



INDEPENDENT AUDITOR'S REPORT

Bagley Police Department



JUNE 23RD, 2025
RAMPART AUDIT LLC

Audit Overview and Recommendations

Dear Bagley City Council and Chief Gunderson:

We have audited the body-worn camera (BWC) program of the Bagley Police Department (BPD) for the two-year period ended 1/31/2025. Minnesota Statute §13.825 mandates that any law enforcement agency operating a portable recording system (PRS)¹ program obtain an independent, biennial audit of its program. This program and its associated data are the responsibility of the Bagley Police Department. Our responsibility is to express an opinion on the operations of this program based on our audit.

On March 27, 2025, Rampart Audit LLC (Rampart) met with Chief Adam Gunderson, who provided information about BPD'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 BPD's recordkeeping.

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

BPD 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.

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.

Chief Gunderson advised us that Bagley Police Department's BWC program was already in operation when he joined the agency in January of 2023. At that time, he was unable to locate an agency-specific body-worn camera policy in BPD's records, though he indicated he found copies of policies from other Minnesota law enforcement agencies that may have been intended as examples to aid in creating a

¹ It should be noted that Minnesota statute uses the broader term "portable recording system" (PRS), which includes body-worn cameras. Because body-worn cameras are the only type of portable recording system employed by BPD, these terms may be used interchangeably in this report.

policy for BPD. To ensure compliance with the requirements of §626.8473 Subd. 3(a), BPD then adopted the Minnesota POST Board's model BWC policy.

Chief Gunderson also advised us that while he has been advised that BPD met the public comment and hearing requirements described above, he has been unable to locate documentation to confirm that these requirements were met.

Rampart Audit staff are familiar with Bagley Police Department, and are aware that its BWC program has been operational since at least 2014, thus predating the public hearing and public comment requirements discussed above; however, because the statute does not address those programs that were already in existence at the time of its adoption, Rampart recommends that agencies with pre-existing BWC programs hold an after-the-fact public hearing to ensure compliance with the requirements discussed above.

Prior to the completion of this report, Chief Gunderson submitted documentation showing that a public notice was posted and comments were solicited for an after-the-fact public hearing, which was held on May 28, 2025. Chief Gunderson submitted the following:

1. A copy of a public notice posted in the City of Bagley office, announcing the hearing and providing information about submitting comments in writing either electronically or through the mail, as well as in person at a public hearing.
2. A copy of the May 28, 2025, Bagley City Council meeting minutes, which show that a public hearing was held for the purpose of receiving public comments related to its BWC program.

Finally, §626.8473 Subd. 3(a) 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 BPD's BWC policy on the City of Bagley website. In our opinion, Bagley Police Department is compliant with the requirements of §626.8473 Subd. 3(a).

BPD BWC WRITTEN POLICY

As part of this audit, we reviewed BPD's BWC policy, a copy of which is attached to this report as Appendix A.

Minnesota Statute §626.8473 Subd. 3(b) requires a written BWC policy to incorporate the following, at a minimum:

1. The requirements of section 13.825 and other data classifications, access procedures, retention policies, and data safeguards that, at a minimum, meet the requirements of chapter 13 and other applicable law;
2. A prohibition on altering, erasing or destroying any recording made with a peace officer's portable recording system or data and metadata related to the recording prior the expiration of the applicable retention period under section 13.825 Subdivision 3, except that the full, unedited, and unredacted recording of a peace officer using deadly force must be maintained indefinitely;

3. A mandate that a portable recording system be worn at or above the mid-line of the waist in a position that maximizes the recording system's capacity to record video footage of the officer's activities;
4. A mandate that officers assigned a portable recording system wear and operate the system in compliance with the agency's policy adopted under this section while performing law enforcement activities under the command and control of another chief law enforcement officer or federal law enforcement official;
5. A mandate that, notwithstanding any law to the contrary, when an individual dies as a result of a use of force by a peace officer, an involved officer's law enforcement agency must allow the deceased individual's next of kin, the legal representative of the deceased individual's next of kin, and the other parent of the deceased individual's child, upon their request, to inspect all portable recording system data, redacted no more than what is required by law, documenting the incident within five days of the request, with the following exception:
 - A law enforcement agency may deny a request if the agency determines that there is a compelling reason that inspection would interfere with an active investigation. If the agency denies access, the chief law enforcement officer must provide a prompt, written denial to the individual who requested the data with a short description of the compelling reason access was denied and must provide notice that relief may be sought from the district court pursuant to section 13.82 subdivision 7;
6. A mandate that, when an individual dies as a result of a use of force by a peace officer, an involved officer's law enforcement agency shall release all portable recording system data, redacted no more than required by law, documenting the incident no later than 14 days after the incident, unless the chief law enforcement officer asserts in writing that the public classification would interfere with an ongoing investigation, in which case the data remain classified by section 13.82 subdivision 7;
7. Procedures for testing the portable recording system to ensure adequate functioning;
8. Procedures to address a system malfunction or failure, including requirements for documentation by the officer using the system at the time of a malfunction or failure;
9. Circumstances where recording is mandatory, prohibited, or at the discretion of the officer using the system;
10. Circumstances under which a data subject must be given notice of a recording;
11. Circumstances under which a recording may be ended while an investigation, response, or incident is ongoing;
12. Procedures for the secure storage of portable recording system data and the creation of backup copies of the data; and
13. Procedures to ensure compliance and address violations of the policy, which must include, at a minimum, supervisory or internal audits and reviews, and the employee discipline standards for unauthorized access to data contained in section 13.09.

