INDEPENDENT AUDITOR'S REPORT

North Branch Police Department

DECEMBER 11TH, 2024

Audit Overview and Recommendations

Dear North Branch City Council and Chief Meyer:

We have audited the body-worn camera (BWC) program of the North Branch Police Department (NBPD) for the two-year period ended 9/19/2024. 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 Branch Police Department. Our responsibility is to express an opinion on the operations of this program based on our audit.

On October 25, 2024, Rampart Audit LLC (Rampart) met with Chief Dan Meyer, who provided information about NBPD'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 NBPD's recordkeeping.

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

NBPD 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.

Chief Meyer advised us that North Branch PD's BWC program began operations on September 20, 2022, following a public notification process that occurred during 2021. Chief Meyer provided the following documentation to show that NBPD had met the public notification, comment and hearing requirements contained in Minnesota Statute §626.8473 Subd. 2:

- A screenshot of a public hearing notice, dated 8/26/2021, posted on the City of North Branch website, advising that a public hearing would be held at 7:00 PM on 9/14/2021 at the North Branch City Hall for the purpose of receiving comments and testimony from members of the

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

public regarding NBPD's proposed BWC program and policy. The post included a link to the proposed BWC policy, as well as a physical address to mail written comments. The notice also indicated that a physical copy of the notice was posted at City Hall, and was published in the Isanti-Chisago *County News*.

- A copy of the questionnaire used in an online survey to solicit public opinion regarding various facets of a BWC program.
- The results of this survey.
- A report from Chief Meyer to the North Branch City Council, providing a cost analysis and a recommendation to purchase Motorola BWCs, as these would integrate with the department's existing squad-based cameras.
- A copy of the minutes of the September 14, 2021, North Branch City Council meeting, documenting that a public hearing was held for the purpose of receiving comments from the public regarding the proposed BWC policy and program.
- A copy of the North Branch City Council resolution approving NBPD's proposed BWC policy, dated November 9, 2021.

In our opinion, NBPD met the requirements contained in Minn. Stat. §626.8473 Subd. 2 prior to the implementation of its BWC program.

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

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

NBPD BWC WRITTEN POLICY

As part of this audit, we reviewed NBPD'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 NBPD 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.

NBPD 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.

North Branch Police Department's BWC policy notes that the agency follows the General Records Retention Schedule for Minnesota Cities, but also provides specific retention periods for certain types of data. The Data Retention section of NBPD'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." This section also includes the required retention period for each of the individual data categories listed above, except for Subd. 3(c) data, which is addressed as follows in the Data Security Safeguards section: "The full, unedited, and unredacted recording of a peace officer using deadly force must be maintained indefinitely." The policy also specifies that:

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

In our opinion, North Branch PD's BWC policy meets the retention requirements contained in Minn. Stat. §13.825 Subd. 3.

The Data Security Safeguards section of NBPD's BWC policy also states that: "Officers and department staff shall not intentionally edit, alter, or erase/destroy any BWC recording prior to [the] expiration of the applicable retention period." As discussed in Clause 2 of the Policy section of this report, a BWC policy must prohibit altering, erasing or destroying not only BWC recordings themselves prior to their scheduled expiration date, but also any data and metadata[2] associated with those recordings. We recommend adding language to the passage quoted above to clarify that the same prohibitions also apply to any associated data or metadata.

Prior to the issuance of this report, NBPD submitted a revised policy that added the words "data, metadata or" so the sentence now reads, "Officers and department staff shall not intentionally edit, alter, or erase/destroy any data, metadata or BWC recording prior to [the] expiration of the applicable retention period."

NBPD employs Motorola V300 body-worn cameras and utilizes Motorola's CommandCentral Cloud Service storage and manages BWC data retention through automated retention settings in the

[2] BWC metadata would commonly include call type or classification and any other associated tags, such as CFS or ICR number, as well as data privacy indicators (e.g., juvenile) that describe or otherwise identify the recording.

VideoManager EL 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 by supervisors and the office manager as needed. If an officer fails to assign a data classification, the default retention period is 90 days.

NBPD's BWC policy states that:

> Each officer using a BWC is responsible for transferring or assuring the proper transfer of the data from his or her camera to data storage 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 the responsibility for transferring the data from it.

The policy further states that "[o]fficers shall label the BWC data files with the proper event tag at the time of capture or transfer to storage…"

Chief Meyer advised that the Motorola body-worn cameras are capable of uploading data wirelessly via NBPD squad cars, but also utilize a physical docking station located at the North Branch Police Department.

