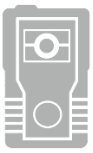
INDEPENDENT AUDITOR'S REPORT

Gaylord Police Department



DECEMBER 22ND, 2025

RAMPART AUDIT LLC

Audit Overview and Recommendations

Dear Gaylord City Council and Chief Eichten:

We have audited the body-worn camera (BWC) program of the Gaylord Police Department (GPD) for the two-year period ended 10/08/2025. 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 Gaylord Police Department. Our responsibility is to express an opinion on the operations of this program based on our audit.

On October 24, 2025, Rampart Audit, LLC (Rampart) met with Chief Charlie Eichten, who provided information about GPD's BWC program policies, procedures and operations. As part of the audit, 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.

Chief Eichten provided copies of the following documents as evidence that GPD had met these requirements:

1. A public notice dated August 3, 2023, and published in the *Gaylord Hub* newspaper, announcing that a public hearing was to be held during the August 16, 2023, Gaylord City Council meeting to discuss the proposed BWC program and policy. The notice provided instructions for reviewing a copy of the proposed BWC policy. It also included an invitation and instructions for providing written comments via mail in advance of the meeting, or oral comments by phone prior to the meeting or in-person at the meeting.
2. A copy of the August 16, 2023, Gaylord City Council meeting minutes, which document that a public hearing was held regarding the proposed GPD BWC program. The minutes noted that

[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.

following the public hearing, the Gaylord City Council voted unanimously to approve implementation of GPD's BWC program.

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

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

As part of the requested audit documentation, Chief Eichten provided a clickable link to the BWC policy on the Gaylord Police Department page of the Gaylord City website. Rampart verified that this was a working link. In our opinion, Gaylord 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 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.

Part A of the Data Retention section of GPD's BWC policy states: "All BWC data shall be retained for a minimum period of 90 days. There are no exceptions for erroneously recorded or non-evidentiary data." This satisfies the requirements of §13.825 Subd. 3(a).

Part B of the Data Retention section of GPD's BWC policy specifies a minimum retention period of one year for that BWC data documenting a reportable firearms discharge, while Part C specifies a minimum retention period of six years for "[d]ata that documents the use of deadly force by a peace officer, or force of a sufficient type or degree to require a use of force report," as well as "[d]ata documenting circumstances that have given rise to a formal complaint against an officer." These meet or exceed the requirements contained in §13.825 Subd. 3(b).

While the passage quoted above specifies a six-year retention period for BWC data documenting the use of deadly force by a peace officer, Part B of the Data Security Safeguards section of GPD's BWC policy states: "…the full, unedited, and unredacted recording of a peace officer using deadly force must be maintained indefinitely." In addition, Part D of the Data Retention section states: "[w]hen a particular recording is subject to multiple retention periods, it shall be maintained for the longest applicable period." These passages collectively satisfy the indefinite retention requirement contained in §13.825 Subd. 3(c). The reference to a six-year retention period for data documenting deadly force incidents appears to be an artifact from an earlier version of the policy. We recommend removing it to improve clarity.

Part F of the Data Retention section states:

> Upon written request by a BWC data subject, the agency shall retain a recording pertaining to that subject for an additional time period requested by the subject of up to 180 days. 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.

This satisfies the requirements contained in §13.825 Subd. 3(d).

Chief Eichten advised us that in the event an officer fails to assign a category to a BWC recording, that recording is retained indefinitely to prevent the accidental loss of data.

As discussed in Clause 2 of the Policy section of this report, a BWC policy must prohibit altering, erasing or destroying any recording made with a peace officer's portable recording system, as well as associated data or metadata, prior to the expiration of the applicable retention period. In addition, the full, unedited, and unredacted recording of a peace officer using deadly force must be maintained indefinitely. This requirement is addressed in Part B of the Data Security Safeguards section of GPD's BWC policy.

Gaylord Police Department employs LensLock body-worn cameras and utilizes LensLock's secure cloud storage. GPD manages BWC data retention through automated retention settings in the Video Evidence Database management software. The retention period for each video is determined by the data classification assigned at the time of upload; however, this retention period can be adjusted as needed.

The Downloading and Labeling Data section of GPD's BWC policy states: "[o]fficers shall label the BWC data files at the time of capture or transfer to storage and should consult with a supervisor if in doubt as to the appropriate labeling."

Chief Eichten advised us that GPD utilizes a physical BWC docking station located at their office.

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

GPD BWC Data Destruction

As discussed above, GPD's BWC data are stored on LensLock's cloud-based storage service, with data retention and deletion schedules managed automatically through the Video Evidence Database video management software based on the assigned data classification of each video.