In our opinion, the BPD 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.

BPD 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.

The Data Retention section of BPD's BWC policy states that "[a]ll BWC data shall be maintained for a minimum period of 90 days. There are no exceptions for erroneously recorded or non-evidentiary data," which satisfies the requirements of §13.825 Subd. 3(a). This section of BPD's BWC policy also specifies a retention period of one year for data documenting reportable firearms discharges and six years for data documenting the use of deadly force, or force "of a sufficient type or degree to require a use of force report or supervisory review." This section of the policy also specifies a retention period of six years for "data documenting circumstances that have given rise to a formal complaint against an officer."

BPD's BWC policy meets or exceeds the retention requirements for the data categories enumerated in §13.825 Subd. 3(b), but specifies a retention period of six years for data documenting an officer's use of deadly force, while §13.825 Subd. 3(c) requires that such data be maintained indefinitely.

BPD's policy addresses the §13.825 Subd. 3(d) requirement, and notes that such additional retention is mandatory.

Prior to the issuance of this report, BPD submitted a revised BWC policy that includes the indefinite retention period for data documenting an officer's use of deadly force as required in Subdivision 3(c). The revised policy is attached to this report as Appendix B. In our opinion, this revised policy meets the retention requirements contained in Minn. Stat. §13.825 Subd. 3.

The Data Security Safeguards section of BPD's BWC policy states: "Officers shall not intentionally edit, alter, or erase any BWC recording unless otherwise expressly authorized by the chief or the chief's designee." As discussed in Clause 2 of the Policy section of this report, Minn. Stat. §626.8473 Subd. 3(b)(1) states that a BWC policy "must prohibit altering, erasing, or destroying any recording made with an officer's portable recording system or data and metadata related to the recording prior to the expiration of the applicable retention period under section 13.825 subdivision 3..."

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

BPD employs Axon body-worn cameras. BPD's BWC policy requires that each officer transfer data from his or her body-worn camera by the end of each shift, and also requires that the officer assign the appropriate label or labels to each file to identify the nature of the data. Chief Gunderson advised us that officers work a seven-on, seven-off schedule and, in practice, commonly download their BWC recordings at the end of their weekly rotation. In addition, while BPD uses the Axon Evidence Sync

program to download recordings from their BWCs, BPD does not employ video management software that would enable the attachment of labels or tags. Instead, officers may add a call or case number to the Axon-generated title given to each recording as a means of further identifying it.

Chief Gunderson advised us that BWC data retention is currently a manual process, with all recordings retained indefinitely to avoid the accidental loss of data. In addition, any BWC recordings documenting incidents referred for prosecution are copied to DVD and submitted to the Clearwater County Attorney's Office.

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

BPD BWC Data Destruction

Due to budgetary constraints, BPD's BWC data are retained on portable hard drives rather than utilizing a server-based system or cloud storage. Recordings are sorted by officer, month and year. When a hard drive becomes full, it is placed in secure storage until Chief Gunderson can be certain that all retention periods have expired. (It should be noted that as of the date of the audit, BPD has not experienced a deadly-force incident and therefore has no videos requiring indefinite retention.) Once all of the retention periods have expired, the hard drive can either be erased and reused by BPD, or else physically destroyed at the firearms range.

This is consistent with FBI CJIS policy, which 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, BPD's BWC policy is compliant with respect to the applicable data destruction requirements.

BPD BWC Data Access

Any request for access to BWC data by a data subject or member of the media would be made in writing using the Bagley Police Department's Data Request Form, which is available on the city website and can be submitted via email to Chief Gunderson. If approved, Chief Gunderson would then fulfill the request using a USB memory device provided by the requesting party.

BPD notes 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." Chief Gunderson advised that all requests from other agencies are directed to him and that verbal requests are acceptable in practice. Existing verbal agreements between BPD and other area law enforcement agencies address data classification, destruction and security requirements, as specified in §13.825 Subd. 8(b). Access to BPD BWC data for outside agencies is normally provided either via optical disc, or a USB memory device supplied by the receiving agency.

Prosecutors contact Chief Gunderson directly when requesting BWC data.

We recommend that BPD enforce the policy requirement that all requests from outside agencies be submitted in writing. We also recommend that BPD obtain a written acknowledgement from each requesting agency that any BWC data obtained from BPD will be managed by the requesting agency in accordance with the requirements of §13.825 Subd. 7 and 8. A copy of this written acknowledgment should be maintained on file.

Prior to the issuance of this report, BPD submitted a revised BWC policy that addresses these recommendations.

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, BPD had not addressed these new requirements. Prior to the issuance of this report, BPD submitted a revised BWC policy that added language to meet these requirements.