In our opinion, NBPD's revised BWC policy is substantially compliant with respect to applicable data retention requirements and is attached as Appendix B.

NBPD BWC Data Destruction

As discussed above, NBPD's BWC data are stored on Motorola's cloud-based storage service, CommandCentral, with data retention and deletion schedules managed automatically through the VideoManager EL video management software based on the assigned data classification of each video.

Motorola describes its CommandCentral cloud service as CJIS compliant and notes that the service is routinely and automatically updated to maintain compliance.

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

NBPD BWC Data Access

The Administering Access to BWC Data section of NBPD's BWC policy states that, "[o]fficers shall refer members of the media or public seeking access to BWC data to the police department's administrative staff who shall process the request in accordance with the MGDPA [Minnesota Government Data Practices Act] and other governing laws."

Chief Meyer advised us that that all requests for BWC data from the public or media are made in writing using North Branch Police Department's data request form, or via email. Requests from the public are processed by the NBPD office manager, while requests from the media are directed to Chief Meyer. BWC video is provided via internet link.

NBPD's BWC policy states 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." In addition, "BWC data shall be made available to prosecutors, courts, and other criminal justice entities as provided by law." Requests from other law enforcement agencies, prosecutors and probation personnel follow the same procedure as the public to request BWC data, and such requests are processed and fulfilled in the same manner. Data requests from prosecutors may also be fulfilled by the NBPD administrative assistant.

Chief Meyer indicated that NBPD has a general verbal understanding about any receiving agency's obligations under §13.825 Subd. 7 and Subd. 8. Chief Meyer also advised us that each BWC data email sent to a requesting agency contains the following message:

> WARNING Anyone with access to this link can view the material. You are responsible for ensuring that only authorized parties are provided with this link.

Rampart recommends obtaining written acknowledgements of these obligations.

Prior to the issuance of this report, NBPD noted they have drafted a written form that needs to be filled out and returned to them prior to another agency receiving BWC data. The requesting agency will acknowledge their understanding and duties and obligations under 13.825 sub 7 & 8 on the form. NBPD subsequently provided an updated BWC policy that states:

> Any law enforcement agency who requests BWC data must complete and sign a BWC Agency Sharing Data Form. Law enforcement agencies that receive the data must comply with all data classification, destruction, and security requirements of Minn. Stat. § 13.825.

An additional change was also made in the updated policy to this section that states:

> Portable recording system data may not be shared with, disseminated to, sold to, or traded with any other individual or entity unless explicitly authorized by this section or other applicable law.

A copy of this revised policy is attached to this report as Appendix B.

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. A review of Part A, Death resulting from force – access to data by survivors and legal counsel, of the Administering Access to BWC Data section of North Branch PD's BWC policy shows that NBPD has incorporated these requirements into its written policy.

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

NBPD BWC Data Classification

The policy defines data subjects "for purposes of administering access to BWC data," and states that "BWC data is [sic] presumptively private." The policy further states that "BWC recordings are classified as private data about the data subjects unless there is a specific law that provides differently." Active criminal investigation data are classified as confidential. NBPD BWC Policy also identifies certain categories of BWC data that are public.

As noted in the preceding section, North Branch PD has incorporated the changes the Minnesota State Legislature made in 2023 regarding BWC data documenting incidents involving the use of deadly force, including the requirement that, subject to limited redaction and certain exceptions, such BWC data be released to the public no later than 14 days after the incident.

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

NBPD BWC Internal Compliance Verification

The Agency Use of Data section of the NBPD BWC policy states that "[a]t least once a month, supervisors will randomly review BWC usage by each officer to whom a BWC is issued or available for use, to ensure compliance with this policy." Chief Meyer advised that in addition to random reviews, supervisors also review use-of-force incidents, pursuits and incidents giving rise to complaints.

The Policy section of NBPD's BWC policy states that "[i]t 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." The Use and Documentation section states that "[o]fficers may only use department-issued BWCs in the performance of official duties for this agency or when otherwise performing authorized law enforcement duties as an employee of this department."

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. The Use and Documentation section of NBPD's BWC policy includes language to address this new requirement:

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

NBPD's written BWC policy addresses consequences associated with violations of the policy, to include both disciplinary action and potential criminal penalties.

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

NBPD BWC Program and Inventory

NBPD currently possesses 14 Motorola V300 body-worn cameras.

The NBPD 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.

As discussed in Clause 3 of the Policy section of this report, the 2023 legislative changes require that an agency's BWC policy must specify that a BWC be worn at or above the mid-line of the waist. The LEO Responsibilities section of NBPD's BWC policy states: "BWCs 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."