LensLock utilizes Microsoft's Azure Government environment for cloud storage. Microsoft certifies this environment as being compliant with current Federal Bureau of Investigation Criminal Justice Information Services Division Security Policy, and notes that it has signed CJIS management agreements with 45 of the 50 U.S. states, including Minnesota, to verify compliance with state CJIS requirements.

FBI CJIS policy requires that hard drives used for CJIS data storage are sanitized by overwriting at least three times or degaussing prior to being released to unauthorized individuals, while inoperable drives must be destroyed through physical means such as shredding.

GPD BWC Data Access

The Access to BWC data by non-employees section of GPD's BWC policy states that: "[o]fficers shall refer members of the media or public seeking access to BWC data to" Chief Eichten, "who shall process the request in accordance with the [Minnesota Governmental Data Practices Act] and other governing laws."

Chief Eichten advised us that members of the media or public seeking access to BWC data submit a written data request form, which is available on the GPD webpage or in the office. The completed form is submitted to Chief Eichten, who reviews it and, if approved, processes it. Requests are fulfilled via an email link.

GPD BWC data is shared with other law enforcement agencies for evidentiary purposes only. All such requests must be made in writing via data request form or email to Chief Eichten. Existing verbal agreements between GPD and other area law enforcement agencies address data classification, destruction and security requirements, as specified in §13.825 Subd. 8(b). In addition, the email generated by the LensLock system when providing a link to the requested video contains a disclaimer addressing these concerns.

We recommend that a file of these requests be maintained for audit purposes.

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. These requirements are addressed in the Access to BWC data by non-employees section of GPD's BWC policy.

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 unless there is a specific law that provides differently." The policy also identifies data that are classified as public or confidential, and provides guidance for instances in which conflicting classifications apply.

In our opinion, GPD's BWC policy is compliant with the BWC data classification requirements specified in Minn. Stat. §13.825.

GPD BWC Internal Compliance Verification

The Agency Use of Data section of the GPD BWC policy states that:

> At least once a month or as soon as practicable, supervisors will randomly review BWC usage by each officer that worked in the previous month, to whom a BWC is issued or available for use, to ensure compliance with this policy and to identify any performance areas in which additional training or guidance is required.

Chief Eichten confirmed during the audit that he conducts reviews monthly and maintains a log of those 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 specify 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. This requirement is addressed in the Use and Documentation section of GPD's BWC policy.

The Compliance section of GPD's 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, GPD's 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 six (6) LensLock body-worn cameras, all of which are in regular use.

The GPD BWC policy identifies those circumstances in which deputies 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 GPD does not maintain a separate log of BWC deployment or use, Chief Eichten advised us that the LensLock cloud software contains a GPS feature that makes it possible to determine in real-time the number of cameras deployed. Alternatively, the number of BWC units deployed each shift can be

determined based on a review of GPD payroll records. BWC use would be determined based on the creation of BWC data.

As of 10/24/2025, GPD maintained 5,168 BWC recordings.

GPD BWC Physical, Technological and Procedural Safeguards

GPD BWC data are initially recorded to an internal hard drive in each camera. Those data are then uploaded to LensLock's cloud-based server via a physical docking station located at the GPD office. Officers have view-only access to their data for report writing.

As noted in Clause 3 of the Policy section of this report, the 2023 legislative updates require that a BWC policy specify that the device be worn at or above the mid-line of the waist. This is addressed in the Use and Documentation section of the GPD BWC policy

Enhanced Surveillance Technology

GPD 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 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 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. The auditors reviewed the retained BWC videos to verify that this data was accurately documented in GPD records.

Audit Conclusions

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

Rampart Audit, LLC

12/22/2025

APPENDIX A:

Title: **Body Cameras**

Policy: **30**

City of Gaylord, Minnesota Use of Body-Worn Cameras Policy

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

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

Scope
This policy governs the use of BWCs in the course of official duties. It does not apply to the use of squad-based (dash-cam) recording systems. The chief or 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. This policy is a living document and any changes to the BWC policy must be approved by the City Council.

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

A. **Body-Worn Cameras** means a device worn by an officer that is capable of both video and audio recording of the officer's activities and interactions with others or collecting digital multimedia evidence as part of an investigation and is provided in Minn. Stat. 13.825.

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

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

D. **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.

E. **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.

F. **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.

G. **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.

H. **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.

I. **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 in an approved, conspicuous location on their body above the mid-line of the waist to maximize the recording capabilities of the officers 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 an ICR summary.
2. Whenever an officer fails to record an activity that is required to be recorded under this policy or fails to record for the entire duration of the activity, the officer must document the circumstances and reasons for not recording in an incident report. Supervisors shall review these reports and initiate any corrective action deemed necessary.

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

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

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

F. While under the command and control of another chief law enforcement officer or federal law enforcement official, officers issued a BWC shall wear it in accordance with policy.