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

BPD BWC Data Classification

The Administering Access to BWC Data section of BPD's BWC policy identifies BWC data as presumptively private and notes that "BWC recordings are classified as private data about the data subjects unless there is a specific law that provides differently." The policy notes that "BWC data pertaining to businesses to businesses and other entities" is also presumptively private. The policy also identifies types of data that are classified as either public or confidential. As discussed in the preceding section of this report, however, at the time of our audit BPD had not addressed the 2023 legislative changes, which established new requirements regarding BWC data that document an officer's use of deadly force.

Prior to the issuance of this report, BPD submitted a revised BWC policy that added language to meet these requirements.

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

BPD BWC Internal Compliance Verification

The Agency Use of Data section of the BPD BWC policy states that "[a]t least once a month, supervisors will randomly review BWC usage by each officer to ensure compliance with this policy and to identify any performance areas in which additional training or guidance is required."

Chief Gunderson advised us that he reviews two recordings for each officer per month. Because BWC recordings are viewed with a Microsoft Windows application that does not log access, we recommend creating a manual log to document video reviews.

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.

BPD's BWC policy does not address the requirements discussed in the preceding paragraph. Prior to the issuance of this report, BPD submitted a revised BWC policy that addressed this requirement.

In our opinion, this revised policy language satisfies the requirements of Clause 4.

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

In our opinion, BPD's BWC policy is compliant with respect to the compliance and disciplinary requirements contained in §626.8473 Subd. 3(b)(12).

BPD BWC Program and Inventory

BPD currently possesses five (5) Axon body-worn cameras, four of which are in regular use.

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

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

As of the date of the audit, BPD maintained 2.1 TB of BWC data.

BPD BWC Physical, Technological and Procedural Safeguards

BPD BWC data are initially recorded to an internal hard drive in each officer's BWC. Those files are then transferred to a portable hard drive located at the Bagley Police Department utilizing a wired connection. The portable hard drive is stored in a locked room inside the Police Department.

While the Data Security Safeguards section of BPD's BWC policy states that the hard drive storing BWC data "will have [a] mirrored drive to prevent any data loss," Chief Gunderson indicated that this is not currently being done. Chief Gunderson noted that BPD does have an additional hard drive, so Rampart recommended that he conduct periodic backups of the active hard drive to reduce the risk of data loss. Rampart also recommended that BPD identify a secure off-site storage location for the backup drive to reduce the risk of loss due to physical hazards such as fire, flood or wind events.

Officers have full access to all BWC data on the portable hard drive for report writing, trial preparation, data administration, investigatory purposes and other legitimate law enforcement purposes. As a small agency with limited financial resources, Bagley Police Department has limited options to impose stronger safeguards without denying officers timely access to BWC data necessary for the day-to-day performance of their duties. Nevertheless, we recommend BPD explore the feasibility of cloud-based storage or video management software that would enable the implementation of access controls and activity logging.

The Use and Documentation section of BPD's BWC policy states that: "Officers may only use 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."

As noted above, requests by other law enforcement agencies for BPD BWC data must be approved by Chief Gunderson and are fulfilled via optical disc or USB drive. A similar method is employed to submit BPD BWC data to the Clearwater County Attorney's Office.

The Member Responsibilities section of BPD's BWC policy states: "Officers should wear their issued BWCs at the location on their body and in the manner specified in training." 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. Prior to the issuance of this report, BPD submitted a revised BWC policy that addresses this requirement. In our opinion, the revised BWC policy satisfies this requirement.

Enhanced Surveillance Technology

BPD currently employs BWCs with only standard audio/video recording capabilities. They have no plans at this time to add enhanced BWC surveillance capabilities, such as thermal or night vision, or to otherwise expand the type or scope of their BWC technology.

If BPD 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.

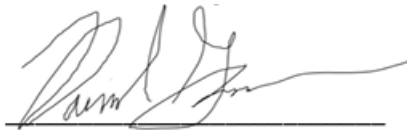
Data Sampling

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 ICRs for which BWC data was created, but which has since been deleted due to the expiration of the retention period.

Our review indicated inconsistent BWC usage and labeling practices, which Chief Gunderson advised he would address through training.

Audit Conclusions

In our opinion, the Bagley Police Department's Body-Worn Camera Program and revised BWC policy are substantially compliant with Minnesota Statutes §13.825 and §626.8473.

A handwritten signature in black ink, appearing to read "Rampart Audit", is written over a horizontal line.

Rampart Audit LLC

6/23/2025

APPENDIX A:

BAGLEY POLICE DEPARTMENT BODY WORN CAMERA POLICY

Policy: 19

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

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.

The purpose of this separate policy is to accommodate legislative mandates that were not present when the previous MVR policy (Section 18.00) encompassed all mobile video recording systems.

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.

