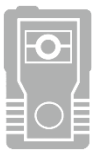
INDEPENDENT AUDITOR'S REPORT

North St. Paul Police Department



FEBRUARY 10TH, 2025

RAMPART AUDIT LLC

Audit Overview and Recommendations

Dear North St. Paul City Council and Chief Rozales:

We have audited the body-worn camera (BWC) program of the North St. Paul Police Department (NSPPD) for the period of 6/01/2021 – 5/31/2023. 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 North St. Paul Police Department. Our responsibility is to express an opinion on the operations of this program based on our audit.

On May 20, 2024, Rampart Audit LLC (Rampart) met with Records Technician Kristen Churchill, who provided information about NSPPD'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 NSPPD's recordkeeping.

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

NSPPD 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.

Records Technician Churchill was not familiar with the steps North St. Paul Police Department had taken prior to implementing its BWC program in 2021.

North St. Paul Police Department Chief Raymond Rozales noted that NSPPD's BWC program was already in place when he joined the agency in August of 2022, and advised us that he was uncertain whether the public hearing requirement had been met. Rampart advised him to suspend NSPPD's BWC program and conduct an after-the-fact public hearing if he was unable to verify that this requirement had been met prior to the program's implementation.

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

After researching the matter, further Chief Rozales was able to verify that a public hearing was held prior to the implementation of his department's BWC program and provided the following documentation:

- An email from City of North St. Paul Human Resources Manager Jennie Kloos advising that a public comment agenda item related to the BWC public hearing was posted on the city bulletin board located in the hallway at City Hall, on the city website and was promoted in the city newsletter.
- A link to the City of North St. Paul website, where Rampart located a copy of the January 6, 2021, City of North St. Paul newsletter, which provided information about the proposed BWC program and invited the public to submit comments via phone or email. (Auditor's note: NSP City Council meetings were conducted via Zoom during this time period due to the COVID-19 pandemic. The newsletter included Ms. Kloos' email address as well as a clickable Zoom link for the meeting.)
- Rampart also located copies of the meeting agenda and meeting minutes for the January 19, 2021, North St. Paul City Council meeting, both of which noted a scheduled public hearing regarding body worn cameras.
- A copy of the January 21, 2021, City of North St. Paul newsletter describing the discussion held during the January 19, 2021, North St. Paul City Council meeting, prior to the City Council's vote to approve the proposed BWC policy. The newsletter includes a link to the policy, as well as a link to an audio recording of the discussion.

Copies of these documents have been retained in Rampart's audit files. In our opinion, the North St. Paul Police Department met the public notice and comment requirements prior to the implementation of their BWC program in 2021.

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."

Rampart verified that there was a working link to NSPPD's BWC policy on the Police Department page of the City of North St. Paul' website. In our opinion, North St. Paul Police Department is compliant with the requirements of §626.8473 Subd. 3(a).

NSPPD BWC WRITTEN POLICY

As part of this audit, we reviewed NSPPD'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) 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 NSPPD 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.

NSPPD BWC Data Retention

North St. Paul Police Department's BWC policy states that: "[a]ll recordings shall be retained for a period consistent with the requirements of the organization's records retention schedule but in no event for a period less than 90 days." This satisfies the 90-day minimum retention period established in Minn. Stat. §13.825 Subd. 3(a) for all BWC data not subject to a longer retention period.

Minn. Stat. §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.

Minn. Stat. §13.825 Subd. 3(c) requires that any portable recording system data documenting a peace officer's use of deadly force must be maintained indefinitely.

NSPPD's BWC policy does not address retention periods for the data categories described in Minn. Stat. §13.825 Subd. 3(b) or (c).

Prior to the completion of this report, NSPPD provided a revised BWC policy that adds the required retention periods described in §13.825 Subd. 3(b) and (c). A copy of this revised policy is attached to this report as Appendix B.

The Data Retention section of NSPPD's BWC policy addresses the requirement contained in Minn. Stat. §13.825 Subd. 3(d) that an agency retain BWC recordings for an additional period when so requested in writing by a data subject, though it does not specify that such recordings be retained for up to 180 days as stated in statute. We recommend adding language to clarify the length of this additional retention period.

Prior to the completion of this report, NSPPD submitted a revised BWC policy that addresses the issue noted in the preceding paragraph.

NSPPD's BWC policy also states that "[m]embers shall not alter, erase, or destroy any recordings before the end of the applicable records retention period," as described in Clause 2 of the Policy section of this report. We noted that §626.8473 Subd. 3(b)(1) requires that this prohibition extend to related data and metadata as well. Prior to the completion of this report, NSPPD submitted a revised BWC policy that states: "[m]embers shall not alter, erase, or destroy any BWC media, before the end of the applicable retention period." NSPPD's BWC policy defines BWC media as "[t]he audio, video, and images captured by department BWCs and the associated metadata." In our opinion, this revised language satisfies the requirements of §626.8473 Subd. 3(b)(1).

NSPPD employs Panasonic iPRO 4000 BWCs and stores BWC data online utilizing Panasonic's UDE[2] cloud storage service. NSPPD manages BWC data retention through automated retention settings in Panasonic's Arbitrator 360 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. If an officer fails to assign a data classification, the default retention period is currently 90 days; however, Ms. Churchill advised us that NSPPD will be extending this retention period to 7 years to avoid the accidental loss of data.

[2] NSP staff referred to "United" cloud storage during the audit. Panasonic's cloud service is called "Unified Digital Evidence" or UDE.

NSPPD's BWC policy states that: "[t]o assist with identifying and preserving data and recordings, members should download, tag or mark the recordings in accordance with procedure and document the existence of the recording in any related case report."

Ms. Churchill advised that the Panasonic body-worn cameras utilize a physical docking station located at the North St. Paul Police Department.

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

NSPPD BWC Data Destruction

As discussed above, North St. Paul PD's BWC data are stored on Panasonic's cloud-based service, iPRO CloUDE [Unified Digital Evidence] *Powered by* Genetic, with data retention and deletion schedules managed automatically through the Arbitrator 360 software based on the assigned data classification of each video.

Panasonic 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 (5.9.2), 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.

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

NSPPD BWC Data Access

Ms. Churchill advised us that that all requests for BWC data from the public or media are made in writing using North St. Paul Police Department's BWC data request form, which is submitted to the Records Department. Other law enforcement agencies can request data by submitting NSPPD's BWC data request form via email to the Records Department. Ms. Churchill advised us that BWC video is shared via "Zip drive[3]." Other law enforcement agencies may also receive data via an emailed UDE link.

NSPPD's BWC policy states that: "[e]xcept as provided by Minn. Stat. §13.825, Subd. 2, audio/video recordings are considered private or nonpublic data. Any person captured in a recording may have access to the recording." We noted that BWC policies usually contain an explicit exception to a data subject's right of access for data classified as confidential, such as recordings that are part of an active investigation. We also noted that BWC policies usually contain language stating that requests for BWC data shall be processed in accordance with the MGDPA [Minnesota Government Data Practices Act] and other

[3] Because Zip drives have been largely obsolete since the early 2000s, we believe the intended term was "USB storage device;" however, NSPPD did not respond to requests for clarification.

governing laws. While NSPPD's policy states that a "coordinator should work with the Custodian of Records… to coordinate the use, access, and release of protected information to ensure that procedures comply with requirements of the Minnesota Government Data Practices Act (MGDPA)," the policy does not document any such procedures. We recommend that NSPPD add clarifying language to their policy.

