INDEPENDENT AUDITOR'S REPORT

Warroad Police Department

SEPTEMBER 25TH, 2025

Audit Overview and Recommendations

Dear Warroad City Council and Chief Steinbring:

We have audited the body-worn camera (BWC) program of the Warroad Police Department (WPD) for the two-year period ended 3/31/2025. 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 Warroad Police Department. Our responsibility is to express an opinion on the operations of this program based on our audit.

On August 7, 2025, Rampart Audit, LLC (Rampart) met with Chief Wade Steinbring, who provided information about WPD's BWC program policies, procedures and operations. As part of the audit, 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.

Rampart previously audited WPD's BWC program in 2021 and 2023. As part of those audit, we were advised that WPD implemented its body-worn camera program in early 2016, prior to the adoption of Minn. Stat. §626.8473. WPD personnel indicated that the public comment requirements had most likely not been met. Because Minnesota Statute §626.8473 did not address pre-existing BWC programs, Rampart recommended WPD suspend use of its BWC program until those requirements could be satisfied.

Prior to the issuance of our 2021 audit report, Chief Steinbring submitted documentation to Rampart showing that WPD had posted a public notice soliciting comments about its BWC program and policy, and that the Warroad City Council had provided an opportunity for public comment at its regularly scheduled meeting on June 14, 2021. The council then adopted the WPD BWC program and policy at that same meeting. Once this was complete, WPD re-implemented their BWC program.

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

Copies of these documents have been retained in Rampart's audit files. In our opinion, Warroad Police Department is compliant with the public notice and comment requirements contained in §626.8473 Subd. 2.

Minn. Stat. §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 Steinbring furnished a copy of WPD's BWC policy as part of this audit. Warroad Police Department has a dedicated page on the City of Warroad website rather than its own standalone website; however, its BWC policy was not accessible on the WPD webpage at the time of our audit. In our opinion, an agency-specific page is functionally equivalent to a standalone website. Prior to the completion of this report, the policy was activate on the website.

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. A prohibition on altering, erasing or destroying any recording made with a peace officer's portable recording system or data and metadata related to the recording prior the expiration of the applicable retention period under section 13.825 Subdivision 3, except that the full, unedited, and unredacted recording of a peace officer using deadly force must be maintained indefinitely;
3. A mandate that a portable recording system be worn at or above the mid-line of the waist in a position that maximizes the recording system's capacity to record video footage of the officer's activities;
4. A mandate that officers assigned a portable recording system wear and operate the system in compliance with the agency's policy adopted under this section while performing law enforcement activities under the command and control of another chief law enforcement officer or federal law enforcement official;
5. A mandate that, notwithstanding any law to the contrary, when an individual dies as a result of a use of force by a peace officer, an involved officer's law enforcement agency must allow the deceased individual's next of kin, the legal representative of the deceased individual's next of kin, and the other parent of the deceased individual's child, upon their request, to inspect all portable recording system data, redacted no more than what is required by law, documenting the incident within five days of the request, with the following exception:
    - A law enforcement agency may deny a request if the agency determines that there is a compelling reason that inspection would interfere with an active investigation. If the agency denies access, the chief law enforcement officer must provide a prompt, written denial to the

individual who requested the data with a short description of the compelling reason access was denied and must provide notice that relief may be sought from the district court pursuant to section 13.82 subdivision 7;

6. A mandate that, when an individual dies as a result of a use of force by a peace officer, an involved officer's law enforcement agency shall release all portable recording system data, redacted no more than required by law, documenting the incident no later than 14 days after the incident, unless the chief law enforcement officer asserts in writing that the public classification would interfere with an ongoing investigation, in which case the data remain classified by section 13.82 subdivision 7;
7. Procedures for testing the portable recording system to ensure adequate functioning;
8. Procedures to address a system malfunction or failure, including requirements for documentation by the officer using the system at the time of a malfunction or failure;
9. Circumstances where recording is mandatory, prohibited, or at the discretion of the officer using the system;
10. Circumstances under which a data subject must be given notice of a recording;
11. Circumstances under which a recording may be ended while an investigation, response, or incident is ongoing;
12. Procedures for the secure storage of portable recording system data and the creation of backup copies of the data; and
13. Procedures to ensure compliance and address violations of the policy, which must include, at a minimum, supervisory or internal audits and reviews, and the employee discipline standards for unauthorized access to data contained in section 13.09.

In our opinion, the WPD BWC policy is compliant with respect to clauses 7 – 11.

Due to their complexity and interrelatedness, clauses 1 and 12 are discussed separately below. Clause 13 is also discussed separately.

Clauses 2 – 6 are newly added as a result of 2023 legislation and will also be discussed separately below.

