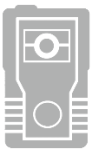


INDEPENDENT AUDITOR'S REPORT

Glenwood Police Department



NOVEMBER 3RD, 2026

RAMPART AUDIT, LLC

Audit Overview and Recommendations

Dear Glenwood City Council and Chief Danter:

We have audited the body-worn camera (BWC) program of the Glenwood Police Department (GPD) for the two-year period ended 8/09/2026. 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 Glenwood Police Department. Our responsibility is to express an opinion on the operations of this program based on our audit.

On September 10, 2026, Rampart Audit, LLC (Rampart) met with Records Manager Estelle Garvin, who provided information about GPD'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 GPD's recordkeeping.

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

GPD BWC Program Implementation and Authorization

Effective August 1, 2016, Minnesota Statute §626.8473 Subd. 2 requires that:

> A local law enforcement agency must provide an opportunity for public comment before it purchases or implements a portable recording system. At a minimum, the agency must accept public comments submitted electronically or by mail, and the governing body with jurisdiction over the budget of the law enforcement agency must provide an opportunity for public comment at a regularly-scheduled meeting.

Rampart previously audited GPD's BWC program in 2025. As part of that audit, GPD personnel advised us that their BWC program was implemented on 8/10/2022. GPD provided the following documentation to show that the public notice and hearing requirements were met prior to the program's implementation:

- A copy of Glenwood City Commission Meeting minutes, dated July 12, 2022, in which a public meeting was opened for comment with no comments submitted and no one attending the meeting to comment. The public comment period was then closed. Assistant City Attorney Troy

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

Nelson said the policy meets all statutory requirements, but he suggested a verbiage change to one paragraph. A majority voted in favor of a motion to approve the body worn camera policy.

- Rampart located a news article published in the Pope County Tribune published June 20th, 2022, which provided public notification of the future meeting to be held regarding the body-worn camera program and invited the public to attend the meeting July 12th, 2022, as well as to submit comments by mail or email.

Copies of these documents have been retained in Rampart's audit files. In our opinion, GPD satisfied the requirements of §626.8473 Subd. 2 prior to the implementation of their BWC program.

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

Rampart verified that there was a working link to GPD's BWC policy on the Public Safety Dashboard of the City of Glenwood's website. In our opinion, Glenwood Police Department is compliant with the requirements of §626.8473 Subd. 3(a).

GPD BWC WRITTEN POLICY

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

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

This same section of GPD's BWC policy establishes a minimum retention period of one year for BWC data documenting a reportable firearms discharge, and a minimum retention period of six years for BWC data documenting "the use of force by a peace officer, or force of a sufficient type or degree to require a use of force report for supervisory review," as well as "data documenting circumstances that have given rise to a formal complaint against an officer." In our opinion, these standards satisfy the requirements of §13.825 Subd. 3(b).

The Use and Documentation section of GPD's BWC policy states that "the full, unedited and… unredacted recording of a peace officer using deadly force must be maintained indefinitely," as required by §13.825 Subd. 3(c).

The Data Retention section of GPD's BWC policy states that "[u]pon written request by a BWC data subject, the agency shall retain a recording pertaining to that data subject for an additional time requested by the subject of up to 180 days…" In our opinion, this satisfies the requirements of §13.825 Subd. 3(d).

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

The Use and Documentation section of GPD's BWC policy states that "[o]fficers are prohibited from altering, erasing or destroying any recording made with a peace officer's portable recording system or data and metadata related to the recording prior [to] the expiration of the applicable retention period…" In our opinion this satisfies the requirement described in Clause 2 of the Policy section of this report.

GPD employs Getac body-worn cameras and utilizes Getac's Cloud Storage and manages BWC data retention through automated retention settings in Getac's 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 corrected or amended by the Chief of Police or Administrative Assistant/Records Manager as needed. If an officer fails to assign a data classification, the default retention period is 368 days to avoid accidental loss of data.

The Downloading and Labeling Data section of GPD'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 the approved docking method to be synchronized with the digital evidence program via the could sever [sic] 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.

