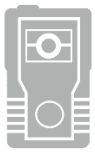
INDEPENDENT AUDITOR'S REPORT

Thief River Falls Police Department



JANUARY 9TH, 2026

RAMPART AUDIT LLC

Audit Overview and Recommendations

Dear Thief River Falls City Council and Chief Adam:

We have audited the body-worn camera (BWC) program of the Thief River Falls Police Department (TRF PD) for the two-year period ended 8/23/2025. 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 Thief River Falls Police Department. Our responsibility is to express an opinion on the operations of this program based on our audit.

On September 10, 2025, Rampart Audit, LLC (Rampart) met with Chief Marisa Adam, who provided information about TRF PD'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 TRF PD's recordkeeping.

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

TRF PD 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 TRF PD's BWC program in 2023. As part of that audit, TRF PD personnel provided documentation showing these requirements had been met prior to the implementation of TRF PD's BWC program. Specifically, TRF PD personnel provided portions of the minutes of the June 16, 2020, Thief River Falls City Council meeting, which noted that a public hearing had been held at the June 2, 2020, City Council meeting to receive public comments, that written and email comments had also been solicited, and a draft BWC policy had been prepared. The meeting minutes further noted that the Public Safety Committee had discussed the proposed program for "several months" and had reached a

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

consensus to present the proposal to the City Council for adoption. The City Council then voted unanimously to approve the recommendation.

A copy of this document has been retained in Rampart's audit files. In our opinion, Thief River Falls Police Department met the public notice and comment requirements prior to the implementation of their BWC program.

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 Adam furnished Rampart a copy of TRF PD's BWC policy, as well as a link to this policy, which was posted on the Police Department page of City of Thief River Falls' website. The Rampart auditor verified that this link worked at the time of the audit. In our opinion, Thief River Falls Police Department is compliant with the requirements of §626.8473 Subd. 3(a).

TRF PD BWC WRITTEN POLICY

As part of this audit, we reviewed TRF PD'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 TRF PD 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.

TRF PD 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.

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

Part B of the Data Retention section of TRF PD's BWC policy states:

> Data documenting the discharge of a firearm by a peace officer in the line of duty, other than for training or the killing of an animal that is sick, injured, or dangerous, must be maintained for a minimum period of one year.

Part C of the Data Retention section of TRF PD's BWC policy requires that the following be retained for six years: "[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 statute requires an "indefinite" retention on data that documents the use of deadly force, Part C of TRF PD's BWC policy above notes six years. However, this appears to be a relic of an old policy, as TRF PD's current policy on the next page notes it "must be kept indefinitely." We recommend removing the first sentence requiring a six year retention of data documenting use of deadly force for clarity.

While the language differs from the "substantial bodily harm" standard identified in statute, in our opinion the "force of a sufficient type or degree to require a use of force report or supervisory review" standard identified in TRF PD's BWC policy is broader and likely to encompass additional incidents beyond what is required by statute. In our opinion, Parts B and C collectively satisfy the requirements of §13.825 Subd. 3(b).

In addition, Part G of the Data Retention section of TRF PD's BWC policy states:

> The following categories of BWC data be retained [sic] 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.

This portion of the BWC policy more clearly aligns with the statutory requirements of §13.825 Subd. 3(b), though we noted that the word "shall" appears to be missing from the opening clause. We recommend that TRF PD review and clarify these portions of the BWC policy to eliminate any conflicts.

Part 1 of the Data classification; court-authorized disclosure section of TRF PD's BWC policy states:

> 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 to the expiration of the applicable retention period under section 13.825 subdivision 3, except that the full, unedited, and (b) unredacted recording of a peace officer using deadly force must be maintained indefinitely.

While this passage addresses both the requirements of §13.825 Subd. 3(c) and the requirement discussed in Clause 2 of the Policy section of this report, it does so in language that seemingly describes these as required elements of a BWC policy, rather than explicitly requiring or prohibiting such actions. We recommend that TRF PD revise the wording of this passage for clarity.

Part F of the Data Retention section of TRF PD'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).

