

INDEPENDENT AUDITOR'S REPORT

Clearbrook-Gonvick Police Department



APRIL 10TH, 2025
RAMPART AUDIT LLC

Audit Overview and Recommendations

Dear Clearbrook City Council and Chief Solee:

We have audited the body-worn camera (BWC) program of the Clearbrook Gonvick Police Department (CGPD)¹ for the two-year period ended 6/30/2024. Minnesota Statute §13.825 mandates that any law enforcement agency operating a portable recording system (PRS)² program obtain an independent, biennial audit of its program. This program and its associated data are the responsibility of the Clearbrook Gonvick Police Department. Our responsibility is to express an opinion on the operations of this program based on our audit.

On December 21, 2024, Rampart Audit LLC (Rampart) met with Chief Ryan Solee, who provided information about CGPD'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 CGPD's recordkeeping.

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

CGPD BWC Program Implementation and Authorization

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

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

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

Chief Solee advised that CGPD's BWC program began in approximately 2012, prior to his employment with the agency. While this was also prior to the public notice and hearing requirements discussed above, he was aware that his predecessor had taken steps during 2016 to meet those requirements. He

¹ The Clearbrook Gonvick Police Department is organized under the City of Clearbrook. The nearby City of Gonvick contracts for coverage and that city's name is included as part of the police department name.

² 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 CGPD, these terms may be used interchangeably in this report.

also advised, however, that because the City of Clearbrook relies heavily on paper records, he was unable to locate documentation to substantiate that the public notice and hearing requirements were met.

Due to the lack of documentation provided by the agency as part of this audit, Rampart does not express an opinion as to whether CGPD met the requirements contained in Minn. Stat. §626.8473 Subd. 2 during 2016. We recommend that if CGPD is unable to locate documentation to substantiate that the public notice and hearing requirements were met previously, that they repost the public notice and hold a new public hearing.

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

While CGPD has neither its own website nor a dedicated page on the City of Clearbrook website, Rampart verified that there was a working link to CGPD's BWC policy on the City of Clearbrook website. In our opinion, Clearbrook Gonvick Police Department is compliant with the requirements of §626.8473 Subd. 3(a).

CGPD BWC WRITTEN POLICY

As part of this audit, we reviewed CGPD'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;
- 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 CGPD 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.

CGPD 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 Retention of Recordings section of CGPD's BWC policy includes the agency's retention schedule, which specifies a retention period of 90 days as the "minimum for ALL video, including accidental or test recordings."

CGPD's BWC policy specifies a retention period of one year for the data categories enumerated in §13.825 Subd. 3(b), and an "indefinite" retention period for "data documenting an officer's use of deadly force," as required in §13.825 Subd. 3(c). CGPD's policy also addresses the §13.825 Subd. 3(d) requirement, and notes that such additional retention is mandatory.

Finally, the policy prohibits "altering, erasing, or destroying any recording made with a peace officer's portable recording system or data or metadata related to the recording prior to the expiration of the applicable retention period," as discussed in Clause 2 above.

CGPD employs Axon body-worn cameras. Chief Solee manages BWC data retention utilizing a Windows desktop computer, for which he has the only login credentials. Although Axon's Evidence software is used for the initial BWC download, Windows Media Player is used for viewing, and files are deleted manually after the expiration of the associated retention period.

Chief Solee is responsible for transferring all data from the BWCs to the desktop computer, and labels each file with the case number and a brief description of its contents.

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

CGPD BWC Data Destruction

In addition to the desktop PC described above, CGPD BWC data are backed up to an external hard drive on a monthly basis.

Data on both the PC and the external hard drive are destroyed through manual deletion. At the time a computer or external hard drive is retired from service, the device is destroyed by physical means, specifically incinerating. This is consistent with FBI CJIS policy, which requires that inoperable drives previously used for CJIS data be destroyed through physical means such as shredding.

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

CGPD BWC Data Access

Any request for access to BWC data by a data subject or member of the media would be made in writing to Chief Solee. Approved requests are fulfilled via USB memory devices.

CGPD's BWC policy states that data are "shared with other law enforcement agencies for legitimate purposes that are documented in writing at the time of the request." Chief Solee advised us that all such requests must be made to him by email. While existing verbal agreements between CGPD and other

area law enforcement agencies address data classification, destruction and security requirements, as specified in §13.825 Subd. 8(b), Chief Solee requested from Rampart an example of a written acknowledgement form used by several of our audit clients for future requests.

Access to CGPD BWC data for outside agencies is provided via USB memory device.

The Clearwater County Attorney's Office contacts Chief Solee directly when requesting BWC data, with these requests also fulfilled via 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. CGPD's BWC policy includes language addressing these requirements, which is copied directly from the statute.

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

CGPD BWC Data Classification

The Release of Recordings section of CGPD's BWC policy identifies those categories of BWC data deemed private, confidential or public, and notes that BWC data will only be released "following Minnesota Private Data Request laws (Minn. Stat. 13)." The Death Resulting from Use of Force – Release of Public Data section of the policy addresses the specific access, release and data classification requirements discussed in Clauses 5 and 6 of the Policy section of this report.