WPD BWC Data Retention

Minn. Stat. §13.825 Subd. 3(a) establishes a minimum retention period of 90 days for all BWC data not subject to a longer retention period, while §13.825 Subd. 3(b) requires that the following categories of BWC data be retained for a minimum period of one year:

1) any reportable firearms discharge;
2) any use of force by an officer that results in substantial bodily harm; and
3) any incident that results in a formal complaint against an officer.

Meanwhile, Subd. 3(c) requires that any portable recording system data documenting a peace officer's use of deadly force must be maintained indefinitely. Finally, Subd. 3(d) requires that an agency retain BWC recordings for an additional period of up to 180 days when so requested in writing by a data subject.

WPD currently follows the General Records Retention Schedule for Minnesota Cities (GRRSMC), but also addresses the categories above separately within its BWC policy:

Part A of the Data Retention section of WPD's BWC policy states: "All BWC data shall be retained for a minimum period of 90 days. There are no exceptions for erroneously recorded or non-evidentiary data," which satisfies the requirements of §13.825 Subd. 3(a).

Part B of the Data Retention section of WPD's BWC policy specifies a minimum retention period of one year for "[d]ata 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…" Part C of the Data Retention section of WPD's BWC policy specifies a minimum retention period of six years for "[d]ata 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," as well as, "[d]ata documenting circumstances that have given rise to a formal complaint against an officer."

While Part C identifies "force of a sufficient type or degree to require a use of force report or supervisory review" as the threshold to prompt extended BWC retention rather than the "substantial bodily harm" threshold described in statute, it is our opinion that Warroad PD's BWC policy establishes a broader standard for retention that will result in additional BWC being subject to extended retention. In our opinion, the retention periods identified in Parts B and C of WPD's BWC policy meet or exceed the requirements of §13.825 Subd. 3(b).

As stated in the preceding paragraphs, Part C of the Retention section of WPD's BWC policy specifies a minimum retention period of six years for "[d]ata that documents the use of deadly force by a peace officer…" Because §13.825 Subd. 3(c) requires that such BWC data be retained indefinitely, WPD's BWC policy is not compliant with this requirement.

Part F of the Data Retention section of WPD's BWC policy states: "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…" This satisfies the requirements of §13.825 Subd. 3(d).

Part C of the Data Security Safeguards section of WPD's BWC policy states: "[o]fficers shall not intentionally edit, alter, or erase any BWC recording unless otherwise expressly authorized by the chief or the chief's designee." As discussed in Clause 2 of the Policy section of this report, a BWC policy must prohibit altering, erasing or destroying any recording made with a peace officer's portable recording system, as well as associated data or metadata, prior to the expiration of the applicable retention period. In our opinion, the language described above does not satisfy this requirement.

Prior to the issuance of this report, WPD submitted a revised BWC policy that addresses the retention issues noted in this section of the report. A copy of the revised policy is attached to this report as Appendix B.

WPD employs WatchGuard Vista WiFi WFC1 body-worn cameras and utilizes WatchGuard's Cloud storage service. WPD manages BWC data retention through automated retention settings in the Evidence Library 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. Chief Steinbring advised us that in the event an officer fails to assign a category to a BWC recording, the default retention period is two years to avoid the accidental loss of data.

The Downloading and Labeling Data section of WPD's BWC policy states that "[e]ach officer using a BWC is responsible for transferring or assuring the proper transfer of the data from his or her camera to the

secure storage system by the end of that officer's shift." Warroad Police Department employs a wireless upload system, with a physical docking station as a backup. Officers are required to assign the appropriate data label or labels to each file at the time of capture or transfer to storage.

Chief Steinbring advised us that WPD has a legacy BWC server in the office; however, the data on that server is also backed up to the Cloud.

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

WPD BWC Data Destruction

As discussed above, WPD's BWC data are stored on WatchGuard's cloud-based storage service, WatchGuard Cloud, with data retention and deletion schedules managed automatically through the Evidence Library video management software based on the assigned data classification of each video.

WatchGuard utilizes Microsoft's Azure Government environment for cloud storage. Microsoft certifies this environment as being compliant with the current Federal Bureau of Investigation Criminal Justice Information Services Division Security Policy, and notes that it has signed CJIS management agreements with 45 of the 50 U.S. states, including Minnesota, to verify compliance with state CJIS requirements.

FBI CJIS policy requires that hard drives used for CJIS data storage are sanitized by overwriting at least three times or degaussing prior to being released to unauthorized individuals, while inoperable drives must be destroyed through physical means such as shredding.