Chief Meyer advised us that he is able to determine the number of BWCs deployed by reviewing the schedule and/or payroll data.

As of November 1, 2024, NBPD maintained 7,899 BWC videos, totaling approximately 9.06 TB.

NBPD BWC Physical, Technological and Procedural Safeguards

North Branch PD's BWC Policy states that: "No employee may have access to the department's BWC data except for legitimate law enforcement or data administration purposes."

NBPD BWC data are initially recorded to a hard drive in each officer's BWC. Data from each BWC are then uploaded to Motorola's CommandCentral cloud service via either wireless upload or a physical docking station located at the Police Department.

Officers have view-only access to their own data for report writing, trial preparation, data administration, investigatory purposes and other legitimate law enforcement purposes, as well as the ability to add or edit case numbers and titles. Supervisors have the ability to view videos created by other personnel; however, all BWC data access is logged automatically and available for audit purposes.

Enhanced Surveillance Technology

NBPD currently employs BWCs with only standard audio/video recording capabilities. NBPD 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.

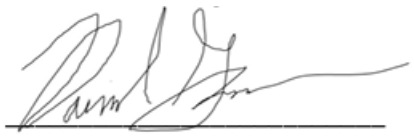
If NBPD should obtain such enhanced technology in the future, Minnesota Statute §13.825 Subd. 10 requires notice to the Minnesota Bureau of Criminal Apprehension within 10 days. This notice must include a description of the technology and its surveillance capability and intended uses.

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 NBPD records.

Audit Conclusions

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



Daniel E. Gazelka

Rampart Audit LLC

12/11/2024

APPENDIX A:

NORTH BRANCH POLICE DEPARTMENT

GENERAL ORDER: EFFECTIVE: SUBJECT:137.0

November 2021, Revised July 2023, Revised January 2024

USE OF PORTABLE RECORDING SYSTEMS (BODY-WORN CAMERAS) - MN STAT 626.8473

137.1 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.

137.2 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.

137.3 SCOPE

This policy governs the use of BWCs in the course of official duties. It does not apply to the use of squad-based (dash-cam) recording systems. The chief or chief's designee may supersede this policy by providing specific instructions for BWC use to individual officers, or providing specific instructions pertaining to particular events or classes of events, including but not limited to political rallies and demonstrations. The chief or designee may also provide

specific instructions or standard operating procedures for BWC use to officers assigned to specialized details, such as carrying out duties in courts or guarding prisoners or patients in hospitals and mental health facilities.

137.4 DEFINITIONS

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

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

B. **Records Retention Schedule** refers 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 inadvertance 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.

137.5 USE AND DOCUMENTATION

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

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

C. Officers shall conduct a function test of their issued BWCs at the beginning of each shift 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.

D. BWCs 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.

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

   a. Whenever an officer makes a recording, the existence of the recording shall be documented in an incident report or other official record of the contact.

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

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

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

b. A daily record of the total number of BWCs actually deployed and used by officers and, if applicable, the precincts in which they were used;

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

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

137.6 GENERAL GUIDELINES FOR RECORDING

A. Uniformed sworn 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 (above). Officers assigned to non-uniform positions may carry their BWC at any time the officer believes that the device would be useful.

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

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

D. Once activated, the BWC should continue recording until the conclusion of the incident or encounter, or until it becomes apparent that additional recording is unlikely to capture information having evidentiary value. The officer having charge of a scene shall likewise direct the discontinuance of recording when further recording is unlikely to capture additional information having evidentiary value. If the recording is discontinued while an investigation, response, or incident is ongoing, officers shall state the reasons for ceasing the recording on camera before deactivating their BWC. If circumstances change, officers shall reactivate their cameras as required by this policy to capture information having evidentiary value.

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

F. Notwithstanding any other provision in this policy, officers shall not use their BWCs to record other 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.

137.7 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.

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.

137.8 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 data storage by the end of that officer's shift. However, if the officer is involved in a shooting, in-custody death, or other law enforcement activity resulting in death or great bodily harm, a supervisor or investigator shall take

custody of the officer's BWC and assume responsibility for transferring the data from it.

B. Officers shall label the BWC data files with the proper event tag at the time of capture or transfer to storage, and should consult with a supervisor if in doubt as to the appropriate labeling. Event tags will determine how the video is classified (if the video contains evidence or non-evidence) and will determine how long the videos are kept per the City's evidence retention schedule. Officers shall also label each video with the pertinent call/case number.