TRF PD employs Panasonic Arbitrator BWC4000 body-worn cameras and manages BWC data retention on their own secure server through automated retention settings in the Arbitrator 360 video management software. The retention period for each video is determined by the data classification ("label") assigned at the time of upload; however, this retention period can be adjusted as needed.

The Downloading and Labeling Data section of TRF PD'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 TRF PD secure server by the end of that officer's shift." The policy also states that "[o]fficers shall transfer BWC data files to storage using the upload/charging bank in the TRF PD squad room. Once uploaded, officers shall label each recording…"

Chief Adam advised that at the time of the audit, one squad has wireless upload capabilities, while officers using any of the other squads must physically dock their BWC in the upload/charging dock located in the squad room of the Thief River Falls Police Department.

Rampart received an updated BWC policy prior to the completion of this report. In our opinion, TRF PD's updated BWC policy is substantially compliant with respect to the applicable data retention requirements.

TRF PD BWC Data Destruction

Chief Adam advised us that TRF PD BWC data are stored on a secure server located on-site. Data on this server are destroyed through automated deletion and overwriting, based on a retention schedule assigned to each video. Though not addressed in the BWC policy, Chief Adam advised us that at the time it is retired from service, any TRF PD-owned physical hard drive used to store BWC data will have all data deleted by formatting the disk.

FBI CJIS policy requires that hard drives used for CJIS data storage be 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.

Formatting a hard disk commonly involves removing the pointers used to locate data, rather than deleting the data, thereby leaving the data recoverable. In our opinion, TRF PD's BWC data destruction practice is likely not compliant with respect to the applicable data destruction requirements. We recommend that TRF PD follow the requirements outlined in the preceding paragraph to ensure compliance with FBI CJIS requirements.

Prior to the completion of this report, Rampart spoke with Chief Adam by phone and we were advised physical destruction by crushing and/or smashing would be used on any physical hard drive needing destruction. Rampart also received an updated policy noting physical destruction as the method. In our opinion, TRF PD's updated BWC policy meets the statutory requirement.

TRF PD BWC Data Access

The Access to BWC data by non-employees section of TRF PD's BWC policy states: "Officers shall refer members of the media or public seeking access to BWC data to the Chief or (sic) Police or Deputy Chief of Police, who shall process the request in accordance with the MGDPA [Minnesota Governmental Data Practices Act] and other governing laws."

Chief Adam advised us that requests for access to BWC data by data subjects or the media are made in writing, either to the Thief River Falls Police Department Records staff using the agency's data request form, or by email to the Chief or Deputy Chief. The Chief or Deputy Chief is then responsible for reviewing and fulfilling each request in accordance with the provisions of the MGDPA and other governing laws. BWC data is shared with data subjects via physical media, such as DVD or USB memory stick.

Part 1 of the Other authorized disclosures of data section of TRF PD'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 disclosure." Chief Adam advised us that requests from other agencies are made either by email or by phone. All requests from other agencies are directed to either herself or the TRF PD Records staff. The Chief or Deputy Chief processes all requests from other agencies. Existing verbal agreements between TRF PD and other area law enforcement agencies address data classification, destruction and security requirements under §13.825 Subd. 7 and Subd. 8. Access to TRF PD BWC data for outside agencies is provided either via physical media, or by sharing over Microsoft OneDrive.

We recommend that TRF PD enforce the requirement contained in their policy that all requests for BWC data from other law enforcement agencies be made in writing and identify a legitimate law enforcement purpose. We also recommend that when TRF PD fulfills BWC data requests from other law enforcement agencies, they include language reminding the receiving agency of their responsibilities under §13.825 Subd. 7 and Subd. 8.

Part 2 of the Other authorized disclosures of data section of TRF PD's BWC policy states: "BWC data shall be made available to prosecutors, courts, and other criminal justice entities as provided by law." Chief Adam advised us that requests from prosecutors for BWC data follow the same process as requests from other law enforcement agencies, with data sharing also occurring via physical media or Microsoft OneDrive.

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. Parts 4 and 5 of the Data classification; court-authorized disclosure section of TRF PD's BWC policy address these requirements, but do so in language that seemingly describes these as required elements of a BWC policy, rather than explicitly requiring such actions. We recommend that TRF PD revise the wording of these passages for clarity.