Chief Steinbring advised us that the BWC data stored on WPD's in-house server will be destroyed through manual deletion and overwriting when the server is retired from service. In addition, the drives will be physically destroyed through mechanical means, specifically by "drilling multiple holes through the drive ensuring it is unusable," according to the BWC policy. Chief Steinbring confirmed this process.

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

WPD BWC Data Access

The Access to BWC Data by non-employees subsection of the Administering Access to BWC Data section of WPD's BWC policy states: "[o]fficers shall refer members of the media or public seeking access to BWC data to [the] Chief, who shall process the request in accordance with the MGDPA [Minnesota Government Data Practices Act] and other governing laws." Chief Steinbring confirmed this process during the audit, noting that all requests are directed to him, and fulfilled using physical media such as a DVD or USB memory device. Chief Steinbring indicated that all such requests from the public are made verbally. We recommend obtaining these requests in writing.

The Other authorized disclosures of data subsection of the Administering Access to BWC Data section of WPD's BWC policy states: "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 request." All

such requests must be made to Chief Steinbring by the requesting agency's chief law enforcement officer (CLEO). These requests are normally made via email, which creates an audit trail. 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).

We recommend such requests continue to be made via email or in other written form, and include a brief explanation of the law enforcement purpose for the request. A file of these requests should be maintained for audit purposes.

The Other authorized disclosures of data subsection of the Administering Access to BWC Data section of WPD's BWC policy states: "BWC data shall be made available to prosecutors, courts, and other criminal justice entities as provided by law." Chief Steinbring advised us that the Roseau County Attorney's Office emails disclosure requests to him and he fulfills those requests via USB memory device.

As discussed in Clauses 5 and 6 of the Policy section of this report, the Minnesota State Legislature in 2023 added specific access requirements related to BWC data that document deadly force incidents, and specified that these requirements must be included in the agency's BWC policy. At the time of our audit, WPD's BWC policy did not address those requirements.

Prior to the issuance of this report, WPD submitted a revised BWC policy that addresses the requirements discussed in the preceding paragraph. In our opinion, this revised BWC policy is compliant with respect to the applicable data access requirements.

WPD BWC Data Classification

The Administering Access to Body Worn Camera Data section of WPD's BWC policy states that "BWC recordings are classified as private data about the data subjects unless there is a specific law that provides differently," and identifies those circumstances in which BWC data are instead classified as either confidential or public.

As discussed in the preceding section of this report, WPD's BWC policy does not address the requirements discussed in Clauses 5 and 6 of the Policy section of this report, which include the public classification of BWC data documenting an officer's use of deadly force.

Prior to the issuance of this report, WPD submitted a revised BWC policy that addresses the requirements discussed in the preceding paragraph.

In our opinion, this revised policy is compliant with respect to the applicable data classification requirements.

WPD BWC Internal Compliance Verification

The WPD BWC Agency Use of Data section states that: "At least once a month, supervisors will randomly review BWC usage by each officer to ensure compliance with this policy." Chief Steinbring advised us that he conducts audits at least monthly, and sometimes multiple times per week. The policy further states that: "Supervisors shall monitor for compliance with this policy. The unauthorized access to or

disclosure of BWC data may constitute misconduct and subject individuals to disciplinary action and criminal penalties pursuant to Minn. Stat. §13.09."

In our opinion, this fulfills the statutory requirements for supervisory review and employee discipline standards.

WPD's BWC policy does not address the requirement that a WPD officer assigned a BWC wear and operate it in compliance with WPD's BWC policy while performing law enforcement activities under the command control of another chief law enforcement officer or federal law enforcement official, as discussed in Clause 4 of the Policy section of this report.

Prior to the issuance of this report, WPD submitted a revised BWC policy that addresses this requirement.

WPD BWC Program and Inventory

WPD currently possesses six (6) WatchGuard Vista WiFi WFC1 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.

While WPD does not maintain a separate log of BWC deployment or use, Chief Steinbring advised us that because each patrol officer wears a BWC while on duty, the number of BWC units deployed each shift can be determined based on a review of WPD payroll records. BWC use would be determined based on the creation of BWC data.

As of 8/07/2025, WPD maintained 6,982 files of WatchGuard data. Chief Steinbring noted that this includes both BWC and squad camera recordings, and the system is unable to provide automated subtotals. Rampart has reviewed WatchGuard systems previously and has determined that while it is possible to separate BWC and squad recordings to determine individual totals, doing so requires reviewing recordings individually to determine classification.

WPD BWC Physical, Technological and Procedural Safeguards

WPD BWC data are initially recorded to a storage unit in each officer's body worn camera. Those data are then transferred via either a wireless connection or through a physical docking station to the WatchGuard Cloud service.

Officers have view-only access to their data for report writing, trial preparation and other legitimate law enforcement purposes. All such access is logged and can be reviewed by WPD supervisors.