Definitions

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

- A. **MGDPA or Data Practices Act** refers to the Minnesota Government Data Practices Act, Minn. Stat. § 13.01, et seq.
- B. **Records Retention Schedule** refers to the General Records Retention Schedule for Minnesota Cities.
- C. **Law enforcement-related information** means information captured or available for capture by use of a BWC that has evidentiary value because it documents events with respect to a stop, arrest, search, citation, or charging decision.
- D. **Evidentiary value** means that the information may be useful as proof in a criminal prosecution, related civil or administrative proceeding, further investigation of an actual or suspected criminal act, or in considering an allegation against a law enforcement agency or officer.
- E. **General citizen contact** means an informal encounter with a citizen that is not and does not become law enforcement-related or adversarial, and a recording of the event would not yield information relevant to an ongoing investigation. Examples include, but are not limited to, assisting a motorist with directions, summoning a wrecker, or receiving generalized concerns from a citizen about crime trends in his or her neighborhood.
- F. **Adversarial** means a law enforcement encounter with a person that becomes confrontational, during which at least one person expresses anger, resentment, or hostility toward the other, or at least one person directs toward the other verbal conduct consisting of arguing, threatening, challenging, swearing, yelling, or shouting. Encounters in which a citizen demands to be recorded or initiates recording on his or her own are deemed adversarial.
- G. **Unintentionally recorded footage** is a video recording that results from an officer's inadvertence or neglect in operating the officer's BWC, provided that no portion of the resulting recording has evidentiary value. Examples of unintentionally recorded footage include, but are not limited to, recordings made in station house locker rooms, restrooms, and recordings made while officers were engaged in conversations of a non-business, personal nature with the expectation that the conversation was not being recorded.
- H. **Official duties**, for purposes of this policy, means that the officer is on duty and performing authorized law enforcement services on behalf of this agency.

Use and Documentation

- A. Officers may use only department-issued BWCs in the performance of official duties for this agency or when otherwise performing authorized law enforcement services as an employee of this department.
- B. Officers who have been issued BWCs shall operate and use them consistent with this policy. Officers shall conduct a function test of their issued BWCs at the beginning of each shift to make sure the devices are operating properly. Officers noting a malfunction during testing or at any other time shall promptly report the malfunction to the officer's supervisor and shall document the report in writing. Supervisors shall take prompt action to address malfunctions and document the steps taken in writing.
- C. Officers should wear their issued BWCs at the location on their body and in the manner specified in training.
- D. Officers must document BWC use and non-use as follows:
 - 1. Whenever an officer makes a recording, the existence of the recording shall be documented in an incident report or on the CFS if no report is written.
 - 2. Whenever an officer fails to record an activity that is required to be recorded under this policy or captures only a part of the activity, the officer must document the circumstances and reasons for not recording in an incident report or on the CFS if no report is written. Supervisors shall review these reports and initiate any corrective action deemed necessary.
- E. The Bagley Police Department will maintain the following records and documents relating to BWC use, which are classified as public data:
 - 1. The total number of BWCs owned or maintained by the agency;
 - 2. A daily record of the total number of BWCs actually deployed and used by officers and, if applicable, the precincts in which they were used;
 - 3. The total amount of recorded BWC data collected and maintained; and
 - 4. This policy, together with the Records Retention Schedule.

General Guidelines for Recording

- A. Officers shall activate their BWCs when anticipating that they will be involved in, become involved in, or witness other officers of this agency involved in a pursuit, *Terry* stop of a motorist or pedestrian, search, seizure, arrest, use of force, adversarial contact, and during other activities

likely to yield information having evidentiary value. However, officers need not activate their cameras when it would be unsafe, impossible, or impractical to do so, but such instances of not recording when otherwise required must be documented as specified in the Use and Documentation guidelines, part (D)(2) (above).

- B. Officers have discretion to record or not record general citizen contacts.
- C. Officers have no affirmative duty to inform people that a BWC is being operated or that the individuals are being recorded.
- D. Once activated, the BWC should continue recording until the conclusion of the incident or encounter, or until it becomes apparent that additional recording is unlikely to capture information having evidentiary value. The officer having charge of a scene shall likewise direct the discontinuance of recording when further recording is unlikely to capture additional information having evidentiary value. If 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.

Special Guidelines for Recording

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

- A. To use their BWCs to record any police-citizen encounter if there is reason to believe the recording would potentially yield information having evidentiary value, unless such recording is otherwise expressly prohibited.
- B. To use their BWCs to take recorded statements from persons believed to be victims of and witnesses to crimes, and persons suspected of committing crimes, considering the needs of the investigation and the circumstances pertaining to the victim, witness, or suspect.

In addition,

- C. Officers need not record persons being provided medical care unless there is reason to believe the recording would document information having evidentiary value. When responding to an apparent mental health crisis or event, BWCs shall be activated as necessary to document any use of force and the basis for it, and any other information having evidentiary value, but need not be activated when doing so would serve only to record symptoms or behaviors believed to be attributable to the mental health issue.
- D. Officers should use their BWCs and squad-based audio/video systems to record their transportation and the physical transfer of persons in their custody to hospitals, detox and mental health care facilities, juvenile detention centers, and jails, but otherwise should not record in these facilities unless the officer anticipates witnessing a criminal event or being involved in or witnessing an adversarial encounter or use-of-force incident.