The policy further states that "[o]fficers 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…"

Records Manager Garvin advised that the Getac body-worn cameras are capable of uploading wirelessly when docked in the officer's squad, but also utilize physical docking stations located at the Glenwood Police Department.

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

GPD BWC Data Destruction

As discussed above, GPD utilizes Getac's Cloud Service for storage, with retention periods determined based on the classification assigned to BWC data. BWC recordings are purged automatically within Getac's data management software upon expiration of the associated retention period.

Getac certifies that its Cloud Service is compliant with the Federal Bureau of Investigation's Criminal Justice Information System Security Division Policy as required by Minn. Stat §13.825 Subd. 11(b). Data destruction is achieved through automated deletion and overwriting, with storage devices sanitized (overwritten three or more times or degaussed) or physically destroyed upon being removed from service.

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

GPD BWC Data Access

The Access to BWC data by non-employees section of GPD's BWC policy states that:

> Officers shall refer members of the media or public seeking access to BWC data to [the] Chief of Police/Administrative Assistant who shall process the request in accordance with the MGDPA [Minnesota Government Data Practices Act] and other governing laws.

Records Manager Garvin advised us that that all requests for BWC data from the public or media are made in writing using Glenwood Police Department's data request form. Requests are directed to either the Chief of Police or the Records Manager, who reviews, approves and processes them. BWC video is provided to members of the public via secure internet link or physical media such as a USB memory device.

As discussed in Clauses 5 and 6 of the Policy section of this report, the Minnesota State Legislature in 2023 added specific access requirements related to BWC data that document deadly force incidents, and specified that these requirements must be included in the agency's BWC policy. A review of the Use and Documentation section of GPD's BWC policy shows that GPD has incorporated these requirements into its BWC policy.

GPD'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."

Requests for BWC data from other law enforcement agencies are submitted in writing to the Records Manager using the BWC Data Agency Sharing form, a copy of which is included with the BWC policy in Appendix A. The form may also be submitted to the Chief of Police if the Records Manager is unavailable. BWC data are shared with other law enforcement agencies via email containing a secure internet link.

The policy also states that "BWC data shall be made available to prosecutors, courts, and other criminal justice entities as provided by law." Prosecutors use the same data request process described for law enforcement above.

The BWC Data Agency Sharing form requires the requesting law enforcement officer to provide a signed acknowledgment of the receiving agency's responsibilities under § 13.825 Subd. 7 and 8 to maintain portable recording system data security. Rampart recommends this practice.

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

GPD BWC Data Classification

The Administering Access to BWC Data section of GPD's BWC Policy states that "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."

Active criminal investigation data are classified as confidential. GPD's BWC Policy also identifies certain categories of BWC data that are public.

As noted in the preceding section, GPD 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, GPD's BWC policy is compliant with respect to the applicable data classification requirements.

GPD BWC Internal Compliance Verification

The Compliance section of GPD's BWC policy states that "[s]upervisors shall monitor for compliance with this policy," while the Agency Use of Data section 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."

All access to BWC data is logged in the Getac software.

The Use and Documentation section of GPD's BWC policy states that: "[o]fficers 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."

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 GPD's BWC policy includes language to address this new requirement and states "[o]fficers assigned a BWC [must] wear and operate the system in compliance with the agency's policy… while performing activities under the command and control of another chief law enforcement officer or federal law enforcement official."

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

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

GPD BWC Program and Inventory

GPD currently possesses 7 Getac body-worn cameras, all of which are assigned to specific officers.

The GPD 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 Use and Documentation section of GPD's BWC policy states: "[o]fficers will wear their BWCs 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."

Records Manager Garvin advised us that she is able to determine the number of BWCs deployed by reviewing the schedule and/or payroll data.

As of 9/10/2026, GPD maintained 1,533 BWC recordings.

GPD BWC Physical, Technological and Procedural Safeguards

GPD BWC data are initially recorded to a hard drive in each officer's BWC. Data from each BWC is then uploaded to Getac's Cloud Service via a wireless upload from the officer's squad, or using a physical docking station located at the Glenwood 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. All BWC data access is logged automatically and available for audit purposes.

Enhanced Surveillance Technology

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

Audit Conclusions

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



Rampart Audit, LLC

11/03/2026

APPENDIX A:

100. BODY WORN CAMERA

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.