Prior to the completion of this report, NSPPD furnished a revised BWC policy that adds the text of Minn. Stat. §13.825, Subd. 2 to address the various data classification requirements. In addition, this revised policy indicates that "[r]equests for BWC media shall be processed in accordance with the Records Maintenance and Release Policy. The Administrative Assistant should review BWC media before public release."

We noted that BWC policies usually contain language stating that 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, and that BWC data shall be made available to prosecutors, courts, and other criminal justice entities as provided by law. We recommend that NSPPD add similar language to their policy.

Ms. Churchill did not provide any information regarding steps NSPPD has taken to obtain verbal or written acknowledgments of any receiving law enforcement agency's obligations under §13.825 Subd. 7 and Subd. 8, which include a requirement to maintain BWC data security.

Due to the lack of information provided, Rampart is unable to express an opinion as to whether NSPPD is compliant with respect to these requirements.

Rampart recommends that NSPPD obtain a written acknowledgement of these responsibilities from any agency receiving BWC data, and that they maintain a copy of each acknowledgement.

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, NSPPD had not revised its BWC policy to address these requirements.

As discussed above, prior to the completion of this report, NSPPD submitted a revised BWC policy that includes the text of Minn. Stat. §13.825, Subd. 2, which addresses the requirements noted in the preceding paragraph. In our opinion, this revised BWC policy is compliant with respect to the applicable data access requirements.

NSPPD BWC Data Classification

At the time of our audit, NSPPD's BWC policy stated that, "[e]xcept as provided by Minn. Stat. §13.825, Subd. 2, audio/video recordings are considered private or nonpublic data," but did not otherwise address the topic. As noted in the preceding section, prior to the completion of this report, NSPPD submitted a revised BWC policy that includes the text of Minn. Stat. §13.825, Subd. 2, which addresses the various BWC data classification requirements. In our opinion, this revised policy is compliant with respect to the applicable data classification requirements.

NSPPD BWC Internal Compliance Verification

The Review of Recorded media section of NSPPD's BWC policy states that, "[r]ecorded files may also be reviewed… [b]y a supervisor as part of internal audits and reviews as required by Minn. Stat. §626.8473." The Supervisor Responsibilities section states that "[a]t least once per month, supervisors will randomly review portable recorder usage by each officer to ensure compliance with this policy." Ms. Churchill indicated that these supervisory reviews occur weekly rather than monthly. All such reviews are logged in the Arbitrator 360 software. In addition, all access to BWC data is logged and supervisory personnel are able to monitor such access.

The Policy section of NSPPD's BWC policy states that, "[t]he North St. Paul Police Department may provide members with access to portable recorders to use during the performance of their duties."

As discussed in Clause 4 of the Policy section of this report, the 2023 legislative changes require that an agency's BWC policy must require that an officer assigned a BWC 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. NSPPD's BWC policy does not address this new statutory requirement.

Prior to the completion of this report, NSPPD submitted a revised version of their BWC policy that states: "The guidelines set forth in this policy shall be followed while working under the command and control of another law enforcement organization or as a federal law enforcement agent."

NSPPD's BWC policy addresses disciplinary consequences associated with violations of the policy, but does not address potential criminal penalties. Prior to the completion of this report, NSPPD submitted a revised BWC policy that addresses potential criminal consequences related to misuse of BWC data.

In our opinion, NSPPD's revised policy is compliant with respect to the compliance and disciplinary requirements contained in §626.8473 Subd. 3(b)(8).

NSPPD BWC Program and Inventory

NSPPD currently possesses 22 Panasonic iPRO 4000 body-worn cameras, which includes one spare device.

The NSPPD BWC policy identifies those circumstances in which officers are expected to activate their body-worn cameras, as well as circumstances in which they are prohibited from activating their body-worn cameras. The policy also provides guidance for those circumstances in which BWC activation is deemed discretionary.

The Member Responsibilities section of NSPPD's BWC policy states that "[u]niformed members should wear the recorder in a conspicuous manner at or above the mid-line of the waist," as discussed in Clause 3 of the Policy section of this report, but merely requires that non-uniformed members who wear a BWC do so in a "conspicuous location." Because §626.8473 Subd. 3(b)(2) does not limit this requirement to uniformed personnel, we recommend that NSPPD modify their policy to require that all BWCs be worn at or above the mid-line of the waist. Prior to the submission of this report, NSPPD submitted a revised BWC policy that addresses this issue.

Ms. Churchill advised that NSPPD does not permit the use of personally-owned recording devices and indicated that in the event an officer's primary BWC failed, his or her NSPPD-issued cell phone could be used as a backup recorder until a replacement BWC could be obtained.

The Prohibited Use of Audio/Video Recorders section of NSPPD's BWC policy states that, "[m]embers are prohibited from using personally owned recording devices while on-duty without the express consent of the Shift Sergeant." Minn. Stat. §13.825 Subd. 6 states that, "[w]hile on duty, a peace officer may only use a portable recording system issued and maintained by the officer's agency in documenting the officer's actions." While it appears that NSPPD is compliant with this requirement in practice, we recommend removing from policy the language allowing a shift sergeant to authorize the use of personally-owned recording devices.

Prior to the completion of this report, NSPPD submitted a revised BWC policy that replaces the language allowing the shift supervisor to authorize the use of personally-owned recording devices with language allowing the Chief of Police or authorized designee to permit the use of personally-owned recording devices. In our opinion, this revised language is still contrary to the prohibition on the use of any device not owned and maintained by the agency, as discussed above. We recommend removing this passage and adding language to clarify that only BWCs issued and maintained by NSSPPD may be used.

Ms. Churchill advised us that the Arbitrator 360 software contains a configuration tool that allows the monitoring of all enabled BWCs in real time. In addition, she is able to determine the number of BWCs deployed by reviewing the schedule and/or payroll data.

As of September 4, 2024, NSPPD maintained a total of 3.375 TB of BWC data.

NSPPD BWC Physical, Technological and Procedural Safeguards

NSPPD BWC data are initially recorded to a hard drive in each officer's BWC. Data from each BWC is then uploaded to Panasonic's iPro CloUDE [Unified Digital Evidence] cloud service via a physical docking station located at the Police Department. In the event an officer fails to label the video, the default retention period is currently 90 days, but is being revised to seven years to avoid the accidental loss of data.

Officers have view-only access to their own data for report writing, trial preparation, data administration, investigatory purposes and other legitimate law enforcement purposes, as well as the ability to add or edit case numbers and titles.