In our opinion, TRF PD's revised BWC policy is compliant with respect to the applicable data access requirements.

TRF PD BWC Data Classification

Consistent with §13.825 Subd. 2, the Administering Access to BWC Data section of TRF PD's BWC policy classifies BWC data as presumptively private while also identifying those circumstances in which BWC data are classified as public or confidential. The policy further addresses circumstances in which another provision of the MGDPA identifies data as private or not otherwise public, and notes that the data then retain that non-public classification.

As noted in the preceding section, TRF PD's BWC policy also addresses the changes the Minnesota State Legislature made in 2023 regarding data classification and access rights for BWC data documenting incidents involving the use of deadly force, albeit in language that lacks clarity.

In our opinion, TRF PD's revised policy is compliant with respect to the applicable data classification requirements.

TRF PD BWC Internal Compliance Verification

The Agency Use of Data section of TRF PD's BWC policy states: "[a]t least once a month, supervisors will randomly review BWC usage by each officer to ensure compliance with this policy and to identify any BWC usage in which additional training or guidance is required." Chief Adam advised us that she is not aware of an audit trail capability in the Panasonic Arbitrator 360 software, and they do not otherwise maintain a record of these reviews.

In the absence of internal tracking in the Panasonic software, Rampart recommends the use of other means to document audits, such as maintaining a log in a spreadsheet program such as Excel.

As discussed in Clause 4 of the Policy section of this report, the 2023 legislative changes require that an agency's BWC policy must specify that an officer assigned a BWC must wear and operate the system in compliance with the agency's BWC policy while performing law enforcement activities under the command and control of another chief law enforcement officer or federal law enforcement official.

Part 3 of the Data classification; court-authorized disclosure section of TRF PD's BWC policy states:

> 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 or another chief law enforcement officer or federal law enforcement official.

As discussed in previous sections of this report, it is our opinion that the language in this passage describes a required policy element, rather than actually requiring the element. We recommend TRF PD revise the wording above to require that officers wear and operate their assigned BWC in compliance with TRF PD's BWC policy under the circumstances described.

The Compliance section of TRF PD's BWC policy states: "[s]upervisors shall monitor for compliance with this policy. The unauthorized access to or disclosure of BWC data may constitute misconduct and subject individuals to disciplinary action and criminal penalties pursuant to Minn. Stat. §13.09."

In our opinion, TRF PD's revised BWC policy meets the compliance and disciplinary requirements specified in §626.8473 Subd. 3(b)(8).

TRF PD BWC Program and Inventory

TRF PD currently possesses 11 Panasonic Arbitrator BWC4000 body-worn cameras.

The TRF PD 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 TRF PD does not maintain a separate log of BWC deployment or use, Chief Adam advised us that deployment can be determined based on a review of TRF PD payroll records. Actual BWC use would be determined based on the creation of BWC data.

The Use and Documentation section of TRF PD's BWC policy states in part: "Officers may only use department-issued portable BWCs in the performance of official duties for this agency or when otherwise performing authorized law enforcement services as an employee of this department."

Part F, Access by peace officers and law enforcement employees, of the Administering Access to BWC Data section of TRF PD's BWC policy states in part:

> Officers may access and view stored BWC video only when there is a business need to do so… 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.

The policy also prohibits accessing BWC data for "non-business reasons," or sharing such data for "non-law enforcement related purposes."

In our opinion, these sections of the policy are compliant with Minnesota Statute §13.825 Subd. 6.

As of 9/10/2025, TRF PD maintained 6.45 TB of BWC data.

TRF PD BWC Physical, Technological and Procedural Safeguards

TRF PD BWC data are initially recorded to an internal hard drive in each officer's BWC. Those files are then transferred to a dedicated server either via physical docking station or wireless upload. TRF PD maintains a second server for back-up purposes. Any files identified as potentially evidentiary in nature are also copied to an external hard drive that is maintained in a separate locked room.

We recommend employing a Cloud-based service or other off-site secure storage to create a backup of BWC data to minimize the risk of a loss of data due to physical hazards such as fire, floods or tornados.

Officers have view-only access to their own data for report writing, trial preparation, data administration, investigatory purposes and other legitimate law enforcement purposes through the Panasonic Arbitrator 360 client. All such access is logged and can be reviewed by TRF PD administrators.