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. In documented circumstances on the BWC audio, officers who desire to discuss additional steps regarding the circumstances of a given law enforcement encounter with fellow law enforcement
officers or officers of the court, shall have the discretion to manually mute the audio recording function temporarily, so long as **all** of the following happen:

   a. Officers shall verbally document their intent to do so on the BWC or in a written report.

   b. Officers must manually mute the device.

   c. The device shall not be muted for longer than necessary to complete the discussion with other law enforcement officers or officers of the court.

G. 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.

H. Officers are prohibited from using department-issued BWC equipment for personal use and are prohibited from making personal copies of recordings created while on-duty or while acting in their official capacity.

I. There are no additional requirements to notify a data subject of a recording as Minnesota is a single party consent state.

Special Guidelines for Recording

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

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

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

In addition,

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

D. Officers shall use their BWCs and squad-based audio/video systems to record their transportation and the physical transfer of persons in their custody to hospitals, detox and mental health care facilities, juvenile detention centers, and jails, but otherwise should not record in these facilities unless the officer anticipates witnessing a criminal event or being involved in or witnessing an adversarial encounter or use-of-force incident.

Downloading and Labeling Data

A. Each officer using a BWC is responsible for transferring or assuring the proper transfer of the data from his or her camera to the cloud storage by the end of that officer's shift. However, if the officer is involved in a shooting, in-custody death, or other law enforcement activity resulting in death or great bodily harm, a supervisor or investigator shall take custody of the officer's BWC and assume responsibility for transferring the data from it.
B. Officers shall label the BWC data files at the time of capture or transfer to storage and should consult with a supervisor if in doubt as to the appropriate labeling.

1. Traffic Warning
2. Traffic Citation
3. Traffic Accident
4. Agency Assist
5. Animal Complaint
6. Arrest
7. Assault/Domestic
8. Burglary
9. Civil Issue
10. Child Protection
11. Death
12. Disorderly/Fight
13. Drugs/Narcotics
14. DUI
15. Fire Call
16. Juvenile
17. Mental Health
18. Motorist Assist
19. Open Door
20. City Ordinance
21. Pursuit/Evading
22. Search Warrant

23. Suspicious Activity
24. Test Recording
25. Theft
26. Warrant
27. Interview
28. Citizen Contact
29. Use of Force
30. Public Assist
31. Medical
32. Investigation
33. Transport
34. Welfare Check

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

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

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

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

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

    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.

3. In the event that an individual dies as a result of a use of force by a peace officer,

an involved officer's law enforcement agency must allow the following individuals, upon their request, to inspect all portable recording system data, redacted no more than what is required by law, documenting the incident within five days of the request.

a. the deceased individual's next of kin;

b. the legal representative of the deceased individual's next of kin; and

c. the other parent of the deceased individual's child.

d. 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;

4. In the event that an individual dies as a result of a use of force by a peace officer, an involved officer's law enforcement agency shall release all portable recording system data, redacted no more than what is required by law, documenting the incident no later than 14 days after the incident, unless the chief law enforcement officer asserts in writing that the public classification would interfere with an ongoing investigation, in which case the data remain classified by section 13.82, subdivision 7;

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

1. Officers may access and view stored BWC video only when there is a business need for doing so, including the need to defend against an allegation of misconduct or substandard performance. Officers may review video footage of an incident in which they were involved prior to preparing a report, giving a statement, or providing testimony about the incident.

2. Agency personnel shall document their reasons for accessing stored BWC data 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 individual identities that are not public. Protecting against incidental disclosure could involve, for instance, showing only a portion of the video, showing only screen shots, muting the audio, or playing the audio but not displaying video. In addition,

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

B. Officers shall not intentionally edit, alter, or erase any BWC recording made with a peace officer's portable recording system or data and metadata related to the recording prior to the expiration of the applicable retention period under section 13.825 Subdivision 3, except that the full, unedited, and unredacted recording of a peace officer using deadly force must be maintained indefinitely.

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

Agency Use of Data

A. At least once a month or as soon as practicable, supervisors will randomly review BWC usage by each officer that worked in the previous month, to whom a BWC is issued or available for use, 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 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.

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.

Conclusion

The use of this technology will add a higher level of transparency of the professional services provided by the Gaylord Police Department. This device will also aid in the documentation of events to be used in an evidentiary manner. There needs to be an understanding that the camera view will not capture the entire incident or event, thus it cannot be construed that images are a complete representation of actions by officers and citizens.

Policy adopted and approved by city council, effective 08/16/2023. Policy amended and approved by city council, effective 11/01/2023. Policy amended and approved by city council, effective 02/05/2025.

Charlie Eichten Chief of Police

Gaylord Police Department