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

Enhanced Surveillance Technology

NSPPD currently employs BWCs with only standard audio/video recording capabilities. NSPPD has 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 NSPPD 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 (CFS) 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 auditor reviewed the retained BWC videos to verify that this data was accurately documented in NSPPD records.

Audit Conclusions

In our opinion, the North St. Paul Police Department's Body-Worn Camera Program is substantially compliant with Minnesota Statutes §13.825 and §626.8473, with following exception:

While Rampart was advised that only agency-issued BWCs are used by NSPPD personnel, section 437.4 (a) of NSPPD's revised BWC policy allows the Chief of Police or designee to authorize the use of personally-owned recording devices, contrary to Minn. Stat. §13.825 Subd. 6, which states that "[w]hile on duty, a peace officer may only use a portable recording system issued and maintained by the officer's agency in documenting the officer's activities."

In addition, due to a lack of information provided by the agency, we are unable to express an opinion regarding NSPPD's compliance with the requirements included in §13.825 Subd. 8, which govern the sharing of BWC data with other agencies.

Finally, we noted that NSPPD's policy manual currently contains two body-worn camera policies: An earlier version, numbered 423, and the revised policy, numbered 437. We recommend removing the outdated policy from the manual in order to avoid confusion.

Daniel Gazelka

Rampart Audit LLC

2/10/2025

APPENDIX A:

Policy

423

North St. Paul Police Department
Policy Manual

Portable Audio/Video Recorders

423.1 PURPOSE AND SCOPE

This policy provides guidelines for the use of portable audio/video recording devices by members of this department while in the performance of their duties (Minn. Stat. § 626.8473). Portable audio/video recording devices include all recording systems whether body-worn, hand-held, or integrated into portable equipment.

This policy does not apply to mobile audio/video recordings, interviews, or interrogations conducted at any North St. Paul Police Department facility, undercover operations, wiretaps, or eavesdropping (concealed listening devices).

423.1.1 DEFINITIONS

Definitions related to this policy include:

Portable recording system - A device worn by a member that is capable of both video and audio recording of the member's activities and interactions with others or collecting digital multimedia evidence as part of an investigation and as provided in Minn. Stat. § 13.825.

423.2 POLICY

The North St. Paul Police Department may provide members with access to portable recorders for use during the performance of their duties. The use of recorders is intended to enhance the mission of the Department by capturing contacts between members of the Department and the public.

423.3 COORDINATOR

The Chief of Police or the authorized designee should designate a coordinator responsible for (Minn. Stat. § 626.8473; Minn. Stat. § 13.825):

(a) Establishing procedures for the security, storage, and maintenance of data and recordings.

1. The coordinator should work with the Custodian of Records and the member assigned to coordinate the use, access, and release of protected information to ensure that procedures comply with requirements of the Minnesota Government Data Practices Act (MGDPA) and other applicable laws (Minn. Stat. § 13.01 et seq.) (see the Protected Information and the Records Maintenance and Release policies).

2. The coordinator should work with the Custodian of Records to identify recordings that must be retained for a specific time frame under Minnesota law (e.g., firearm discharges,

certain use of force incidents, formal complaints).

(b) Establishing procedures for accessing data and recordings.

1. These procedures should include the process to obtain written authorization for access to non-public data by NSPPD members and members of other governmental entities and agencies.

(c) Establishing procedures for logging or auditing access.

(d) Establishing procedures for transferring, downloading, tagging, or marking events.

(e) Establishing an inventory of portable recorders including:

1. Total number of devices owned or maintained by the North St. Paul Police Department.

2. Daily record of the total number deployed and used by members and, if applicable, the precinct or district in which the devices were used.

3. Total amount of recorded audio and video data collected by the devices and maintained by the North St. Paul Police Department.

(f) Preparing the biennial audit required by Minn. Stat. § 13.825, Subd. 9.

(g) Notifying the Bureau of Criminal Apprehension (BCA) in a timely manner when new equipment is obtained by the North St. Paul Police Department that expands the type or scope of surveillance capabilities of the department's portable recorders.

(h) Ensuring that this Portable Audio/Video Recorders Policy is posted on the Department website.

423.4 MEMBER PRIVACY EXPECTATION

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

423.5 MEMBER RESPONSIBILITIES

Prior to going into service, uniformed members will be responsible for making sure that they are equipped with a portable recorder issued by the Department, and that the recorder is in good working order (Minn. Stat. § 13.825). If the recorder is not in working order or the member becomes aware of a malfunction at any time, the member shall promptly report the failure to their supervisor and obtain a functioning device as soon as reasonably practicable. Uniformed members should wear the recorder in a conspicuous manner at or above the mid-line of the waist and notify persons that they are being recorded, whenever reasonably practicable (Minn. Stat. § 626.8473).

Any member assigned to a non-uniformed position may carry an approved portable recorder at any time the member believes that such a device may be useful. Unless conducting a lawful recording in an authorized undercover capacity, non-uniformed members should wear the recorder in a conspicuous manner when in use or otherwise notify persons that they are being recorded, whenever reasonably practicable.

When using a portable recorder, the assigned member shall record their name, employee number, and the current date and time at the beginning and the end of the shift or other period of use, regardless of whether any activity was recorded. This procedure is not required when the recording device and related software captures the user's unique identification and the date and time of each recording.

Members should document the existence of a recording in any report or other official record of the contact, including any instance where the recorder malfunctioned or the member deactivated the recording (Minn. Stat. § 626.8473). Members should include the reason for deactivation.

423.6 ACTIVATION OF THE AUDIO/VIDEO RECORDER

This policy is not intended to describe every possible situation in which the recorder should be used, although there are many situations where its use is appropriate. Members should activate the recorder any time the member believes it would be appropriate or valuable to record an incident.

The recorder should be activated in any of the following situations:

(a) All enforcement and investigative contacts including stops and field interview (FI) situations

(b) Dispatched calls for service, prior to the arrival in the area or location for service, if practicable.

(c) Traffic stops including, but not limited to, traffic violations, stranded motorist assistance and all crime interdiction stops

(d) Self-initiated activity in which a member would normally notify Dispatch

(e) Any other contact that becomes adversarial after the initial contact in a situation that would not otherwise require recording

(f) When transporting a person relating to a call for service or self-initiated activity.

Members should remain sensitive to the dignity of all individuals being recorded and exercise sound discretion to respect privacy by discontinuing recording whenever it reasonably appears to the member that such privacy may outweigh any legitimate law enforcement interest in recording. Requests by members of the public to stop recording should be considered using this same criterion. Recording should resume when privacy is no longer at issue unless the circumstances no longer fit the criteria for recording.

At no time is a member expected to jeopardize his/her safety in order to activate a portable recorder or change the recording media. However, the recorder should be activated in situations described above as soon as reasonably practicable.

Except as otherwise directed, officers have discretion to record or not record incidental general citizen contacts that do not become law enforcement-related or adversarial and when a recording of the event would not yield information relevant to an ongoing investigation. Examples include, but are not limited to, assisting a motorist with directions, summoning a tow truck, or receiving general concerns from a citizen about crime trends.