BWC data are only destroyed via an automated process upon the expiration of the retention period defined for the specific data classification in the Arbitrator 360 software.

As noted above, requests by other law enforcement agencies for TRF PD BWC data must be reviewed by the Chief Adam and are fulfilled via physical media. A similar method is employed to submit TRF PD BWC data to the Pennington County Attorney's Office and the Thief River Falls City Attorney's Office.

As noted in Clause 3 of the Policy section of this report, the 2023 legislative updates require that a BWC policy specify that the device be worn at or above the mid-line of the waist. Part 2 of the Data classification; court-authorized disclosure section of TRF PD's BWC policy states: "[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."

As discussed in previous sections of this report, it is our opinion that the language in this passage describes a required policy element, rather than actually requiring the element. We recommend TRF PD revise the wording above to clarify that officers are required to wear their assigned BWC at or above the mid-line of the waist.

Prior to the issuance of this report, TRF PD furnished a revised BWC policy that clarifies this language.

Enhanced Surveillance Technology

TRF PD 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.

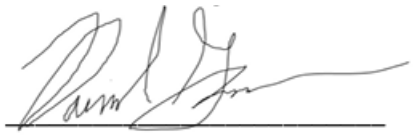
If TRF PD should obtain such enhanced technology in the future, Minnesota Statute §13.825 Subd. 10 requires notice to the Minnesota Bureau of Criminal Apprehension within 10 days. This notice must include a description of the technology and its surveillance capability and intended uses.

Data Sampling

Rampart selected a random sample of 132 calls 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 pre-audit covers a period of one year, 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 auditor reviewed the retained BWC videos to verify that this data was accurately documented in TRF PD records.

Audit Conclusions

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



Rampart Audit, LLC

1/9/2026

APPENDIX A:

THIEF RIVER FALLS POLICE DEPARTMENT 1. ANUAL

Policy Type: Operations

Series: 284

Policy Title: Body-Worn Cameras (BWCs)

Reviewed Date: 5/04/21

Authorized by: Chief Marissa Adam

Page 1 of 9

CITY OF THIEF RIVER FALLS USE OF BODY-WORN CAMERAS POLICY

Purpose

The primary purpose of using body-worn-cameras (BWCs) is to capture evidence arising from police-citizen encounters. This policy sets forth guidelines governing the use of BWCs and administering the data that results. Compliance with these guidelines is mandatory, but it is recognized that officers must also attend to other primary duties and the safety of all concerned, sometimes in circumstances that are tense, uncertain, and rapidly evolving.

Policy

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

Scope

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

Definitions

The following phrases have special meanings as used in this policy:

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

seq.

B. Records Retention Schedule refers to the General Records Retention Schedule for Minnesota Cities.

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

D. Evidentiary value means that the information may be useful as proof in a criminal prosecution, related civil or administrative proceeding, further investigation of an actual or suspected criminal act, or in considering an allegation against a law enforcement agency or officer.

E. **General citizen contact** means an informal encounter with a citizen that is not and does not become law enforcement-related or adversarial, and a recording of the event would not yield information relevant to an ongoing investigation. Examples include, but are not limited to, assisting a motorist with directions,summoning a wrecker, or receiving generalized concerns from a citizen about crime trends in his or her neighborhood.

F. **Adversarial** means a law enforcement encounter with a person that becomes confrontational, during which at least one person expresses anger, resentment, or hostility toward the other, or at least one person directs toward the other verbal conduct consisting of arguing, threatening, challenging, swearing, yelling, or shouting. Encounters in which a citizen demands to be recorded or initiates recording on his or her own are deemed adversarial.

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

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

Use and Documentation

A. Officers may use only department-issued BWCs in the performance of official duties for this agency or when otherwise performing authorized law enforcement services as an employee of this department.