C. In addition, officers may 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:

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

b. Victims of child abuse or neglect.

c. Vulnerable adults who are victims of maltreatment.

d. Undercover officers.

e. Informants.

f. When the video is clearly offensive to common sensitivities.

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

h. Individuals who ca11ed 911, and services subscribers whose lines were used to place a call to the 911 system.

1. Mandated reporters.

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

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

l. Individuals who make complaints about violations with respect to the use of real property.

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

n. Other individuals whose identities the officer believes may be

legally protected from public disclosure.

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

137.9 ADMINISTERING ACCESS TO BWC DATA:

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

1. The deceased individual's next of kin.

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

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

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

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

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

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

b. The officer who collected the data.

c. Any other officer whose voice or image is documented in the

data, regardless of whether that officer is or can be identified by the recording.

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

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

b. Some BWC data is classified as confidential (see E. below).

c. Some BWC data is classified as public (see F. below).

E. Confidential data. Confidential data. BWC data that is collected or created as part of an active criminal investigation is confidential. This classification takes precedence over the "private" classification listed above in part D, and the "public" classifications listed below in parts F(2)(a) and (b). However, special classifications and access rights are applicable to BWC data documenting incidents where an officer's use of force results in death (see parts A and B, above).

F. Public data. The following BWC data is public:

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

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

1. Data that record, describe, or otherwise document actions and circumstances surrounding the use of force by a peace officer that results in substantial bodily harm, or the discharge of a firearm by a peace officer in the course of duty other than for training or the killing of an animal that is sick, injured, or dangerous.

11. Data that a data subject requests to be made accessible to the public, subject to redaction. Data on any data subject (other than a peace officer) who has not consented to the

public release must be redacted, if practicable. In addition, any data on undercover officers must be redacted.

G. **Access to BWC data by non-employees.** Officers shall refer members of the media or public seeking access to BWC data to the police department's administrative staff who shall process the request in accordance with the MGDPA and other governing laws. In particular:

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

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

11. 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.

b. 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:

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

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

m. Data on other officers who are not undercover, and who are on duty and engaged in the performance of official duties, may not be redacted.

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

a. 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.

b. 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.

c. 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.

l. **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 individual identities that are not public. Protecting against incidental disclosure could involve, for instance, showing only a portion of the video, showing only screen shots, muting the audio, or playing the audio but not displaying video. In addition,

a. 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.

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

137.10 DATA SECURITY SAFEGUARDS

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

B. Officers and department staff shall not intentionally edit, alter, or erase/des any BWC recording prior to expiration of the applicable retention period. - full, unedited, and unredacted recording of a peace officer using deadly force must be maintained indefinitely.

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.

137.11 AGENCY USE OF DATA

A. At least once a month, supervisors will randomly review BWC usage by each officer to whom a BWC is issued or available for use, to ensure compliance with this policy.

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.

137.12 DATA RETENTION

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

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

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

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

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

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

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

employee who is the subject of the investigation

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

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

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

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

J. The department will post this policy, together with a link to the City's Records Retention Schedule, on its website.

137.13 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.

APPENDIX B:

NORTH BRANCH POLICE DEPARTMENT

GENERAL ORDER:	137.0
EFFECTIVE:	November 2021, Revised July 2023, Revised January 2024, Revised December 2024
SUBJECT:	**USE OF PORTABLE RECORDING SYSTEMS (BODY-WORN CAMERAS)** - MN STAT 626.8473

137.1 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.

137.2 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.

137.3 SCOPE

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

137.4 DEFINITIONS

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

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

B. **Records Retention Schedule** refers 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.

137.5 USE AND DOCUMENTATION

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

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

C. Officers shall conduct a function test of their issued BWCs at the beginning of each shift 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.

D. BWCs 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.

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

   a. Whenever an officer makes a recording, the existence of the recording shall be documented in an incident report or other official record of the contact.

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

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

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

b. A daily record of the total number of BWCs actually deployed and used by officers and, if applicable, the precincts in which they were used;

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

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

137.6 GENERAL GUIDELINES FOR RECORDING

A. Uniformed sworn 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 (above). Officers assigned to non-uniform positions may carry their BWC at any time the officer believes that the device would be useful.

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

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

D. Once activated, the BWC should continue recording until the conclusion of the incident or encounter, or until it becomes apparent that additional recording is unlikely to capture information having evidentiary value. The officer having charge of a scene shall likewise direct the discontinuance of recording when further recording is unlikely to capture additional information having evidentiary value. If the recording is discontinued while an investigation, response, or incident is ongoing, officers shall state the reasons for ceasing the recording on camera before deactivating their BWC. If circumstances change, officers shall reactivate their cameras as required by this policy to capture information having evidentiary value.