Officers need not record persons being provided medical care unless there is reason to believe that the recording would document information having evidentiary value.

423.6.1 CESSATION OF RECORDING

Once activated, the portable recorder should continue recording until the conclusion of the incident or until it becomes readily apparent that additional recording is unlikely to capture information having any evidentiary value. A sergeant, supervisor or detective in charge of a scene can likewise direct the discontinuance of a recording when further recording is unlikely to capture additional information having evidentiary value. Officers should state the reasons for ceasing the recording on camera before deactivating their portable recorder. If circumstances change, officers should reactivate their cameras as required by this policy.

Officers may cease recording under the following situations:

(a) To protect the identity of an officer in an undercover capacity.

(b) To protect the identity of an informant.

(c) If a request is made for a portable recorder to be turned off by a party being contacted. The Officer should take into account the overall circumstances and what is most beneficial to all involved, before deciding to honor the request. For example, an officer may choose to turn off the portable recorder if its operation is inhibiting a victim or witness from giving a statement. Factors to consider may include the type of call and the vulnerability of the victim, such as the victim of a sexual assault.

(d) Members may temporarily stop recording the audio (tactical mute) only when discussing sensitive tactics with other personnel. The use and justification of the tactical mute should be verbalized with specificity before muting or documented with specificity in the incident report (or CAD notes if no report completed).

(e) When a supervisor has determined in advance the video or audio data could result in the disclosure of operational or tactical information which would compromise the effectiveness of future actions or jeopardize officer safety if released.

(f) When it reasonably appears to the officer that an individual's privacy outweighs any legitimate law enforcement interest in recording. Recording should resume when privacy is no longer an issue unless the circumstances no longer fit the criteria for recording.

(g) When recording is prohibited by a detention facility, detox, or medical facility.

(h) At search warrant scenes, the portable recorder may be deactivated once the entry is complete and the scene is safe. This deactivation would only occur after suspects are arrested and removed from the warrant location. If removing all other occupants is not possible or reasonable, at a minimum the cover officer(s) will have their portable recorder activated.

423.6.2 SURREPTITIOUS RECORDINGS

Minnesota law permits an individual to surreptitiously record any conversation in which one party to the conversation has given his/her permission (Minn. Stat. § 626A.02).

Members of the Department may surreptitiously record any conversation during the course of a criminal investigation in which the member reasonably believes that such a recording will be lawful and beneficial to the investigation.

Members shall not surreptitiously record another department member without a court order unless lawfully authorized by the Chief of Police or the authorized designee.

423.6.3 EXPLOSIVE DEVICE

Many portable recorders, including body-worn cameras and audio/video transmitters, emit radio waves that could trigger an explosive device. Therefore, these devices should not be used where an explosive device may be present.

423.7 PROHIBITED USE OF AUDIO/VIDEO RECORDERS

Members are prohibited from using department-issued portable recorders and recording media for personal use and are prohibited from making personal copies of recordings created while on- duty or while acting in their official capacity.

Members are also prohibited from retaining recordings of activities or information obtained while on-duty, whether the recording was created with department-issued or personally owned recorders. Members shall not duplicate or distribute such recordings, except for authorized legitimate department business purposes. All such recordings shall be retained at the Department.

Members are prohibited from using personally owned recording devices while on-duty without the express consent of the Shift Sergeant. Any member who uses a personally owned recorder for department-related activities shall comply with the provisions of this policy, including retention and release requirements and should notify the on-duty supervisor of such use as soon as reasonably practicable.

Recordings shall not be used by any member for the purpose of embarrassment, harassment or ridicule.

423.8 RETENTION OF RECORDINGS

All recordings shall be retained for a period consistent with the requirements of the organization's records retention schedule but in no event for a period less than 90 days.

If an individual captured in a recording submits a written request, the recording shall be retained for an additional time period. The coordinator should be responsible for notifying the individual prior to destruction of the recording (Minn. Stat. § 13.825).

Members shall not alter, erase, or destroy any recordings before the end of the applicable records retention period (Minn. Stat. § 626.8473).

423.8.1 RELEASE OF AUDIO/VIDEO RECORDINGS

Requests for the release of audio/video recordings shall be processed in accordance with the Records Maintenance and Release Policy.

423.8.2 ACCESS TO RECORDINGS

Except as provided by Minn. Stat. § 13.825, Subd. 2, audio/video recordings are considered private or nonpublic data.

Any person captured in a recording may have access to the recording. If the individual requests a copy of the recording and does not have the consent of other non-law enforcement individuals captured on the recording, the identity of those individuals must be blurred or obscured sufficiently to render the subject unidentifiable prior to release. The identity of on-duty peace officers may not be obscured unless their identity is protected under Minn. Stat. § 13.82, Subd. 17.

423.9 IDENTIFICATION AND PRESERVATION OF RECORDINGS

To assist with identifying and preserving data and recordings, members should download, tag or mark the recordings in accordance with procedure and document the existence of the recording in any related case report.

A member should transfer, tag or mark recordings when the member reasonably believes:

(a) The recording contains evidence relevant to potential criminal, civil or administrative matters.

(b) A complainant, victim or witness has requested non-disclosure.

(c) A complainant, victim or witness has not requested non-disclosure but the disclosure of the recording may endanger the person.

(d) Disclosure may be an unreasonable violation of someone's privacy.

(e) Medical or mental health information is contained.

(f) Disclosure may compromise an under-cover officer or confidential informant.

(g) The recording or portions of the recording may be protected under the Minnesota Data Practices Act.

Any time a member reasonably believes a recorded contact may be beneficial in a non-criminal matter (e.g., a hostile contact), the member should promptly notify a supervisor of the existence of the recording.

423.10 REVIEW OF RECORDED MEDIA FILES

When preparing written reports, members should review their recordings as a resource (see the Officer-Involved Shootings and Deaths Policy for guidance in those cases). However, members shall not retain personal copies of recordings. Members should not use the fact that a recording was made as a reason to write a less detailed report.

Supervisors are authorized to review relevant recordings any time they are investigating alleged misconduct or reports of meritorious conduct or whenever such recordings would be beneficial in reviewing the member's performance.

Recorded files may also be reviewed:

(a) By a supervisor as part of internal audits and reviews as required by Minn. Stat. § 626.8473.

(b) Upon approval by a supervisor, by any member of the Department who is participating in an official investigation, such as a personnel complaint, administrative investigation, or criminal investigation.

(c) Pursuant to lawful process or by court personnel who are otherwise authorized to review evidence in a related case.

(d) By media personnel with permission of the Chief of Police or the authorized designee.

(e) In compliance with the Minnesota Data Practices Act request, if permitted or required by the Act, including pursuant to Minn. Stat. § 13.82, Subd. 15, and in accordance with the Records Maintenance and Release Policy.

All recordings should be reviewed by the Custodian of Records prior to public release (see the Records Maintenance and Release Policy). Recordings that are clearly offensive to common sensibilities should not be publicly released unless disclosure is required by law or order of the court (Minn. Stat. § 13.82, Subd. 7; Minn. Stat. § 13.825, Subd. 2).