8. Officers who have been issued BWCs shall operate and use them consistent with this policy. Officers shall conduct a function test of their issued BWCs at the beginning of each shift to make sure the devices are operating properly. Officers noting a malfunction during testing or at any other time shall promptly report the malfunction to the officer's supervisor and shall document the report in writing. Supervisors shall take prompt action to address malfunctions and document the steps taken in writing._

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

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

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

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

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

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

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

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

4. This policy, together with the Records Retention Schedule.

General Guidelines for Recording

A. Officers shall activate their BWCs when responding to all calls for service and during all law enforcement-related encounters and activities, including but not limited to pursuits, *Terry* stops of motorists or pedestrians, arrests, searches, suspect interviews and interrogations, and during any police/citizen contacts that becomes adversarial. However, officers need not activate their cameras when it would be unsafe, impossible, or impractical to do so, but such instances of not recording when otherwise required must be documented as specified in the Use and Documentation guidelines, part (D){2) (above).

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

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

D. Once activated, the BWC should continue recording until the conclusion of the incident or encounter, or until it becomes apparent that additional recording is unlikely to capture information having evidentiary value. The officer having charge of a scene shall likewise direct the discontinuance of recording when further recording is unlikely to capture additional information having evidentiary value. If a recording is accidentally discontinued while an

investigation, response, or incident is ongoing, the officer shall document the discontinuation. Officers shall reactivate their cameras as soon as possible following any accidental discontinuation.

E. Officers shall not intentionally block the BWC's audio or visual recording functionality to defeat the purposes of this policy. The mute function available on the Panasonic Arbitrator BWCs shall not be used by officers of the TRF PD.

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

Special Guidelines for Recording

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

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

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

In addition,

C. Officers need not record persons being provided medical care unless there is reason to believe the recording would document information having evidentiary value. When responding to an apparent mental health crisis or event, BWCs shall be activated as necessary to document any use of force and the basis for it, and any other information having evidentiary value, but need not be activated when doing so would serve only to record symptoms or behaviors believed to be attributable to the mental health issue.

D. Officers 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 his or her camera to the TRF PD secure server 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 transfer BWC data files to storage using the upload/charging bank in the TRF PD squad room. Once uploaded, officers shall label each recording and should consult with a supervisor if in doubt as to the appropriate labeling. Officers should assign as many of the following labels as are applicable to each file:

1. **Evidence-criminal:** The information has evidentiary value with respect to an actual or suspected criminal incident or charging decision. Retention periods for cases that have been charged are based on the status of court proceedings and retention periods for uncharged offenses will be seven years or permanent in homicide cases.

2. **Evidence-force:** Whether or not enforcement action was taken, or an arrest resulted, the event involved the application of force by a law enforcement officer of this or another agency. Retention periods for such recordings will be six years regardless of the disposition of any related criminal case.

3. • **Evidence-property:** Whether or not enforcement action was taken, or an arrest resulted, an officer seized property from an individual or directed an individual to dispossess property. Retention periods for such recordings will be one year.

4. **Evidence-administrative:** The incident involved an adversarial encounter or resulted in a complaint against the officer. Retention periods for such recordings will be six years if an internal investigation is initiated but may be shorter if no complaint or internal investigation arises.

5. **Evidence-other:** The recording has potential evidentiary value for reasons identified by the officer at the time of labeling. Retention periods for such recordings will depend on the reason stated for maintaining the data.

6. **Training:** The event was such that it may have value for training. No minimal retention period will be set for such a recording.

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. Retention periods for such recordings will be 90 days.

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 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 911system.
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 and flagging designations may be corrected or amended based on additional information.

Administering Access to BWC Data:

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

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

2. The officer who collected the data.

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

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

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

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

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

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

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

I. Data documenting the discharge of a firearm by a peace officer in the course of duty, other than for training or the killing of an animal that is sick, injured, or dangerous.

2. Data that documents the use of force by a peace officer that results in substantial bodily harm.

3. Data that a data subject requests to be made accessible to the public, subject to redaction. Data on any data subject (other than a peace officer) who has not consented to the public release must be redacted [if *practicable].* In addition, any data on undercover officers must be redacted.

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

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

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

request in accordance with the MGDPA and other governing laws. In particular:

1. An individual shall be allowed to review recorded BWC data about him- or herself and other data subjects in the recording, but access shall not be granted:

    a. If the data was collected or created as part of an active investigation.

    b. To portions of the data that the agency would otherwise be prohibited by law from disclosing to the person seeking access, such as portions that would reveal identities protected by Minn. Stat. § 13.82, subd. 17.

