used to place a call to the 911 system;
- I. Mandated reporters;
- J. Juvenile witnesses, if the nature of the event or activity justifies protecting the identity of the witness;
- K. Juveniles who are or may be delinquent or engaged in criminal acts;
- L. Individuals who make complaints about violations with respect to the use of real property;
- M. Officers and employees who are the subject of a complaint related to the events captured on video;
- N. Other individuals whose identities the officer believes may be legally protected from public disclosure; or
- O. Labeling designations may be corrected



or amended based on additional information. Access to BWC Device Data Personally owned devices, including but not limited to computers and mobile devices, shall not be programmed or used to access or view portable audio/video recording device data. Officers may access and view stored BWC device data only when there is a business need for doing so, including the need to defend against an allegation of misconduct or substandard performance. Except as provided in the critical incident response policy, 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. Wyoming Police Department Manual Wyoming Police Department Policy: 109 7 of 9 Officers may display portions of BWC device footage to witnesses as necessary for purposes of investigation as allowed by Minn. Stat. §13.82, sub. 15. Officers should limit these displays to protect against the incidental disclosure of individuals whose identities are not public. Agency personnel are prohibited from accessing BWC recording device data for non-business reasons and from sharing the data for non-law enforcement related purposes including, but not limited to, uploading BWC device data recorded or maintained by this agency onto public and social media websites, unless otherwise expressly authorized by the Chief or the Chief's designee. Any member of the Department who accesses or releases recordings without authorization may be subject to discipline. (Minn. Stat. § 626.8473) Officers shall refer members of the media or public seeking access to BWC device data to the data practices designee, who will process the request in accordance with the MGDPA and other governing laws. Employees seeking access to BWC device data for non-business reasons may make a request for it in the same manner as any member of the public. BWC device data shall be made available to prosecutors, courts, and other criminal justice entities as provided by law. Agency Use of Data Supervisors and other assigned personnel may access BWC device 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. Nothing in this policy limits or prohibits the use of BWC device data as evidence of misconduct or as a basis for discipline. This agency will conduct an independent biennial audit to check for the occurrence of unauthorized access to BWC recording device data as required by Minn. Stat. § 13.825, Sub. 9. The Chief or designee will conduct monthly supervisory and/or internal audits and reviews to ensure compliance with the BWC policy. Officers should contact their supervisors to discuss retaining and using BWC device 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 device data with trainees for the purpose of providing coaching and feedback on the trainee's performance as authorized by a supervisor. Coordinator The Chief of Police or the authorized designee should designate a coordinator responsible for: A. Establishing procedures for the security, storage and maintenance of data and recordings. 1. The coordinator will work to ensure that procedures comply with requirements of the MGDPA and other applicable laws (Minn. Stat. § 13.01 et seq.) B. Establishing procedures for accessing data and recording. Wyoming Police Department Manual Wyoming Police Department Policy: 109 8 of 9 1. These procedures should include the process to obtain written authorization for access to non-public data by Wyoming PD members and members of other governmental entities and agencies. C. Establishing procedures for logging or auditing access. D. Establishing procedures for transferring, downloading, tagging or marking events. E. Establishing an inventory of BWC including: 1. Total number of devices owned or maintained by Wyoming Police Department. 2. Daily record of the total number deployed and used by members. 3. Total amount of recorded audio and video data collected by the devices and maintained by the Wyoming Police Department. F. Preparing the biennial audit required by Minn. Stat. § 13.825 Subd. 9. G. Notifying the Bureau of Criminal Apprehension (BCA) in a timely manner when new equipment is obtained by the

Wyoming Police Department that expands the type or scope of surveillance capabilities of the department's BWC. Data Retention All recordings shall be retained for a period consistent with the requirements of the organization's records retention schedule, but in no event for a period less than 180 days. If an individual captured in a recording submits a written request, the recording shall be retained for an additional time period. The coordinator is required to notifying the individual prior to destruction of the recording (Minn. Stat. § 13.825). Requests for the release of audio/video recordings shall be processed in accordance with the Records Maintenance and Release Appendix. Except as provided by Minn. Stat. § 13.825, Subd. 2, audio/video recordings are considered private or nonpublic data. Any person captured in a recording may have access to the recording. If the individual requests a copy of the recording and does not have the consent of other non-law enforcement individuals captured on the recording, the identity of those individuals must be blurred or obscured sufficiently to render the subject unidentifiable prior to release. The identity of on-duty peace officers may not be obscured unless their identity is protected under Minn. Stat. § 13.82, Subd. 17. Wyoming Police Department Manual Wyoming Police Department Policy: 109 9 of 9 Categories and Retention Schedule

| Name                   | Retention Duration     | Category Restrictions   | Category Information  |
|------------------------|------------------------|---|---|
| Uncategorized          | Until Manually Deleted | Unrestricted  | Video not assigned a category (Officer forgot to choose a category) |
| Crash                  | 3 years                | Unrestricted  | Crash Arrest or Citation  |
| 7 years                | Unrestricted           | Arrest made and/or citation given   | Evidence  |
| 7 years                | Unrestricted           | Contains evidentiary value  | False Activation  |
| 180 days               | Unrestricted           | Accidental activation   | Not Evidence  |
| 180 days               | Unrestricted           | No evidentiary value  | Officer Injury  |
| 7 years                | Unrestricted           | Injury to officer   | Officer Involved Shoot  |
| 20 years               | Restricted             | Officer Involved Shoot Pending  | Review  |
| Until Manually Deleted | Unrestricted           | For administrative purposes, when a supervisory review of call/case/conduct is needed | Pursuit   |
| 7 years                | Unrestricted           | Pursuit Use of Force  | 7 years   |
| Unrestricted           | Force used             | CSC/Homicide  | Until Manually Deleted  |
| Restricted             | CSC/Homicide Case      |   |   |