Downloading and Labeling Data

- A. Each officer using a BWC is responsible for transferring or assuring the proper transfer of the data from his or her camera to that officer's folder located on the digital evidence computer by the end of that officer's shift. However, if the officer is involved in a shooting, in-custody death, or other law enforcement activity resulting in death or great bodily harm, a supervisor or investigator shall take custody of the officer's BWC and assume responsibility for transferring the data from it.
- B. Officers shall label the BWC data files at the time of transfer to storage, and should consult with a supervisor if in doubt as to the appropriate labeling. Officers should assign as many of the following labels as are applicable to each file:
 - 1. **Evidence—criminal:** The information has evidentiary value with respect to an actual or suspected criminal incident or charging decision.
 - 2. **Evidence—force:** Whether or not enforcement action was taken or an arrest resulted, the event involved the application of force by a law enforcement officer of this or another agency.
 - 3. **Evidence—property:** Whether or not enforcement action was taken or an arrest resulted, an officer seized property from an individual or directed an individual to dispossess property.

4. **Evidence—administrative:** The incident involved an adversarial encounter or resulted in a complaint against the officer.
 5. **Evidence—other:** The recording has potential evidentiary value for reasons identified by the officer at the time of labeling.
 6. **Training:** The event was such that it may have value for training.
 7. **Not evidence:** The recording does not contain any of the foregoing categories of information and has no apparent evidentiary value. Recordings of general citizen contacts and unintentionally recorded footage are not evidence.
- C. In addition, officers shall flag each file as appropriate to indicate that it contains information about data subjects who may have rights under the MGDPA limiting disclosure of information about them. These individuals include:
1. Victims and alleged victims of criminal sexual conduct and sex trafficking.
 2. Victims of child abuse or neglect.
 3. Vulnerable adults who are victims of maltreatment.
 4. Undercover officers.
 5. Informants.
 6. When the video is clearly offensive to common sensitivities.
 7. Victims of and witnesses to crimes, if the victim or witness has requested not to be identified publicly.
 8. Individuals who called 911, and services subscribers whose lines were used to place a call to the 911 system.
 9. Mandated reporters.
 10. Juvenile witnesses, if the nature of the event or activity justifies protecting the identity of the witness.

11. Juveniles who are or may be delinquent or engaged in criminal acts.
12. Individuals who make complaints about violations with respect to the use of real property.
13. Officers and employees who are the subject of a complaint related to the events captured on video.
14. Other individuals whose identities the officer believes may be legally protected from public disclosure.

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

Administering Access to BWC Data:

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

1. Any person or entity whose image or voice is documented in the data.
2. The officer who collected the data.
3. Any other officer whose voice or image is documented in the data, regardless of whether that officer is or can be identified by the recording.

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

1. BWC data pertaining to people is presumed private, as is BWC data pertaining to businesses or other entities.
2. Some BWC data is classified as confidential (see C. below).
3. Some BWC data is classified as public (see D. below).

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

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

1. Data documenting the discharge of a firearm by a peace officer in the course of duty, other than for training or the killing of an animal that is sick, injured, or dangerous.
2. Data that documents the use of force by a peace officer that results in substantial bodily harm.
3. Data that a data subject requests to be made accessible to the public, subject to redaction. Data on any data subject (other than a peace officer) who has not consented to the public release must be redacted [*if practicable*]. In addition, any data on undercover officers must be redacted.
4. Data that documents the final disposition of a disciplinary action against a public employee.

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

E. **Access to BWC data by non-employees.** Officers shall refer members of the media or public seeking access to BWC data to Chief of Police/Administrative Assistant who shall process the request in accordance with the MGDPA and other governing laws. In particular:

1. An individual shall be allowed to review recorded BWC data about him- or herself and other data subjects in the recording, but access shall not be granted:
 - a. If the data was collected or created as part of an active investigation.
 - b. To portions of the data that the agency would otherwise be prohibited by law from disclosing to the person seeking access, such as portions that would reveal identities protected by Minn. Stat. § 13.82, subd. 17.
2. Unless the data is part of an active investigation, an individual data subject shall be provided with a copy of the recording upon request, but subject to the following guidelines on redaction:
 - a. Data on other individuals in the recording who do not consent to the release must be redacted.
 - b. Data that would identify undercover officers must be redacted.
 - c. Data on other officers who are not undercover, and who are on duty and engaged in the performance of official duties, may not be redacted.

- F. **Access by peace officers and law enforcement employees.** No employee may have access to the Bagley Police Department's BWC data except for legitimate law enforcement or data administration purposes:
1. Officers may access and view stored BWC video only when there is a business need for doing so, including the need to defend against an allegation of misconduct or substandard performance. Except as provided in the critical incident response policy, officers may review video footage of an incident in which they were involved prior to preparing a report, giving a statement, or providing testimony about the incident.
 2. Agency personnel shall document their reasons for accessing stored BWC data within incident reports/supplements to the case file relate to the video, at the time of each access. Agency personnel are prohibited from accessing BWC data for non-business reasons and from sharing the data for non-law enforcement related purposes, including but not limited to uploading BWC data recorded or maintained by this agency to public and social media websites.
 3. Employees seeking access to BWC data for non-business reasons may make a request for it in the same manner as any member of the public.
- G. **Other authorized disclosures of data.** Officers may display portions of BWC footage to witnesses as necessary for purposes of investigation as allowed by Minn. Stat. § 13.82, subd. 15, as may be amended from time to time. Officers should generally limit these displays in order to protect against the incidental disclosure of individuals whose identities are not public. Protecting against incidental disclosure could involve, for instance, showing only a portion of the video, showing only screen shots, muting the audio, or playing the audio but not displaying video. In addition,
1. BWC data may be shared with other law enforcement agencies only for legitimate law enforcement purposes that are documented in writing at the time of the disclosure.
 2. BWC data shall be made available to prosecutors, courts, and other criminal justice entities as provided by law.