423.10.1 MEMBER RESPONSIBILITIES

When preparing written reports, members should review their recordings as a resource. Members shall not retain personal copies of recordings. Members may access and view stored portable recorder data of incidents in which they have been directly involved and view saved data to:

(a) Refresh memories of events and statements prior to completing reports or making statements.

(b) Ensure the system is operating properly.

(c) Self-critique.

Officers may display portions of the portable recorder footage to witnesses for purposes of investigation as allowed by Minn. Stat. § 13.82, Subd. 15. Officers should generally limit these displays in order to protect against the incidental disclosure of individuals whose identities are not public.

All employees who access portable recorder data outside of policy requirements and standard operating procedures will be required to document the reason for their access according to system capabilities. Members are prohibited from accessing portable recorder data for non-business reasons and from sharing the data for non-law enforcement related purposes, including uploading portable recorder data recorded or maintained by this agency to public and social media websites. Employees seeking access to portable recorder data for non-business reasons may make a request for it in the same manner as any member of the public.

Field Training Officers may utilize portable recorder data with trainees for the purpose of providing coaching and feedback on the trainee's performance.

Officers shall not intentionally edit, alter or erase any portable recorder recording unless otherwise expressly authorized by the Chief or designee.

423.10.2 SUPERVISOR RESPONSIBILITIES

When preparing written reports, members should review their recordings as a resource (See the Officer-Involved Shootings and Deaths Policy for guidance in those cases). However, members shall not retain personal copies of recordings.

Supervisors are authorized to review relevant recordings any time they are investigating alleged misconduct or reports of meritorious conduct or whenever such recordings would be beneficial in reviewing the member's performance. It is not the intent of the department to review digital evidence for the purpose of general performance review, for routine preparations of performance reports, or to discover policy violations.

Recorded files may also be reviewed:

(a) Upon approval by a supervisor, by any member of the Department who is participating in an official investigation, such as a personnel complaint, administrative investigation or criminal investigation.

(b) Pursuant to lawful process or by court personnel who are otherwise authorized to review evidence in a related case.

(c) In compliance with the Minnesota Data Practices Act request, if permitted or required by the Act, including pursuant to Minn. Stat. § 13.82, Subd. 15, and in accordance with the Records Maintenance and Release Policy.

At least once per month, supervisors will randomly review portable recorder usage by each officer to ensure compliance with this policy (Minn. Stat. § 626.8473, Subd 3). Supervisors reviewing event recording should remain focused on the incident or incidents in question and review only those recordings relevant to their investigative scope. If improper conduct is discovered during any review of digital evidence, the Supervisor may take the necessary steps to counsel or initiate an internal affairs investigation in adherence with department policy.

Portable recorder data may be viewed for supervisory or administrative purposes including, but not limited to:

(a) Any incident where a member of the department is injured or killed during the performance of their duties.

(b) Any incident involving the use of force by a member of the department so the supervisor can validate the force used was within policy.

(c) Any in-custody death.

(d) Any police pursuit.

(e) When any member of the department intentionally or unintentionally discharges a firearm at a person regardless of whether an individual is struck.

(f) Officer involved traffic collision.

(g) Prior to release of a recording in response to proper legal request (e.g., subpoena or other court order).

(h) In preparation for a civil deposition or responding to an interrogatory where the incident arises from the employee's official duties.

(i) For investigations undertaken by the department, for the purpose of proving or disproving specific allegations of misconduct.

423.11 COPYING OF RECORDED DATA

Much of the data saved on the server will not be needed for long term retention and will be automatically purged after a minimal time period or when a determination is made that the data no longer needs to be retained. Other recorded data will require long term retention and/or transfer to another type of media. Copies of recorded data may be made for the following reasons:

(a) For use as evidence in court.

(b) For review by prosecuting or defense attorneys.

(c) For use in investigating complaints against officers.

(d) To assist officers and investigators in an investigation.

(e) For officer review prior to a court appearance.

(f) For long term records archiving.

(g) For use as authorized training material.

(h) As part of a data request.

(i) Other uses as approved by the Chief of Police.

The duplication of recorded data from the server to other media is the responsibility of a person(s) designated by the Chief of Police. Requests for duplicate recorded data should be made in writing and submitted to the person(s) designated by the Chief of Police to duplicate data. The data request should include the reason for the request. After use, all duplicates shall be returned to the designee. The copying of all data will be for official business only and subject to Minnesota Data Practices laws. Exceptions shall be approved by the Chief of Police. Data recorded by the portable recorder and stored on any media is classified as official government data and subject to Minnesota Data Practices.

423.12 ACCOUNTABILITY

Any member who accesses or releases recordings without authorization may be subject to discipline (See the Standards of Conduct and the Protected Information policies) (Minn. Stat. § 626.8473).

An independent biennial audit will be conducted of the portable recorder data to determine if the data is appropriately classified, how the data is used, and whether the data is destroyed per Minn, Stat. § 13.82. The results of the audit are public information and will be reported to the North St Paul City Council and the Legislative Commission on Data Practices and Personal Data Privacy no later than 60 days following the completion of the audit (Minn. Stat. § 13.825 Subd. 9).

APPENDIX B:

Policy

437

North St. Paul Police Department

Policy Manual

Body-Worn Cameras

437.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the use of a body-worn camera (BWC) by members of this department and for the access, use, and retention of department BWC media (Minn. Stat. § 626.8473).

The provisions of this policy, including notice, documentation, access, and retention, also apply to other portable audio/video recording devices used by members, where applicable.

This policy does not apply to undercover operations, wiretaps, or eavesdropping (concealed listening devices).

437.1.1 DEFINITIONS

Definitions related to this policy include:

Activate - To place a BWC in active mode (also called event mode). In active mode, the BWC records both video and audio.

BWC media - The video, audio, and images captured by department BWCs and the associated metadata.

BWC media systems - Any software, including web-based programs and mobile applications, used by the Department to upload/download, store, view, transfer, and otherwise maintain BWC media.

Deactivate - To place a BWC in buffering mode (also called ready or pre-event mode). In buffering mode, the BWC records video (without audio) in short, predetermined intervals that are retained only temporarily. However, when a BWC is activated, the interval recorded immediately prior to activation is then stored as part of the BWC media. Deactivate does not mean powering off the BWC.

Event - A general term referring to a set of circumstances that may, but does not necessarily, correlate directly to a single public safety incident.

437.2 POLICY

It is the policy of the Department to use BWCs and BWC media for evidence collection and to accurately document events in a way that promotes member safety and department accountability and transparency while also protecting the privacy of members of the public.

437.3 RESPONSIBILITIES

437.3.1 BWC COORDINATOR RESPONSIBILITIES

The Chief of Police or the authorized designee should delegate certain responsibilities to a BWC coordinator (Minn. Stat. § 13.825; Minn. Stat. § 626.8473).

The responsibilities of the coordinator include:

(a) Serving as a liaison between the Department and the BWC manufacturer/distributor and any third-party media storage vendor.