As discussed above, WPD's BWC data are stored on WatchGuard's cloud-based service, with data retention and deletion schedules managed automatically through the Evidence Library video management software based on the assigned data classification of each video.

As noted above, requests by other law enforcement agencies for WPD BWC data must be approved by Chief Steinbring.

WPD's BWC policy does not address the requirement described in Clause 3 of the Policy section of this report, which mandates that a BWC policy specify that that a BWC be worn at or above the mid-line of the waist. Prior to the submission of this report, WPD furnished a revised BWC policy that satisfies this requirement.

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 calls for service from which to review any available BWC recordings. It should be noted that not every call will result in an officer activating his or her BWC. For example, an officer who responds to a driving complaint but is unable to locate the suspect vehicle would be unlikely to activate his or her BWC. It should also be noted that because the audit covers a period of two years, while most BWC data is only required to be retained for 90 days, there is a significant likelihood that the sample population will include calls for which BWC data was created, but which has since been deleted due to the expiration of the retention period. The auditors reviewed the retained BWC videos to verify that this data was accurately documented in WPD records.

The Rampart auditor noted that while BWC recordings in our sample were retained properly, labeling was inconsistent. We recommend that Chief Steinbring review labeling practices and expectations with WPD officers.

Audit Conclusions

In our opinion, the Warroad Police Department's Body-Worn Camera Program is substantially compliant with Minnesota Statute §13.825, with the following exception.

Rampart Audit, LLC

9/25/2025

APPENDIX A:

POLICY 3-3501	**SUBJECT: BODY WARN CAMERAS**
ISSUE DATE: 08/27/2025	**PERSONNEL:** LICENSED PEACE OFFICERS
REFERENCE:	**ISSUED BY:** CHIEF WADE STEINBRING

PURPOSE

The primary purpose of using BWCs is to capture evidence arising from police-citizen encounters. While this technology allows for the collection of valuable information, it opens many questions about how to balance public demands for accountability and transparency with the privacy concerns of those being recorded. In deciding what to record, this policy also reflects a balance between the desire to establish exacting and detailed requirements and the reality that officers must attend to their primary duties and the safety of all concerned, often in circumstances that are tense, uncertain, and rapidly evolving.

POLICY

It is the policy of 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. Unless otherwise prohibited by law, the chief or chief's designee may supersede this policy by providing specific instructions for BWC use to individual officers, or by 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 and words 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, depending on context, to the General Records Retention Schedule for Minnesota Cities (last revised March 2021) or to the agency's records retention schedule approved pursuant to Minnesota Statutes section 138.17. \

C. **Law enforcement-related** refers to activities or information pertaining to a stop, arrest, search, seizure, use of force, investigation, 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** refers to 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 BWC, provided that no portion of the resulting recording has evidentiary value. Examples of unintentionally recorded footage include, but are not limited to, recordings made in station house locker rooms and 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, refers to law enforcement activities and services performed by an officer of this agency while on duty. In circumstances where an officer is also employed by another agency as a peace officer, the officer is not performing official duties on behalf of this agency while acting in the course and scope of their employment for the other agency.

USE AND DOCUMENTATION

A. Officers may use only department issued BWCs while engaged in the performance of official duties.

B. Officers who are engaged in the performance of official duties and have been issued BWCs shall use and operate them in compliance with this policy. This requirement includes situations where the officer is under the command and control of another chief law enforcement officer or federal law enforcement official while performing official duties for this agency.

C. Officers shall conduct a function test of their issued BWCs at the beginning of each shift. Officers noting a malfunction during testing or at any other time shall promptly report it to the officer's supervisor and shall document the report in writing. Supervisors shall take prompt action to address malfunctions and document the steps taken in writing.

D. Officers shall wear their issued BWC at or above the midline of the waist in a position that maximizes the capacity of the device to record video footage of the officer's activities.

E. 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.

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

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

a. The total number of BWCs owned or maintained by the agency;

b. A daily record of the total number of BWCs actually deployed and used by officers;

c. The total amount of recorded BWC data collected and maintained; and

d. This policy, together with the applicable records retention schedule.

GENERAL GUIDELINES FOR RECORDING

A. Officers shall activate their BWCs when they become involved in, should reasonably anticipate becoming involved in, or when witnessing another officer engage 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 (E)(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, officers should continue recording with their BWCs 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 direct that recording be discontinued when additional recording is unlikely to capture information having evidentiary value. If the recording is discontinued while an investigation, response, or incident is ongoing, the officer shall state the reasons for ceasing the recording on camera before deactivating their BWC. If circumstances change, officers shall reactivate their cameras as required by this policy to capture information having evidentiary value.