Data Security Safeguards

- A. All BWC files recorded will be only downloaded onto the Bagley Police Departments Digital Evidence computer. This computer will not be connected to any network and will have mirrored drive to prevent any data loss.
- B. Personally owned devices, including but not limited to computers and mobile devices, shall not be programmed or used to access or view agency BWC data.

- C. Officers shall not intentionally edit, alter, or erase any BWC recording unless otherwise expressly authorized by the chief or the chief's designee.
- D. As required by Minn. Stat. § 13.825, subd. 9, as may be amended from time to time, this agency shall obtain an independent biennial audit of its BWC program.

Agency Use of Data

- A. At least once a month, supervisors will randomly review BWC usage by each officer to ensure compliance with this policy and to identify any performance areas in which additional training or guidance is required.
- B. In addition, supervisors and other assigned personnel may access BWC data for the purposes of reviewing or investigating a specific incident that has given rise to a complaint or concern about officer misconduct or performance.
- C. Nothing in this policy limits or prohibits the use of BWC data as evidence of misconduct or as a basis for discipline.
- D. Officers should contact their supervisors to discuss retaining and using BWC footage for training purposes. Officer objections to preserving or using certain footage for training will be considered on a case-by-case basis. Field training officers may utilize BWC data with trainees for the purpose of providing coaching and feedback on the trainees' performance.

Data Retention

- A. All BWC data shall be retained for a minimum period of 90 days. There are no exceptions for erroneously recorded or non-evidentiary data.
- B. Data documenting the discharge of a firearm by a peace officer in the course of duty, other than for training or the killing of an animal that is sick, injured, or dangerous, must be maintained for a minimum period of one year.
- C. Certain kinds of BWC data must be retained for six years:
 - 1. Data that documents the use of deadly force by a peace officer, or force of a sufficient type or degree to require a use of force report or supervisory review.
 - 2. Data documenting circumstances that have given rise to a formal complaint against an officer.

- D. Other data having evidentiary value shall be retained for the period specified in the Records Retention Schedule. When a particular recording is subject to multiple retention periods, it shall be maintained for the longest applicable period.
- E. Subject to Part F (below), all other BWC footage that is classified as non-evidentiary, becomes classified as non-evidentiary, or is not maintained for training shall be destroyed after 90 days.
- F. Upon written request by a BWC data subject, the agency shall retain a recording pertaining to that subject for an additional time period requested by the subject of up to 180 days. The agency will notify the requestor at the time of the request that the data will then be destroyed unless a new written request is received.
- G. The Bagley Police Department shall maintain an inventory of BWC recordings having evidentiary value.
- H. The Bagley Police Department will post this policy, together with its Records Retention Schedule, on its website.

Compliance

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

APPENDIX B:

BAGLEY POLICE DEPARTMENT BODY WORN CAMERA POLICY

Policy: 19

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

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.

The purpose of this separate policy is to accommodate legislative mandates that were not present when the previous MVR policy (Section 18.00) encompassed all mobile video recording systems.

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.

Definitions

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

- I. **MGDPA or Data Practices Act** refers to the Minnesota Government Data Practices Act, Minn. Stat. § 13.01, et seq.
- J. **Records Retention Schedule** refers to the General Records Retention Schedule for Minnesota Cities.
- K. **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.
- L. **Evidentiary value** means that the information may be useful as proof in a criminal prosecution, related civil or administrative proceeding, further investigation of an actual or suspected criminal act, or in considering an allegation against a law enforcement agency or officer.
- M. **General citizen contact** means an informal encounter with a citizen that is not and does not become law enforcement-related or adversarial, and a recording of the event would not yield information relevant to an ongoing investigation. Examples include, but are not limited to, assisting a motorist with directions, summoning a wrecker, or receiving generalized concerns from a citizen about crime trends in his or her neighborhood.
- N. **Adversarial** 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.
- O. **Unintentionally recorded footage** is a video recording that results from an officer's inadvertence or neglect in operating the officer's BWC, provided that no portion of the resulting recording has evidentiary value. Examples of unintentionally recorded footage include, but are not limited to, recordings made in station house locker rooms, restrooms, and recordings made while officers were engaged in conversations of a non-business, personal nature with the expectation that the conversation was not being recorded.
- P. **Official duties**, for purposes of this policy, means that the officer is on duty and performing authorized law enforcement services on behalf of this agency.