(b) Developing inventory and documentation procedures for issuing and tracking BWC equipment, including properly marking BWCs as property of the Department, recording the date each BWC is placed into or taken out of service, and maintaining the following information:

1. The total number of devices owned or maintained by the North St. Paul Police Department
2. The daily record of the total number deployed and used by members and, if applicable, the precinct or district in which the devices were used
3. The total amount of recorded audio and video data collected by the BWC media systems and maintained by the North St. Paul Police Department

(c) Assisting with troubleshooting and maintenance of BWC equipment and media systems and, when necessary, coordinating the repair or replacement of BWCs.

1. All equipment and system malfunctions and their resolutions should be documented, and maintenance and repair records should be maintained for all BWCs.

(d) Managing BWC media systems so that:

1. Access is limited to the minimum necessary authorized users and user privileges are restricted to those necessary for the member to conduct assigned department duties.
2. Security requirements, such as two-factor authentication and appropriate password parameters, are in place for user credentials.
3. Procedures include a process to obtain written authorization for access to non- public data by NSPPD members and members of other governmental entities and agencies. The procedures are as follows: County Attorney will request via email, which is then attached to the case record(s); City Attorney will request via email, which is delivered on a USB drive by Community Service Officer and/ or Officer.
4. Portable Audio/Video Recorder data shall be made available to prosecutors, courts, and other criminal justice entities as provided by law.

(e) Configuring BWC media systems, or developing manual procedures, so that media is appropriately categorized and retained according to the event type tagged by members.

(f) Retaining audit logs or records of all access, alteration, and deletion of BWC media and media

systems, and conducting periodic audits to ensure compliance with applicable laws, regulations, and department policy.

(g) Developing and updating BWC training for members who are assigned a BWC or given access to BWC media systems.

(h) Coordinating with the community relations coordinator to (see the Community Relations Policy):

1. Provide the public with notice of the department's use of BWCs (e.g., posting on the department website or social media pages).
2. Gain insight into community expectations regarding BWC use.

(i) Coordinating with the Administrative Assistant to (see the Administration/Records, Records Maintenance and Release, and Protected Information policies):

1. Determine and apply proper retention periods to BWC media (e.g., firearm discharges, certain use of force incidents, formal complaints).
2. Develop procedures for the appropriate release of BWC media.
3. Ensure procedures comply with the requirements of the Minnesota Government Data Practices Act and other applicable laws (Minn. Stat. § 13.01 et seq.).

U) Coordinating with the Evidence Room to develop procedures for the transfer, storage, and backup of evidentiary BWC media (see the Evidence Room Policy).

(k) Preparing the biennial audit required by Minn. Stat. § 13.825, Subd. 9.

(l) Notifying the Bureau of Criminal Apprehension (BCA) in a timely manner when new equipment is obtained by the North St. Paul Police Department that expands the type or scope of surveillance capabilities of the department's portable recorders.

437.3.2 MEMBER RESPONSIBILITIES

Every member issued a BWC is responsible for its proper use, safekeeping, and maintenance.

At the beginning of each shift or period of BWC use, the member should inspect their assigned BWC to confirm it is charged and in good working order. As part of the inspection, the member should perform a function test by activating the BWC and recording a brief video stating their name, identification number, assignment, and the date and time (Minn. Stat. § 13.825; Minn. Stat. § 626.8473).

Members should wear their assigned BWC on their outermost garment positioned at or above the mid-line of the waist (Minn. Stat.§ 626.8473). Members are responsible for ensuring there are no obstructions and that the BWC remains in a position suitable for recording.

When a BWC is not in the physical possession of the member to which it is assigned, it should be placed on the charging dock and stored in a secure location.

Members shall report any malfunction or damage to the BWC coordinator or on-duty supervisor as soon as practicable and, if possible, obtain a functioning BWC to use either temporarily while repairs are being made to the member's BWC or as a permanent replacement (Minn. Stat. § 626.8473).

Members shall comply with this policy's provisions while performing law enforcement activities under the command and control of another law enforcement agency (Minn. Stat. § 626.8473).

437.3.3 MEMBER POLICY RESPONSIBILITIES

The guidelines set forth in this policy shall be followed while working under the command and control of another law enforcement organization or as a federal law enforcement agent.

437.4 BWC USE

The following guidelines apply to the use of BWCs:

(a) Only department-issued BWCs should be used unlessthe express consent of the Chief of Police or the authorized designee (Minn. Stat. § 13.825).

(b) BWCs should only be used by the member or members to whom it was issued unless otherwise authorized by a supervisor.

(c) The use of department-issued BWCs shall be strictly limited to department-related activities.

(d) Members shall not use BWCs or BWC media systems for which they have not received prior authorization and appropriate training.

(e) Members shall immediately report unauthorized access or use of BWCs or BWC media systems by another member to their supervisor or the Chief of Police.

437.4.1 PROHIBITIONS

BWCs should not be used to record:

(a) Routine administrative activities of the Department that do not involve interactions with the public. Care should be taken to avoid incidentally recording confidential documents that the Department has a duty to keep secure (i.e., criminal justice information).

(b) Areas within the department facilities where members have a reasonable expectation of privacy (e.g., locker rooms or dressing areas, breakrooms) unless responding to a call for service or conducting an investigation.

(c) Conversations of other members without their knowledge.

(d) When a member is taking an authorized break or otherwise engaged in personal activities.

(e) In a courtroom unless responding to a call for service or emergency situation.

(f) Interactions with undercover officers or confidential informants.

(g) Strip searches.

BWCs shall not be used for the purpose of embarrassment, harassment, or ridicule of any individual or group.

437.5 ACTIVATION OF BWC

Members should activate their BWC during all calls for service and the performance of law enforcement-related functions. Members are not required to activate their BWC during casual or informal contacts with members of the public that are not part of or related to law enforcement functions. However, members should activate their BWC any time a contact with an individual

becomes hostile or adversarial.

Unless otherwise authorized by this policy or approved by a supervisor, BWCs should remain activated until the call for service or law enforcement-related function has concluded. A member may cease recording if they are simply waiting for a tow truck or a family member to arrive, or in other similar situations.

At no time is a member expected to jeopardize their safety to activate their BWC. However, the BWC should be activated as soon as reasonably practicable in required situations.

If a member attempts to activate their BWC but the BWC fails to record an event, the member should notify their supervisor as soon as practicable.

437.5.1 NOTICE OF RECORDING

Unless otherwise approved based on unique circumstances, a member should wear the BWC in a manner that is conspicuous and shall answer truthfully if asked whether they are equipped with a BWC or if their BWC is activated.

437.5.2 PRIVACY CONSIDERATIONS

Members should remain sensitive to the dignity of individuals being recorded and should exercise sound discretion with respect to privacy concerns.

When responding to a place where individuals have an expectation of privacy (e.g., private residences, medical or mental health facilities, restrooms) or to a sensitive situation (e.g., individuals partially or fully unclothed), members are permitted to mute or deactivate their BWC if it reasonably appears that the privacy concern outweighs any legitimate department interest in recording the event. Members may also mute or deactivate their BWC:

(a) To protect the privacy of a victim or witness.