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.

F. **Access by peace officers and law enforcement employees.** No employee may have access to the department's BWC data except for legitimate law enforcement or data administration purposes:

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 shall document their reasons for accessing stored BWC data in the manner provided within the database at the time of each access. Agency personnel are prohibited from accessing BWC data for non-business reasons and from sharing the data for non-law enforcement related purposes, including but not limited to uploading BWC data recorded or maintained by this agency to public and social media websites.

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

G. **Other authorized disclosures of data.** Officers may display portions of BWC footage to witnesses as necessary for purposes of investigation as allowed by Minn. Stat. § 13.82, subd. 15, as may be amended from time to time. Officers should generally limit these displays in order to protect against the incidental disclosure of individuals whose identities are not public. Protecting against incidental disclosure could involve, for instance, showing only a portion of the video, showing only screen shots, muting the audio, or playing the audio but not displaying video. In addition,

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. A username and password will be required to access the Arbitrator BWC software and, except for system administrators, limited permissions will be given for purposes of uploading recordings, labelling recordings, and viewing recordings for reports.

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

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

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

Agency Use of Data

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

B. In addition, supervisors and other assigned personnel may access BWC data for the purposes of reviewing or investigating a specific incident that has given rise to a complaint or concern about officer misconduct or performance.

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

D. Officers should contact their supervisors to discuss retaining and using BWC footage for training purposes. Officer objections to preserving or using certain footage for training will be considered on a case-by-case basis. Field training officers may utilize BWC data with trainees for the purpose of providing coaching and feedback on the trainees' performance.

Data Retention

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

B. Data documenting the discharge of a firearm by a peace officer in the course of duty, other than for training or the killing of an animal that is sick, injured, or dangerous, must be maintained for a minimum period of one year.

C. Certain kinds of BWC data must be retained for six years:

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

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

D. Other data having evidentiary value shall be retained for the period specified in the Records Retention Schedule. When a particular recording is subject to multiple retention periods, it shall be maintained for the longest applicable period.

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

F. Upon written request by a BWC data subject, the agency shall retain a recording pertaining to that subject for an additional time period requested by the subject of up to 180 days. The agency will notify the requester at the time of the request that the data will then be destroyed unless a new written request is received.

G. 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

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

I. The department will post this policy, including its Records Retention Schedule within, on its website.

Compliance

Supervisors shall monitor for compliance with this policy. The unauthorized access to or disclosure of BWC data may constitute misconduct and subject individuals to disciplinary action and criminal penalties pursuant to Minn. Stat. § 13.09.

Data classification; court-authorized disclosure

1. (a) 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 (b) unredacted recording of a peace officer using deadly force must be maintained fiveitely;

2. 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;

3. 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;

4. 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;

5. 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;

APPENDIX B:

THIEF RIVER FALLS POLICE DEPARTMENT MANUAL

Policy Type: Operations | Series: 284

Policy Title: Body-Worn Cameras (BWCs) | Reviewed Date: 5/04/21

Authorized by: Chief Marissa Adam | Page 1 of 9

CITY OF THIEF RIVER FALLS
USE OF BODY-WORN CAMERAS POLICY

Purpose

The primary purpose of using body-worn-cameras (BWCs) is to capture evidence arising from police-citizen encounters. This policy sets forth guidelines governing the use of BWCs and administering the data that results. Compliance with these guidelines is mandatory, but it is recognized that officers must also attend to other primary duties and the safety of all concerned, sometimes in circumstances that are tense, uncertain, and rapidly evolving.

Policy

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

Scope

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

Definitions

The following phrases have special meanings as used in this policy:

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

B. **Records Retention Schedule** refers to the General Records Retention Schedule for Minnesota Cities.

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

D. **Evidentiary value** means that the information may be useful as proof in a criminal prosecution, related civil or administrative proceeding, further investigation of an actual or suspected criminal act, or in considering an allegation against a law enforcement agency or officer.