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

F. Notwithstanding any other provision in this policy, officers shall not use their BWCs to record other agency personnel during non-enforcement related activities, such as during pre- and post-shift time in locker rooms, during meal breaks, or during other private conversations, unless the recording is authorized as part of an administrative or criminal investigation.

G. Officers shall not intentionally edit, alter, or erase any BWC recording made with a peace officer's portable recording system or data and metadata related to the recording prior the expiration of the applicable retention period under section 13.825 Subdivision 3, except that the full, unedited, and unredacted recording of a peace officer using deadly force must be maintained indefinitely.

SPECIAL GUIDELINES FOR RECORDING

Officers may, in the exercise of sound discretion, use their BWCs:

A. 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 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, the basis for any transport

   hold, 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 shall use their BWCs and squad-based audio/video systems to record their transportation and the physical transfer of persons in their custody to hospitals, detox and mental health care facilities, juvenile detention centers, and jails, but otherwise should not record in these facilities unless the officer anticipates witnessing a criminal event or being involved in or witnessing an adversarial encounter or use-of-force incident.

DOWNLOADING AND LABELING DATA

A. Each officer using a BWC is responsible for transferring or assuring the proper transfer of the data from their camera to the Motorola Solutions cloud 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.

B. Officers shall label the BWC data files at the time of capture or transfer to storage. Officers should consult with a supervisor if in doubt as to the appropriate labeling.

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

   2. **Evidence—force:** Whether or not enforcement action was taken or an arrest resulted, the event involved the application of force by an officer of this agency of sufficient degree or under circumstances triggering a requirement for supervisory review. Recordings that document the use of deadly are covered separately.

3. **Evidence—deadly force:** The event involved the application of deadly force by a peace officer, regardless of whether death occurred.

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

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.

C. 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 portions of the video are 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 made a complaint of a violation pertaining 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 and flagging designations may be corrected or amended based on additional information.

ADMINISTERING ACCESS TO BODY WORN CAMERA DATA

A. **Death resulting from force—access to data by survivors and legal counsel.** Notwithstanding any other law or policy to the contrary, when an individual dies as a result of force used by an officer of this agency, all BWC data documenting the incident, redacted only as required by law, must be made available for inspection by any of the following individuals within five days of their request:

1. The deceased individual's next of kin.

2. The legal representative of the deceased individual's next of kin.

3. The other parent of the deceased individual's child.

The request may be denied if there is a compelling reason that inspection would interfere with an active investigation. If access is denied, the chief of police must provide a prompt, written denial to the requestor with a short description of the compelling reason that access was denied. The written denial must also provide notice that relief may be sought from the district court pursuant to Minnesota Statutes section 13.82, subdivision 7.

B. **Death resulting from force—release of data to the public.** When an individual dies as a result of force used by an officer of this agency, all BWC data documenting the incident, redacted only as required by law, must be released and classified as public within 14 days after the incident, unless the chief of police asserts in writing that the public classification would interfere with an ongoing investigation, in which case the data remain classified by Minnesota Statutes section 13.82, subdivision 7.

C. **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.

D. **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* part E, below).

3. Some BWC data is classified as public (*see* part F, below).

E. **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 in part D, and the "public" classifications listed below in parts F(2)(a) and (b). However, special classifications and access rights are applicable to BWC data documenting incidents where an officer's use of force results in death (*see* parts A and B, above).

F. **Public data.**

1. Data that documents the final disposition of a disciplinary action against a public employee is classified as public without regard to any ongoing criminal investigation.

2. The following data is public unless it is part of an active criminal investigation or is subject to a more restrictive classification. For instance, data that reveals protected identities under Minnesota Statutes section 13.82, subdivision 17 (e.g., certain victims, witnesses, and others), should not be released even if it would otherwise fit into a category of data classified as public.

a. Data that record, describe, or otherwise document actions and circumstances surrounding the use of force by a peace officer that results in substantial bodily harm, or 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.

b. 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.

G. **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 or their designee, who shall process the request in accordance with the MGDPA and other governing laws. In particular:

1. An individual shall be provided with access and 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 Minnesota Statutes section 13.82, subdivision 17.

2. Unless the data is part of an active investigation, an individual data subject shall be provided with a copy of the recording upon request, but subject to the following guidelines on redaction:

   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.

H. **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:

1. 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 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 to inspect or have copies of BWC data for non-business reasons may make a request for it in the same manner as any member of the public.