(b) When an individual wishes to provide information anonymously.

(c) To avoid recording a confidential informant or undercover officer.

(d) When discussing case tactics or strategy.

(e) During private conversations with other members or emergency responders.

Members should choose to mute rather than deactivate BWCs when practicable. Deactivation should only be used when muting the BWC will not accomplish the level of privacy necessary for the situation.

Before muting or deactivating their BWC, the member should verbally narrate the reason on the recording. As soon as possible once the privacy concern is no longer an issue, or when circumstances change so that the privacy concern no longer outweighs the department's interest in recording the event (e.g., the individual becomes combative, the conversation ends), the member should unmute or reactivate their BWC and verbally note that recording has resumed.

437.5.3 LIVESTREAMING

Livestreaming enables authorized individuals to remotely view the audio and video captured by a member's BWC in real time. Only supervisors and dispatchers approved by the Chief of Police or the authorized designee shall have access to livestreaming capabilities.

Livestreaming should only be activated:

(a) For purposes of member safety when the member is not responding to their radio or there is some other indication of distress.

(b) To assist with situational awareness or tactical decisions during a significant incident.

(c) When requested by the member.

437.5.4 DOCUMENTATION

Members are encouraged to provide narration while using a BWC when it would be useful to provide context or clarification of the events being recorded. However, the use of a BWC is not a replacement for written reports and should not be referred to in a written report in place of detailing the event.

Every report prepared by a member who is issued a BWC should state "BWC available" or "BWC unavailable," as applicable, and should document:

(a) To the extent practicable and relevant, the identity of individuals appearing in the BWC media.

(b) An explanation of why BWC media is unavailable including any malfunction, damage, or battery issue that resulted in the failure of the BWC to capture all or part of the event.

(c) Any exigency or other circumstances that prevented the member from immediately activating the recording at the beginning of the event.

(d) Any period of the event in which the member deactivated or muted their BWC and the reason for such action.

(e) If livestreaming was activated during the event, the reason for livestreaming and the members who communicated or participated in the event through BWC livestreaming.

437.6 UPLOADING BWC MEDIA

Unless otherwise authorized by a supervisor, all media from a member's BWC should be properly uploaded and tagged before the end of their shift. BWC media related to a serious or high-profile event (e.g., search for a missing child, active shooter situation) should be uploaded and tagged as soon as practicable upon returning to the Department.

Following an officer involved shooting or death or other event deemed necessary, a supervisor should take possession of the BWC for each member present and upload and tag the BWC media.

437.6.1 TAGGING BWC MEDIA

Members should tag all media captured by their BWC with their name and/or identification number, the case or incident number, and the event type. BWC media should be tagged upon uploading or, if capabilities permit tagging in the field, as close to the time of the event as possible. If more

than one event type applies to BWC media, it should be tagged with each event type. If BWC media can only be tagged with a single event type, the media should be tagged using the event type with the longest retention period.

BWC media depicting sensitive circumstances or events should be tagged as restricted. BWC media should be flagged for supervisor review when it pertains to a significant event such as:

(a) An incident that is the basis of a formal or informal complaint or is likely to result in a complaint.

(b) When a member has sustained a serious injury or a line-of-duty death has occurred.

(c) When a firearm discharge or use of force incident has occurred.

(d) An event that has attracted or is likely to attract significant media attention.

Supervisors should conduct audits at regular intervals to confirm BWC media is being properly uploaded and tagged by their subordinates.

437.7 BWC MEDIA

All BWC media is the sole property of the Department. Members shall have no expectation of privacy or ownership interest in the content of BWC media.

All BWC media shall be stored and transferred in a manner that is physically and digitally secure with appropriate safeguards to prevent unauthorized modification, use, release, or transfer. Contracts with any third-party vendors for the storage of BWC media should include provisions specifying that all BWC media remains the property of the Department and shall not be used by the vendor for any purpose without explicit approval of the Chief of Police or the authorized designee.

Members shall not alter, copy, delete, release, or permit access to BWC media other than as permitted in this policy without the express consent of the Chief of Police or the authorized designee.

BWC media systems should not be accessed using personal devices unless authorized by the Chief of Police or the authorized designee.

437.7.1 ACCESS AND USE OF BWC MEDIA

BWC media systems shall only be accessed by authorized members using the member's own login credentials and in accordance with the Information Technology Use Policy.

BWC media shall only be accessed and viewed for legitimate department-related purposes in accordance with the following guidelines:

(a) BWC media tagged as restricted should only be accessible by those designated by the Chief of Police or the authorized designee.

(b) Members may review their own BWC media for department-related purposes. Members should document in their report if they reviewed BWC media before completing the report.

(c) Investigators may review BWC media pertaining to their assigned cases.

(d) A member testifying regarding a department-related event may review the pertinent BWC media before testifying.

(e) Supervisors are permitted to access and view BWC media of their subordinates.

1. Supervisors should review BWC media that is tagged as a significant event or that the supervisor is aware pertains to a significant event.

2. Supervisors should conduct documented reviews of their subordinate's BWC media at least annually to evaluate the member's performance, verify compliance with department procedures, and determine the need for additional training. The review should include a variety of event types when possible. Supervisors should review BWC media with the recording member when it would be beneficial to provide guidance or to conduct one-on-one informal training for the member (Minn. Stat.§ 626.8473).

3. Supervisors should conduct periodic reviews of a sample of each subordinate's BWC media to evaluate BWC use and ensure compliance with this policy.

(f) The Training Officer is permitted to access and view BWC media for training purposes.

1. The Training Officer should conduct a quarterly review of a random sampling of BWC media to evaluate department performance and effectiveness and to identify specific areas where additional training or changes to protocols would be beneficial. Training Committee members may review BWC media as part of their review to identify training needs.

2. The Training Officer may use BWC media for training purposes with the approval of the Chief of Police or the authorized designee. The Training Officer should use caution to avoid embarrassing or singling out a member and, to the extent practicable, should seek consent from the members appearing in the BWC media before its use for training. When practicable, sensitive issues depicted in BWC media should be redacted before being used for training.

(g) The Administrative Assistant may access BWC media when necessary to conduct department-related duties.

(h) The BWC coordinator may access BWC media and the BWC media system as needed to ensure the system is functioning properly, provide troubleshooting assistance, conduct audits, and fulfill other responsibilities related to their role.

(i) Any member who accesses or releases BWC media without authorization may be subject to consequences, civil or criminal (see the Standards of Conduct and the Protected Information policies for additional guidance) (Minn. Stat.§ 626.8473).

437.7.2 PUBLIC ACCESS

Unless disclosure is required by law or a court order, BWC media should not be released to the public if:

(a) It is clearly offensive to common sensibilities (Minn. Stat. § 13.82, Subd. 7; Minn. Stat. § 13.825, Subd. 2).

(b) It unreasonably violates a person's privacy or depicts the interior of:

1. A private residence.
2. A facility that offers health care, mental health or substance abuse treatment, or social services.
3. A school building.
4. Any other building in which public access is restricted or which implicates heightened security concerns.