E. **General citizen contact** means an informal encounter with a citizen that is not and does not become law enforcement-related or adversarial, and a recording of the event would not yield information relevant to an ongoing investigation. Examples include, but are not limited to, assisting a motorist with directions,summoning a wrecker, or receiving generalized concerns from a citizen about crime trends in his or her neighborhood.

F. **Adversarial** means a law enforcement encounter with a person that becomes confrontational, during which at least one person expresses anger, resentment, or hostility toward the other, or at least one person directs toward the other verbal conduct consisting of arguing, threatening, challenging, swearing, yelling, or shouting. Encounters in which a citizen demands to be recorded or initiates recording on his or her own are deemed adversarial.

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

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

Use and Documentation

A. Officers may use only department-issued BWCs in the performance of official duties for this agency or when otherwise performing authorized law enforcement services as an employee of this department.

8. Officers who have been issued BWCs shall operate and use them consistent with this policy. Officers shall conduct a function test of their issued BWCs at the beginning of each shift to make sure the devices are operating properly. Officers noting a malfunction during testing or at any other time shall promptly report the malfunction to the officer's supervisor and shall document the report in writing. Supervisors shall take prompt action to address malfunctions and document the steps taken in writing._

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

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

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

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

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

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

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

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

4. This policy, together with the Records Retention Schedule.

General Guidelines for Recording

A. Officers shall activate their BWCs when responding to all calls for service and during all law enforcement-related encounters and activities, including but not limited to pursuits, *Terry* stops of motorists or pedestrians, arrests, searches, suspect interviews and interrogations, and during any police/citizen contacts that becomes adversarial. However, officers need not activate their cameras when it would be unsafe, impossible, or impractical to do so, but such instances of not recording when otherwise required must be documented as specified in the Use and Documentation guidelines, part (D){2) (above).

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

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

D. Once activated, the BWC should continue recording until the conclusion of the incident or encounter, or until it becomes apparent that additional recording is unlikely to capture information having evidentiary value. The officer having charge of a scene shall likewise direct the discontinuance of recording when further recording is unlikely to capture additional information having evidentiary value. If a recording is accidentally discontinued while an investigation, response, or incident is ongoing, the officer shall document the discontinuation. Officers shall reactivate their cameras as soon as possible following any

accidental discontinuation.

E. Officers shall not intentionally block the BWC's audio or visual recording functionality to defeat the purposes of this policy. The mute function available on the Panasonic Arbitrator BWCs shall not be used by officers of the TRF PD.

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

Special Guidelines for Recording

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

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

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

In addition,

C. Officers need not record persons being provided medical care unless there is reason to believe the recording would document information having evidentiary value. When responding to an apparent mental health crisis or event, BWCs shall be activated as necessary to document any use of force and the basis for it, and any other information having evidentiary value, but need not be activated when doing so would serve only to record symptoms or behaviors believed to be attributable to the mental health issue.

D. Officers 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 his or her camera to the TRF PD secure server 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 transfer BWC data files to storage using the upload/charging bank in the TRF PD squad room. Once uploaded, officers shall label each recording and should consult with a supervisor if in doubt as to the appropriate labeling. Officers should assign as many of the following labels as are applicable to each file:

1. **Evidence-criminal:** The information has evidentiary value with respect to an actual or suspected criminal incident or charging decision. Retention periods for cases that have been charged are based on the status of court proceedings and retention periods for uncharged offenses will be seven years or permanent in homicide cases.

2. **Evidence-force:** Whether or not enforcement action was taken, or an arrest resulted, the event involved the application of force by a law enforcement officer of this or another agency. Retention periods for such recordings will be six years regardless of the disposition of any related criminal case.

3. • **Evidence-property:** Whether or not enforcement action was taken, or an arrest resulted, an officer seized property from an individual or directed an individual to dispossess property. Retention periods for such recordings will be one year.

4. **Evidence-administrative:** The incident involved an adversarial encounter or resulted in a complaint against the officer. Retention periods for such recordings will be six years if an internal investigation is initiated but may be shorter if no complaint or internal investigation arises.

5. **Evidence-other:** The recording has potential evidentiary value for reasons identified by the officer at the time of labeling. Retention periods for such recordings will depend on the reason stated for maintaining the data.

6. **Training:** The event was such that it may have value for training. No minimal retention period will be set for such a recording.