I. **Other authorized disclosures of data.** Officers may display portions of BWC footage to witnesses as necessary for purposes of investigation as allowed by Minnesota Statutes

section 13.82, subdivision 15, as may be amended from time to time. Officers should generally limit these displays in order to protect against the incidental disclosure of identities that are not public. Protecting against incidental disclosure could involve, for instance, showing only a portion of the video, showing only screen shots, muting the audio, or playing the audio but not displaying video. In addition,

1. BWC data may be shared with other law enforcement agencies only for legitimate law enforcement purposes that are documented in writing at the time of the disclosure.

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

DATA SECURITY SAFEGUARDS

A. 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.

B. This policy prohibits altering, erasing, or destroying any BWC data or metadata prior to the expiration of the applicable retention period.

C. As required by Minnesota Statutes section 13.825, subdivision 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 whom a BWC is issued, or available for use, to ensure compliance with this policy and to identify any performance areas in which additional training or guidance is required. This review will include a minimum of 3 recordings which will be documented in a database maintained by this department.

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. Retention periods for BWC data are established by law and the Records Retention Schedule. When a particular recording is subject to more than one retention period, it shall be maintained for the longest applicable period.

B. All BWC data shall be retained for a minimum period of 90 days. There are no exceptions for erroneously recorded or non-evidentiary data.

C. Certain kinds of BWC data must be maintained for a minimum period of one year. These are:

1. Data that documents the discharge of a firearm by a peace officer in the course of duty.

2. Data that documents an incident resulting in a formal complaint against an officer. However, a longer retention period applies if the recording is relevant to an internal affairs investigation.

D. Data documenting the use of force by a peace officer that results in substantial bodily harm, or force that is of a sufficient type or degree to require supervisory review under the agency's policy, must be retained for a minimum period of seven years.

E. Data determined to have evidentiary value in any internal affairs investigation must be retained for five years after termination or separation of the employee who is the subject of the investigation.

F. Other data having evidentiary value shall be retained for the period specified by law or the records retention schedule.

G. Subject to Part H (below), all other BWC footage that is classified as non-evidentiary, becomes classified as non-evidentiary, or is not maintained for training shall be destroyed after 90 days.

H. 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.

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

J. The department will post this policy, together with its records retention schedule, on its website.

COMPLIANCE

Supervisors shall monitor for compliance with this policy. Noncompliance may constitute misconduct and subject individuals to disciplinary action and criminal penalties pursuant to Minnesota Statutes section 13.09.

REFERENCES AND REVISIONS:

REFERENCES: MN STATUTE 13.825 PORTABLE RECORDING SYSTEMS

REVISIONS: January 2024

APPENDIX B:

POLICY 3-3501	**SUBJECT: BODY WARN CAMERAS**
ISSUE DATE: 08/27/2025	**PERSONNEL:** LICENSED PEACE OFFICERS
REFERENCE:	**ISSUED BY:** CHIEF WADE STEINBRING

PURPOSE

The primary purpose of using BWCs is to capture evidence arising from police-citizen encounters. While this technology allows for the collection of valuable information, it opens many questions about how to balance public demands for accountability and transparency with the privacy concerns of those being recorded. In deciding what to record, this policy also reflects a balance between the desire to establish exacting and detailed requirements and the reality that officers must attend to their primary duties and the safety of all concerned, often in circumstances that are tense, uncertain, and rapidly evolving.

POLICY

It is the policy of 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. Unless otherwise prohibited by law, the chief or chief's designee may supersede this policy by providing specific instructions for BWC use to individual officers, or by 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 and words have special meanings as used in this policy:

I. **MGDPA or Data Practices Act** refers to the Minnesota Government Data Practices Act, Minn. Stat. § 13.01, et seq.

J. **Records Retention Schedule** refers, depending on context, to the General Records Retention Schedule for Minnesota Cities (last revised March 2021) or to the agency's records retention schedule approved pursuant to Minnesota Statutes section 138.17. \

K. **Law enforcement-related** refers to activities or information pertaining to a stop, arrest, search, seizure, use of force, investigation, citation, or charging decision.

L. **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.

M. **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.

N. **Adversarial** refers to 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.

O. **Unintentionally recorded footage** is a video recording that results from an officer's inadvertence or neglect in operating the officer's BWC, provided that no portion of the resulting recording has evidentiary value. Examples of unintentionally recorded footage include, but are not limited to, recordings made in station house locker rooms and 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.

P. **Official duties,** for purposes of this policy, refers to law enforcement activities and services performed by an officer of this agency while on duty. In circumstances where an officer is also employed by another agency as a peace officer, the officer is not performing official duties on behalf of this agency while acting in the course and scope of their employment for the other agency.

USE AND DOCUMENTATION

G. Officers may use only department issued BWCs while engaged in the performance of official duties.

H. Officers who are engaged in the performance of official duties and have been issued BWCs shall use and operate them in compliance with this policy. This requirement includes situations where the officer is under the command and control of another chief law enforcement officer or federal law enforcement official while performing official duties for this agency.