Use and Documentation

- F. 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.
- G. Officers who have been issued BWCs shall operate and use them consistent with this policy. Officers shall conduct a function test of their issued BWCs at the beginning of each shift to make sure the devices are operating properly. Officers noting a malfunction during testing or at any other time shall promptly report the malfunction to the officer's supervisor and shall document the report in writing. Supervisors shall take prompt action to address malfunctions and document the steps taken in writing.
- H. Officers should wear their issued BWCs at the location on their body and in the manner specified in training.
- I. Officers must document BWC use and non-use as follows:
 - 3. Whenever an officer makes a recording, the existence of the recording shall be documented in an incident report or on the CFS if no report is written.
 - 4. Whenever an officer fails to record an activity that is required to be recorded under this policy or captures only a part of the activity, the officer must document the circumstances and reasons for not recording in an incident report or on the CFS if no report is written. Supervisors shall review these reports and initiate any corrective action deemed necessary.
- J. The Bagley Police Department will maintain the following records and documents relating to BWC use, which are classified as public data:
 - 1. The total number of BWCs owned or maintained by the agency;
 - 2. A daily record of the total number of BWCs actually deployed and used by officers and, if applicable, the precincts in which they were used;
 - 3. The total amount of recorded BWC data collected and maintained; and
 - 4. This policy, together with the Records Retention Schedule.

General Guidelines for Recording

- G. Officers shall activate their BWCs when anticipating that they will be involved in, become involved in, or witness other officers of this agency involved in a pursuit, *Terry* stop of a motorist or pedestrian, search, seizure, arrest, use of force, adversarial contact, and during other activities likely to yield information having evidentiary value. However, officers need not activate their cameras when it would be unsafe, impossible, or impractical to do so, but such instances of not recording when otherwise required must be documented as specified in the Use and Documentation guidelines, part (D)(2) (above).
- H. Officers have discretion to record or not record general citizen contacts.
- I. Officers have no affirmative duty to inform people that a BWC is being operated or that the individuals are being recorded.
- J. 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.
- K. Officers shall not intentionally block the BWC's audio or visual recording functionality to defeat the purposes of this policy.
- L. Notwithstanding any other provision in this policy, officers shall not use their BWCs to record other agency personnel during non-enforcement related activities, such as during pre- and post-shift time in locker rooms, during meal breaks, or during other private conversations, unless recording is authorized as part of an administrative or criminal investigation.

Special Guidelines for Recording

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

- E. 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.

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

In addition,

- G. Officers need not record persons being provided medical care unless there is reason to believe the recording would document information having evidentiary value. When responding to an apparent mental health crisis or event, BWCs shall be activated as necessary to document any use of force and the basis for it, and any other information having evidentiary value, but need not be activated when doing so would serve only to record symptoms or behaviors believed to be attributable to the mental health issue.
- H. Officers should 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.
- I. Officers portable recording system should 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;
- J. Officers that are 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;
- K. Notwithstanding any law to the contrary, when an individual dies as a result of a use of force by a peace officer, an involved officer's law enforcement agency must allow the deceased individual's next of kin, the legal representative of the deceased individual's next of kin, and the other parent of the deceased individual's child, upon their request, to inspect all portable recording system data, redacted no more than what is required by law, documenting the incident within five days of the request, with the following exception:

A law enforcement agency may deny a request if the agency determines that there is a compelling reason that inspection would interfere with an active investigation. If the agency denies access, the chief law enforcement officer must provide a prompt, written denial to the individual who requested the data with a short description of the compelling reason access was denied and must provide notice that relief may be sought from the district court pursuant to section 13.82 subdivision 7

H. 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;

Downloading and Labeling Data

- E. Each officer using a BWC is responsible for transferring or assuring the proper transfer of the data from his or her camera to that officer's folder located on the digital evidence computer by the end of that officer's shift. However, if the officer is involved in a shooting, in-custody death, or other law enforcement activity resulting in death or great bodily harm, a supervisor or investigator shall take custody of the officer's BWC and assume responsibility for transferring the data from it.
- F. Officers shall label the BWC data files at the time of transfer to storage, and should consult with a supervisor if in doubt as to the appropriate labeling. Officers should assign as many of the following labels as are applicable to each file:
 - 8. **Evidence—criminal:** The information has evidentiary value with respect to an actual or suspected criminal incident or charging decision.
 - 9. **Evidence—force:** Whether or not enforcement action was taken or an arrest resulted, the event involved the application of force by a law enforcement officer of this or another agency.
 - 10. **Evidence—property:** Whether or not enforcement action was taken or an arrest resulted, an officer seized property from an individual or directed an individual to dispossess property.
 - 11. **Evidence—administrative:** The incident involved an adversarial encounter or resulted in a complaint against the officer.
 - 12. **Evidence—other:** The recording has potential evidentiary value for reasons identified by the officer at the time of labeling.
 - 13. **Training:** The event was such that it may have value for training.

14. **Not evidence:** The recording does not contain any of the foregoing categories of information and has no apparent evidentiary value. Recordings of general citizen contacts and unintentionally recorded footage are not evidence.

G. In addition, officers shall flag each file as appropriate to indicate that it contains information about data subjects who may have rights under the MGDPA limiting disclosure of information about them. These individuals include:

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

16. Victims of child abuse or neglect.

17. Vulnerable adults who are victims of maltreatment.

18. Undercover officers.

19. Informants.

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

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

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

23. Mandated reporters.

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

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

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

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

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

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

Administering Access to BWC Data:

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

4. Any person or entity whose image or voice is documented in the data.
5. The officer who collected the data.
6. Any other officer whose voice or image is documented in the data, regardless of whether that officer is or can be identified by the recording.

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

4. BWC data pertaining to people is presumed private, as is BWC data pertaining to businesses or other entities.
5. Some BWC data is classified as confidential (see C. below).
6. Some BWC data is classified as public (see D. below).