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. Retention periods for such recordings will be 90 days.

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 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 911system.
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 and flagging designations may be corrected or amended based on additional information.

Administering Access to BWC Data:

A. **Data subjects.** Under Minnesota law, the following are considered data subjects for purposes

of administering access to BWC data:

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

2. The officer who collected the data.

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

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

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

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

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

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

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

I. Data documenting the discharge of a firearm by a peace officer in the course of duty, other than for training or the killing of an animal that is sick, injured, or dangerous.

2. Data that documents the use of force by a peace officer that results in substantial bodily harm.

3. Data that a data subject requests to be made accessible to the public, subject to redaction. Data on any data subject (other than a peace officer) who has not consented to the public release must be redacted [if *practicable].* In addition, any data on undercover officers must be redacted.

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

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

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

the request in accordance with the MGDPA and other governing laws. In particular:

1. An individual shall be allowed to review recorded BWC data about him- or herself and other data subjects in the recording, but access shall not be granted:

    a. If the data was collected or created as part of an active investigation.

    b. To portions of the data that the agency would otherwise be prohibited by law from disclosing to the person seeking access, such as portions that would reveal identities protected by Minn. Stat. § 13.82, subd. 17.

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.

F. **Access by peace officers and law enforcement employees.** No employee may have access to the department's BWC data except for legitimate law enforcement or data administration purposes:

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 shall document their reasons for accessing stored BWC data in the manner provided within the database at the time of each access. Agency personnel are prohibited from accessing BWC data for non-business reasons and from sharing the data for non-law enforcement related purposes, including but not limited to uploading BWC data recorded or maintained by this agency to public and social media websites.

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

G. **Other authorized disclosures of data.** Officers may display portions of BWC footage to witnesses as necessary for purposes of investigation as allowed by Minn. Stat. § 13.82, subd. 15, as may be amended from time to time. Officers should generally limit these displays in order to protect against the incidental disclosure of individuals whose identities are not public. Protecting against incidental disclosure could involve, for instance, showing only a portion of the video,

showing only screen shots, muting the audio, or playing the audio but not displaying video. In addition,

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. A username and password will be required to access the Arbitrator BWC software and, except for system administrators, limited permissions will be given for purposes of uploading recordings, labelling recordings, and viewing recordings for reports.

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

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

Agency Use of Data

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

B. In addition, supervisors and other assigned personnel may access BWC data for the purposes of reviewing or investigating a specific incident that has given rise to a complaint or concern about officer misconduct or performance.

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

D. Officers should contact their supervisors to discuss retaining and using BWC footage for training purposes. Officer objections to preserving or using certain footage for training will be considered on a case-by-case basis. Field training officers may utilize BWC data with trainees for the purpose of providing coaching and feedback on the trainees' performance.

Data Retention

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

B. Data documenting the discharge of a firearm by a peace officer in the course of duty, other than for training or the killing of an animal that is sick, injured, or dangerous, must be maintained for a minimum period of one year.

C. Certain kinds of BWC data must be retained for six years:

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

D. Other data having evidentiary value shall be retained for the period specified in the Records Retention Schedule. When a particular recording is subject to multiple retention periods, it shall be maintained for the longest applicable period.

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

F. Upon written request by a BWC data subject, the agency shall retain a recording pertaining to that subject for an additional time period requested by the subject of up to 180 days. The agency will notify the requester at the time of the request that the data will then be destroyed unless a new written request is received.

G. The following categories of BWC data shall 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

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

I. The department will post this policy, including its Records Retention Schedule within, on its website.

J. Any drives that contain old BWC that is not longer needed will be physically destroyed.

Compliance

Supervisors shall monitor for compliance with this policy. The unauthorized access to or disclosure of BWC data may constitute misconduct and subject individuals to disciplinary action and criminal penalties pursuant to Minn. Stat. § 13.09.

Data classification; court-authorized disclosure

1. (a) There shall be no 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 (b) unredacted recording of a peace officer using deadly force must be maintained indefinitely;

2. A portable recording system shall 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;

3. Officers assigned a portable recording system shall 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;

4. 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 shall 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 shall 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;

5. 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;