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

F. Notwithstanding any other provision in this policy, officers shall not use their BWCs to record other 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.

137.7 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.

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.

137.8 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 data storage by the end of that officer's shift. However, if the officer is involved in a shooting, in-custody death, or other law enforcement activity resulting in death or great bodily harm, a supervisor or investigator shall take custody of the officer's BWC and assume responsibility for transferring the data from it.

B. Officers shall label the BWC data files with the proper event tag at the time of capture or transfer to storage, and should consult with a supervisor if in doubt as to the appropriate labeling. Event tags will determine how the video is classified (if the video contains evidence or non-evidence) and will determine how long the videos are kept per the City's evidence retention schedule. Officers shall also label each video with the pertinent call/case number.

C. In addition, officers may 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:

   a. Victims and alleged victims of criminal sexual conduct and sex trafficking.
   b. Victims of child abuse or neglect.
   c. Vulnerable adults who are victims of maltreatment.
   d. Undercover officers.
   e. Informants.
   f. When the video is clearly offensive to common sensitivities.
   g. Victims of and witnesses to crimes, if the victim or witness has requested not to be identified publicly.
   h. Individuals who called 911, and services subscribers whose lines were used to place a call to the 911 system.
   i. Mandated reporters.
   j. Juvenile witnesses, if the nature of the event or activity justifies protecting the identity of the witness.
   k. Juveniles who are or may be delinquent or engaged in criminal acts.
   l. Individuals who make complaints about violations with respect to the use of real property.
   m. Officers and employees who are the subject of a complaint related to the events captured on video.
   n. Other individuals whose identities the officer believes may be legally protected from public disclosure.

D. Labeling and flagging designations may be corrected or amended

based on additional information.

137.9 ADMINISTERING ACCESS TO BWC DATA:

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

1. The deceased individual's next of kin.

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

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

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

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

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

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

b. The officer who collected the data.

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

by the recording.

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

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

   b. Some BWC data is classified as confidential (see E. below).

   c. Some BWC data is classified as public (see F. below).

E. **Confidential data.** Confidential data. BWC data that is collected or created as part of an active criminal investigation is confidential. This classification takes precedence over the "private" classification listed above in part D, and the "public" classifications listed below in parts F(2)(a) and (b). However, special classifications and access rights are applicable to BWC data documenting incidents where an officer's use of force results in death (see parts A and B, above).

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

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

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

      i. Data that record, describe, or otherwise document actions and circumstances surrounding the use of force by a peace officer that results in substantial bodily harm, or the discharge of a firearm by a peace officer in the course of duty other than for training or the killing of an animal that is sick, injured, or dangerous.

      ii. Data that a data subject requests to be made accessible to the public, subject to redaction. Data on any data subject (other than a peace officer) who has not consented to the public release must be redacted, if

practicable. In addition, any data on undercover officers must be redacted.

G. **Access to BWC data by non-employees.** Officers shall refer members of the media or public seeking access to BWC data to the police department's administrative staff who shall process the request in accordance with the MGDPA and other governing laws. In particular:

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

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

      ii. 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.

   b. 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:

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

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

      iii. Data on other officers who are not undercover, and who are on duty and engaged in the performance of official duties, may not be redacted.

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

   a. 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.

b. 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.

c. 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.

l. **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 individual identities that are not public. Protecting against incidental disclosure could involve, for instance, showing only a portion of the video, showing only screen shots, muting the audio, or playing the audio but not displaying video. In addition,

a. 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. Any law enforcement agency who requests BWC data must complete and sign a BWC Agency Sharing Data Form. Law enforcement agencies that receive the data must comply with all data classification, destruction, and security requirements of Minn. Stat. § 13.825.

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

c. Portable recording system data may not be shared with, disseminated to, sold to, or traded with any other individual or entity unless explicitly authorized by this section or other applicable law.

137.10 DATA SECURITY SAFEGUARDS

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

B. Officers and department staff shall not intentionally edit, alter, or erase/destroy any data, metadata, or BWC recording prior to expiration of the applicable retention period. The full, unedited, and unredacted recording of a peace officer using deadly force must be maintained indefinitely.

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.

137.11 AGENCY USE OF DATA

A. At least once a month, supervisors will randomly review BWC usage by each officer to whom a BWC is issued or available for use, to ensure compliance with this policy.

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.

137.12 DATA RETENTION

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

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

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

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

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

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

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

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

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

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

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

J. The department will post this policy, together with a link to the City's Records Retention Schedule, on its website.

137.13 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.