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

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

5. Data documenting the discharge of a firearm by a peace officer in the course of duty, other than for training or the killing of an animal that is sick, injured, or dangerous.
6. Data that documents the use of force by a peace officer that results in substantial bodily harm.

7. 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.
8. Data that documents the final disposition of a disciplinary action against a public employee.

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

L. Access to BWC data by non-employees. Officers shall refer members of the media or public seeking access to BWC data to Chief of Police/Administrative Assistant who shall process the request in accordance with the MGDPA and other governing laws. In particular:

3. An individual shall be allowed to review recorded BWC data about him- or herself and other data subjects in the recording, but access shall not be granted:
 - a. If the data was collected or created as part of an active investigation.
 - b. To portions of the data that the agency would otherwise be prohibited by law from disclosing to the person seeking access, such as portions that would reveal identities protected by Minn. Stat. § 13.82, subd. 17.
4. Unless the data is part of an active investigation, an individual data subject shall be provided with a copy of the recording upon request, but subject to the following guidelines on redaction:
 - a. Data on other individuals in the recording who do not consent to the release must be redacted.
 - b. Data that would identify undercover officers must be redacted.
 - c. Data on other officers who are not undercover, and who are on duty and engaged in the performance of official duties, may not be redacted.

M. Access by peace officers and law enforcement employees. No employee may have access to the Bagley Police Department's BWC data except for legitimate law enforcement or data administration purposes:

4. Officers may access and view stored BWC video only when there is a business need for doing so, including the need to defend against an allegation of misconduct or substandard performance. Except as provided in the critical incident response policy, officers may review video footage of an incident in which they were involved prior to preparing a report, giving a statement, or providing testimony about the incident.
5. Agency personnel shall document their reasons for accessing stored BWC data within incident reports/supplements to the case file relate to the video, at the time of each access. Agency personnel are prohibited from accessing BWC data for non-business reasons and from sharing the data for non-law enforcement related purposes, including but not limited to uploading BWC data recorded or maintained by this agency to public and social media websites.
6. 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.
7. Law Enforcement requests for BWC footage in writing, as well as an acknowledgment of the receiving agency's responsibilities under 13.875 Subd. 7 and 8. This could be done by sending an email with the verbiage and receiving an email back confirming their understanding

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

1. BWC data may be shared with other law enforcement agencies only for legitimate law enforcement purposes that are documented in writing at the time of the disclosure.
2. BWC data shall be made available to prosecutors, courts, and other criminal justice entities as provided by law.

Data Security Safeguards

- E. All BWC files recorded will be only downloaded onto the Bagley Police Departments Digital Evidence computer. This computer will not be connected to any network and will have mirrored drive to prevent any data loss.

- F. 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.
- G. Officers shall not intentionally edit, alter, or erase any BWC recording unless otherwise expressly authorized by the chief or the chief's designee.
- H. As required by Minn. Stat. § 13.825, subd. 9, as may be amended from time to time, this agency shall obtain an independent biennial audit of its BWC program.

Agency Use of Data

- E. At least once a month, supervisors will randomly review BWC usage by each officer to ensure compliance with this policy and to identify any performance areas in which additional training or guidance is required.
- F. In addition, supervisors and other assigned personnel may access BWC data for the purposes of reviewing or investigating a specific incident that has given rise to a complaint or concern about officer misconduct or performance.
- G. Nothing in this policy limits or prohibits the use of BWC data as evidence of misconduct or as a basis for discipline.
- H. Officers should contact their supervisors to discuss retaining and using BWC footage for training purposes. Officer objections to preserving or using certain footage for training will be considered on a case-by-case basis. Field training officers may utilize BWC data with trainees for the purpose of providing coaching and feedback on the trainees' performance.

Data Retention

- I. All BWC data shall be retained for a minimum period of 90 days. There are no exceptions for erroneously recorded or non-evidentiary data.
- J. Data documenting the discharge of a firearm by a peace officer in the course of duty, other than for training or the killing of an animal that is sick, injured, or dangerous, must be maintained for a minimum period of one year.

13.825

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

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

1. (a) A prohibition on altering, erasing or destroying any recording made with a peace officer's portable recording system or data and metadata related to the recording prior the expiration of the applicable retention period under section 13.825 Subdivision 3, except that the full, unedited, and (b) unredacted recording of a peace officer using deadly force must be maintained indefinitely;

4. Data documenting circumstances that have given rise to a formal complaint against an officer.
- L. Other data having evidentiary value shall be retained for the period specified in the Records Retention Schedule. When a particular recording is subject to multiple retention periods, it shall be maintained for the longest applicable period.
 - M. Subject to Part F (below), all other BWC footage that is classified as non-evidentiary, becomes classified as non-evidentiary, or is not maintained for training shall be destroyed after 90 days.
 - N. 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.
 - O. The Bagley Police Department shall maintain an inventory of BWC recordings having evidentiary value.
 - P. The Bagley Police Department will post this policy, together with its Records Retention Schedule, on its website.
 - Q. BWC data that must be retained for a minimum period of one year: "Any use of force by an officer that results in substantial bodily harm."

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.