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.

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 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.

4. 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.

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 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, or as soon as practically possible, 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 will wear their BWCs 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;

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 Evidence Section in RMS (LETG) 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 in the Case Notes in RMS (LETG) if no report is written. Supervisors shall review these reports and initiate any corrective action deemed necessary.

3. Officers are prohibited from 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. 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. 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;

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

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

2. A daily record of the total number of BWCs 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.

6. 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* stops 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.

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.

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.

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 the approved docking method to be synchronized with the digital evidence program via the could sever 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. Traffic Stop

2. Test

3. Suspicious

4. Other

5. Medical

6. Interview

7. Fire

8. Escort

9. DWI

10. Domestic

11. Criminal Activity

12. Citizen Interaction

13. Assault

14. Arrest

15 Animal

16 Accident.

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.

9. 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 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/case notes 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.

10 DATA SECURITY SAFEGUARDS

A. All BWC files recorded will be only uploaded onto the department's approved Digital Evidence cloud server. This server will not be connected to any unapproved network and will have server data loss prevention measures in place.

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.

11. 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.

12. 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 force by a peace officer, or force of a sufficient type or degree to require a use of force report for 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 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 department shall maintain an inventory of BWC recordings having evidentiary value.

H. The department will post this policy, together with its Records Retention Schedule, on its website.

I. 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;

J. 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.

K. The following categories of BWC data be retained for a minimum period of one year:

a. any reportable firearms discharge;

b. any use of force by an officer that results in substantial bodily harm; and
c. any incident that results in a formal complaint against an officer.

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.

FOR ANY OTHER OFFICER MISCONDUCT INVESTIGATIONS PLEASE REFER TO GLENWOOD POLICE DEPARTMENT'S POLICY ON OFFICER MISCONDUCT.

101. BWC DATA AGENCY SHARING

BWC DATA AGENCY SHARING FORM

Requesting Agency: _____ Dated:

_____

Email:_____ Telephone:

_____

Address:

_____

Purpose for data request:

_____

By signing below, I acknowledge any BWC data obtained from the Glenwood Police Department will be managed by my agency in compliance with the most current requirements of §13.825 Subd. 7 & 8. Below is an example of the requirements within §13.825.

Subd. 7. Authorization to access data.

(a) A law enforcement agency must comply with sections 13.05, subdivision 5, and 13.055 in the operation of portable recording systems and in maintaining portable recording system data.

(b) The responsible authority for a law enforcement agency must establish written procedures to ensure that law enforcement personnel have access to the portable recording system data that are not public only if authorized in writing by the chief of police, sheriff, or head of the law enforcement agency, or their designee, to obtain access to the data for a **legitimate, specified law enforcement purpose.**

Subd. 8. Sharing among agencies.

(a) Portable recording system data that are not public may only be shared with or disseminated to another law enforcement agency, a governmental entity, or a federal agency upon meeting the standards for requesting access to data as provided in subdivision 7.

(b) If data collected by a portable recording system are shared with another state or local law enforcement agency under this subdivision, the agency that receives the data must

comply with all data classification, destruction, and security requirements of this section.

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

Authorized Requesting Agency Designee:

_____

Return this completed for to the Glenwood Police Department

Pursuant to Minnesota Law this data request may be subject to charges as outlined in the Glenwood Police Department's Data Practices Policy

This portion of the form is to be completed by the Glenwood Police Department	
Department/Division name	Request Handled by
Request Type · In Person · Mail · Phone · Electronic	Request by · Subject of Data · Not Subject of data
Classification of information requested · Public Non Public · Private Protected · Confidential	Request · Approved · Denied Authorized Signature **X**
Remarks/ Comments	

Fees: (Flat Rate)_____ x _____ Pages Rate Per Page Staff Preparation Time: (Where Applicable) _____ X _____ Rate Hours	** *A receipted copy of this form must be provided to the requestor each time money is received* ** I have Received from the above named, the amount indicated opposite my signature in payment for providing the data.	
Total Amount Due:	Received By	Date
Amount to be prepaid	Received By	Date
Balance due	Received By	Date

GPD REV 04/11/2025