I. Officers shall conduct a function test of their issued BWCs at the beginning of each shift. Officers noting a malfunction during testing or at any other time shall promptly report it to the officer's supervisor and shall document the report in writing. Supervisors shall take prompt action to address malfunctions and document the steps taken in writing.

J. Officers shall wear their issued BWC at or above the midline of the waist in a position that maximizes the capacity of the device to record video footage of the officer's activities.

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

3. Whenever an officer makes a recording, the existence of the recording shall be documented in an incident report.

4. Whenever an officer fails to record an activity that is required to be recorded under this policy or fails to record for the entire duration of the activity, the officer must document the circumstances and reasons for not recording in an incident report. Supervisors shall review these reports and initiate any corrective action deemed necessary.

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

a. The total number of BWCs owned or maintained by the agency;

b. A daily record of the total number of BWCs actually deployed and used by officers;

c. The total amount of recorded BWC data collected and maintained; and

d. This policy, together with the applicable records retention schedule.

GENERAL GUIDELINES FOR RECORDING

H. Officers shall activate their BWCs when they become involved in, should reasonably anticipate becoming involved in, or when witnessing another officer engage 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 (E)(2) (above).

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

J. Officers have no affirmative duty to inform people that a BWC is being operated or that the individuals are being recorded.

K. Once activated, officers should continue recording with their BWCs 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 direct that recording be discontinued when additional recording is unlikely to capture information having evidentiary value. If the recording is discontinued while an investigation, response, or incident is ongoing, the officer 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.

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

M. Notwithstanding any other provision in this policy, officers shall not use their BWCs to record other agency personnel during non-enforcement related activities, such as during pre- and post-shift time in locker rooms, during meal breaks, or during other private conversations, unless the recording is authorized as part of an administrative or criminal investigation.

N. Officers shall not intentionally edit, alter, or erase any BWC recording made with a peace officer's portable recording system or data and metadata related to the recording prior the expiration of the applicable retention period under section 13.825 Subdivision 3, except that the full, unedited, and unredacted recording of a peace officer using deadly force must be maintained indefinitely.

SPECIAL GUIDELINES FOR RECORDING

Officers may, in the exercise of sound discretion, use their BWCs:

E. 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.

F. 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,

G. 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, the basis for any transport

hold, 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.

H. Officers shall use their BWCs and squad-based audio/video systems to record their transportation and the physical transfer of persons in their custody to hospitals, detox and mental health care facilities, juvenile detention centers, and jails, but otherwise should not record in these facilities unless the officer anticipates witnessing a criminal event or being involved in or witnessing an adversarial encounter or use-of-force incident.

DOWNLOADING AND LABELING DATA

E. Each officer using a BWC is responsible for transferring or assuring the proper transfer of the data from their camera to the Motorola Solutions cloud 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.

F. Officers shall label the BWC data files at the time of capture or transfer to storage. Officers should consult with a supervisor if in doubt as to the appropriate labeling.

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

9. **Evidence—force:** Whether or not enforcement action was taken or an arrest resulted, the event involved the application of force by an officer of this agency of sufficient degree or under circumstances triggering a requirement for supervisory review. Recordings that document the use of deadly are covered separately.

10. **Evidence—deadly force:** The event involved the application of deadly force by a peace officer, regardless of whether death occurred.

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

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

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

14. **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.

G. 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:

15. Victims and alleged victims of criminal sexual conduct and sex trafficking.

16. Victims of child abuse or neglect.

17. Vulnerable adults who are victims of maltreatment.

18. Undercover officers.

19. Informants.

20. When portions of the video are clearly offensive to common sensitivities.

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

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

23. Mandated reporters.

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

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

26. Individuals who made a complaint of a violation pertaining to the use of real property.

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

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

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

ADMINISTERING ACCESS TO BODY WORN CAMERA DATA

J. **Death resulting from force—access to data by survivors and legal counsel.** Notwithstanding any other law or policy to the contrary, when an individual dies as a result of force used by an officer of this agency, all BWC data documenting the incident, redacted only as required by law, must be made available for inspection by any of the following individuals within five days of their request:

1. The deceased individual's next of kin.

2. The legal representative of the deceased individual's next of kin.

3. The other parent of the deceased individual's child.

The request may be denied if there is a compelling reason that inspection would interfere with an active investigation. If access is denied, the chief of police must provide a prompt, written denial to the requestor with a short description of the compelling reason that access was denied. The written denial must also provide notice that relief may be sought from the district court pursuant to Minnesota Statutes section 13.82, subdivision 7.