Except as provided by Minn. Stat. § 13.825, Subd. 2 or pursuant to Minn. Stat. § 13.82, Subd. 15, BWC media is considered private or nonpublic data.

Any person captured on BWC media may have access to the BWC media. If the individual requests a copy of the BWC media and does not have the consent of other non-law enforcement individuals captured on the BWC media, the identity of those individuals must be blurred or obscured sufficiently to render the person unidentifiable prior to release. The identity of on-duty peace officers may not be obscured unless their identity is protected under Minn. Stat. § 13.82, Subd. 17 (Minn. Stat.§ 13.825, Subd. 4).

Requests for the release of BWC media shall be processed in accordance with the Records Maintenance and Release Policy. The Administrative Assistant should review BWC media before public release.

See the Officer-Involved Shootings and Deaths Policy regarding BWC media requests pursuant to Minn. Stat. § 13.825 relating to deaths by use of force.

437.7.3 DATA CLASSIFICATION AND COURT AUTHORIZED DISCLOSURE

For specific classification and court disclosure rules please see the Minnesota Statute:

a) Data collected by a portable recording system are private data on individuals or nonpublic data, subject to the following:

(1) data that record, describe, or otherwise document actions and circumstances surrounding either the discharge of a firearm by a peace officer in the course of duty, if a notice is required under section 626.553, subdivision 2, or the use of force by a peace officer that results in substantial bodily harm, as defined in section 609.02, subdivision 7a, are public;

(2) data are public if a subject of the data requests it be made accessible to the public, except that, if practicable, (i) data on a subject who is not a peace officer and who does not consent to the release must be redacted, and (ii) data on a peace officer whose identity is protected under section 13.82, subdivision 17, clause (a), must be redacted;

(3) subject to paragraphs (b) to (d), portable recording system data that are active criminal investigative data are governed by section 13.82, subdivision 7, and portable recording system data that are inactive criminal investigative data are governed by this section;

(4) portable recording system data that are public personnel data under section 13.43, subdivision 2, clause (5), are public; and

(5) data that are not public data under other provisions of this chapter retain that classification.

(b) Notwithstanding section 13.82, subdivision 7, 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 following individuals, 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, subject to paragraphs (c) and (d):

(1) the deceased individual's next of kin;

(2) the legal representative of the deceased individual's next of kin; and

(3) the other parent of the deceased individual's child.

(c) A law enforcement agency may deny a request to inspect portable recording system data under paragraph (b) if the agency determines that there is a compelling reason that inspection would interfere with an active investigation. If the agency denies access under this paragraph, the chief law enforcement officer must provide a prompt, written denial to the individual in paragraph (b) 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.

(d) 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 what is 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.

(e) A law enforcement agency may redact or withhold access to portions of data that are public under this subdivision if those portions of data are clearly offensive to common sensibilities.

(f) Section 13.04, subdivision 2, does not apply to collection of data classified by this subdivision.

(g) Any person may bring an action in the district court located in the county where portable recording system data are being maintained to authorize disclosure of data that are private or nonpublic under this section or to challenge a determination under paragraph (e) to redact or withhold access to portions of data because the data are clearly offensive to common sensibilities. The person bringing the action must give notice of the action to the law enforcement agency and subjects of the data, if known. The law enforcement agency must give notice to other subjects of the data, if known, who did not receive the notice from the person bringing the action. The court may order that all or part of the data be released to the public or to the person bringing the action. In making this determination, the court shall consider whether the benefit to the person bringing the action or to the public outweighs any harm to the public, to the law enforcement agency, or to a subject of the data and, if the action is challenging a determination under paragraph (e), whether the data are clearly offensive to common sensibilities. The data in dispute must be examined by the court in camera. This paragraph does not affect the right of a defendant in a criminal proceeding to obtain access to portable recording system data under the Rules of Criminal Procedure.

437.8 RETENTION OF BWC MEDIA

Non-evidentiary BWC media should be retained in accordance with state records retention laws but in no event for a period less than 90 days (Minn. Stat. § 13.825).

Unless circumstances justify continued retention, BWC media should be permanently deleted upon the expiration of the retention period in a way that it cannot be retrieved. BWC media shall not otherwise be deleted by any person without the authorization of the Chief of Police or the authorized designee.

If an individual captured on BWC media submits a written request, the BWC media shall be retained for an additional time period. The BWC coordinator should be responsible for notifying the individual prior to destruction of the BWC media (Minn. Stat. § 13.825).

Members shall not alter, erase, or destroy any BWC media, before the end of the applicable retention period (Minn. Stat. § 626.8473).

437.8.1 EVIDENTIARY BWC MEDIA

BWC media relevant to a criminal prosecution should be exported from the BWC media system and securely transferred to digital evidence storage according to established department procedures. Evidentiary BWC media is subject to the same laws, policies, and procedures as all other evidence, including chain of custody, accessibility, and retention periods (see the Evidence Room Policy).

Evidentiary BWC media that documents an officer's use of deadly force must be maintained indefinitely (Minn. Stat. § 13.825; Minn. Stat. § 626.8473).

437.8.2 MINNESOTA DATA RETENTION STATUTE§ 13.825

(a) Portable recording system data that are not active or inactive criminal investigative data and are not described in paragraph (b) or (c) must be maintained for at least 90 days and destroyed according to the agency's records retention schedule approved pursuant to section 138.17.

(b) Portable recording system data must be maintained for at least one year and destroyed according to the agency's records retention schedule approved pursuant to section 138.17 if:

(1) the data document (i) the discharge of a firearm by a peace officer in the course of duty if a notice is required under section 626.553, subdivision 2, or (ii) the use of force by a peace officer that results in substantial bodily harm; or

(2) a formal complaint is made against a peace officer related to the incident.

(c) Portable recording system data that document a peace officer's use of deadly force must be maintained indefinitely.

(d) If a subject of the data submits a written request to the law enforcement agency to retain the recording beyond the applicable retention period for possible evidentiary or exculpatory use related to the circumstances under which the data were collected, the law enforcement agency shall retain the recording for an additional time period requested by the subject of up to 180 days

and notify the requester that the recording will then be destroyed unless a new request is made under this paragraph.

(e) Notwithstanding paragraph (b), (c), or (d), a government entity may retain a recording for as long as reasonably necessary for possible evidentiary or exculpatory use related to the incident with respect to which the data were collected.

437.9 TRAINING

The BWC coordinator should ensure that each member issued a BWC receives initial training before use, and periodic refresher training thereafter. Training should include:

(a) Proper use of the BWC device and accessories.

(b) When BWC activation is required, permitted, and prohibited.

(c) How to respond to an individual's request to stop recording.

(d) Proper use of the BWC media systems, including uploading and tagging procedures.

(e) Security procedures for BWC media, including appropriate access and use.

Members who are not issued a BWC but who have access to BWC media systems shall receive training on the BWC media system, including appropriate access, use, and security procedures.