K. **Death resulting from force—release of data to the public.** When an individual dies as a result of force used by an officer of this agency, all BWC data documenting the incident, redacted only as required by law, must be released and classified as public within 14 days after the incident, unless the chief of police asserts in writing that the public classification would interfere with an ongoing investigation, in which case the data remain classified by Minnesota Statutes section 13.82, subdivision 7.

L. **Data subjects.** Under Minnesota law, the following are considered data subjects for purposes of administering access to BWC data:

4. Any person or entity whose image or voice is documented in the data.

5. The officer who collected the data.

6. 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.

M. **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:

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

5. Some BWC data is classified as confidential (*see* part E, below).

6. Some BWC data is classified as public (*see* part F, below).

N. **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 in part D, and the "public" classifications listed below in parts F(2)(a) and (b). However, special classifications and access rights are applicable to BWC data documenting incidents where an officer's use of force results in death (*see* parts A and B, above).

O. **Public data.**

3. Data that documents the final disposition of a disciplinary action against a public employee is classified as public without regard to any ongoing criminal investigation.

4. The following data is public unless it is part of an active criminal investigation or is subject to a more restrictive classification. For instance, data that reveals protected identities under Minnesota Statutes section 13.82, subdivision 17 (e.g., certain victims, witnesses, and others), should not be released even if it would otherwise fit into a category of data classified as public.

c. Data that record, describe, or otherwise document actions and circumstances surrounding the use of force by a peace officer that results in substantial bodily harm, or 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.

d. 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.

P. **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 or their designee, who shall process the request in accordance with the MGDPA and other governing laws. In particular:

3. An individual shall be <u>provided with access and allowed to review</u> 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 Minnesota Statutes section 13.82, subdivision 17.

4. Unless the data is part of an active investigation, an individual data subject shall be <u>provided with a copy</u> 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.

Q. **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:

4. 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.

5. 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.

6. Employees seeking to inspect or have copies of BWC data for non-business reasons may make a request for it in the same manner as any member of the public.

R. **Other authorized disclosures of data.** Officers may display portions of BWC footage to witnesses as necessary for purposes of investigation as allowed by Minnesota Statutes

section 13.82, subdivision 15, as may be amended from time to time. Officers should generally limit these displays in order to protect against the incidental disclosure of identities that are not public. Protecting against incidental disclosure could involve, for instance, showing only a portion of the video, showing only screen shots, muting the audio, or playing the audio but not displaying video. In addition,

1. BWC data may be shared with other law enforcement agencies only for legitimate law enforcement purposes that are documented in writing at the time of the disclosure.

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

DATA SECURITY SAFEGUARDS

D. 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.

E. This policy prohibits altering, erasing, or destroying any BWC data or metadata prior to the expiration of the applicable retention period.

F. As required by Minnesota Statutes section 13.825, subdivision 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

E. At least once a month, supervisors will randomly review BWC usage by each officer to whom a BWC is issued, or available for use, to ensure compliance with this policy and to identify any performance areas in which additional training or guidance is required. This review will include a minimum of 3 recordings which will be documented in a database maintained by this department.

F. 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.

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

H. 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

K. Retention periods for BWC data are established by law and the Records Retention Schedule. When a particular recording is subject to more than one retention period, it shall be maintained for the longest applicable period.

L. All BWC data shall be retained for a minimum period of 90 days. There are no exceptions for erroneously recorded or non-evidentiary data.

M. Certain kinds of BWC data must be maintained for a minimum period of one year. These are:

1. Data that documents the discharge of a firearm by a peace officer in the course of duty.

2. Data that documents an incident resulting in a formal complaint against an officer. However, a longer retention period applies if the recording is relevant to an internal affairs investigation.

N. Data documenting the use of force by a peace officer that results in substantial bodily harm, or force that is of a sufficient type or degree to require supervisory review under the agency's policy, must be retained for a minimum period of seven years.

O. Data determined to have evidentiary value in any internal affairs investigation must be retained for five years after termination or separation of the employee who is the subject of the investigation.

P. Other data having evidentiary value shall be retained for the period specified by law or the records retention schedule.

Q. Subject to Part H (below), all other BWC footage that is classified as non-evidentiary, becomes classified as non-evidentiary, or is not maintained for training shall be destroyed after 90 days.

R. 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.

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

T. The department will post this policy, together with its records retention schedule, on its website.

COMPLIANCE

Supervisors shall monitor for compliance with this policy. Noncompliance may constitute misconduct and subject individuals to disciplinary action and criminal penalties pursuant to Minnesota Statutes section 13.09.

REFERENCES AND REVISIONS:

REFERENCES: MN STATUTE 13.825 PORTABLE RECORDING SYSTEMS

REVISIONS: January 2024