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

CGPD BWC Internal Compliance Verification

The Review of Recorded Media Files section of the CGPD BWC policy states that "[r]ecorded files may be reviewed as part of an internal audit and review." This section of the BWC policy also states: "[t]he Chief of Police will review the recordings of each device randomly periodically and also audit history and compare information detailed in written reports." Chief Solee advised us that because he is responsible for transferring all BWC recordings, he reviews any significant recordings made by other officers.

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. This requirement is included in the Members Responsibilities section of the BWC policy.

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

CGPD's BWC policy states that "[a]ny member who violates any part of this policy is subject to discipline action and/or criminal prosecution."

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

CGPD BWC Program and Inventory

CGPD currently possesses two (2) Axon 2 body-worn cameras. As the only full-time officer, Chief Solee uses one of the BWCs, while the other is made available to the agency's three part-time officers, all of whom work infrequently.

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

The CGPD BWC policy explicitly prohibits the use of personally-owned portable recording devices, consistent with Minn. Stat. §13.825 Subd. 6.

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

As of the date of the audit, CGPD maintained five (5) BWC data files.

CGPD BWC Physical, Technological and Procedural Safeguards

CGPD BWC data are initially recorded to an internal hard drive in each officer's BWC. Those files are then transferred to Chief Solee's PC by means of a USB cable. Chief Solee has the only login credentials for this computer, though he is able to provide supervised access to part-time officers on a case-by-case basis as needed to review recordings.

Chief Solee's PC is secured inside the Clearbrook Gonvick Police Department, which is a locked office suite inside a larger city facility. As noted earlier in this report, Chief Solee backs up BWC recordings onto an external hard drive monthly to guard against possible loss of data due to a hardware failure. This external hard drive is stored in a concrete vault located inside the police department that is built to withstand fires and wind events, while its elevation makes flooding unlikely. In addition, evidentiary recordings are provided to the Clearwater County Attorney promptly.

Officers have supervised, view-only access to their own data for report writing, trial preparation, data administration, investigatory purposes and other legitimate law enforcement purposes.

CGPD's BWC policy states that: "Members my not use department-issued recorders for personal use."

As noted above, requests by other law enforcement agencies for CGPD BWC data must be approved by Chief Solee and are fulfilled via USB memory device. A similar method is employed to submit CGPD BWC data to the Clearwater County Attorney's Office.

Rampart Audit, LLC

The Member Responsibilities section of CGPD's BWC policy states: "Uniformed members should conspicuously wear the recorder at or above the midline or (sic) the waist and notify persons that they are being recorded, whenever reasonably practicable." While we recommend adding language to clarify that unless acting in an undercover capacity, all members are required to wear the BWC at or above the mid-line of the waist, in our opinion, this satisfies the requirement discussed in Clause 3 of the Policy section of this report.

Enhanced Surveillance Technology

CGPD 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 CGPD 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

Because CGPD is a small agency with few calls for service and only intermittent patrol coverage, Rampart conducted a review of all five (5) of the agency's retained BWC recordings. All five recordings were clearly labeled by case number and type.

Audit Conclusions

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

Rampart Audit LLC

04/10/2025

APPENDIX A:



Portable Audio/Video Recorders

Purpose and Scope:

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

This policy does not apply to mobile audio/video recordings, interviews, or interrogations conducted by the Clearbrook-Gonvick Police Department facility, undercover operations, wiretaps, or eavesdropping (Concealed listening devices).

Definitions:

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

BWC-Body worn camera.

CGPD-Clearbrook-Gonvick Police Department.

Policy:

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

Coordinator:

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

- (a) Establishing procedures for the security, storage, and maintenance of data and recordings.
 - The coordinator should work with the Custodian of Records and the member assigned to coordinate the use, access, and release of protected information to ensure that the procedures comply with requirements of the Minnesota Government Data Practices Act (MGDPA) and other applications laws (Minn. Stat 13.01 et seq).
 - 2. The coordinator should work with the custodian of Records to identify recordings that must be retained for the specific time frame under Minnesota law (e.g., firearm discharges, certain use of force incidents, formal complaints).
- (b) Establish procedures for accessing data and recordings.
 - 1. These procedures should include the process to obtain written authorization for access to non-public data by CGPD members and members of other governmental entities and agencies.
- (c) Establishing procedures for logging or auditing access.
- (d) Establishing procedures for transferring, downloading, tagging, or making events.
- (e) Establishing an inventory of portable recordings including:
 - 1. Total number of devices owned or maintained by the CGPD.
 - 2. Daily record of the total number deployed and used by members.
 - 3. Total amount of recorded audio and video data collected by the devices and maintained by the CGPD
- (f) Preparing the biennial audit required by Minn. Stat. 13.825, Subd. 9.
- (g) Notifying the Bureau of Criminal Apprehension (BCA) on time when new equipment is obtained by the CGPD that expands the type or scope of surveillance capabilities of the CGPD portable recorders.
- (h) Ensuring that the Portable Audio/Video Recorders Policy is posted on the CGPD public website.

Members Privacy Expectations:

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

Members Responsibilities:

All officers who choose to wear an assigned portable recording system shall wear and operate the system in compliance with the CGPD policy adopted under 13.825, while performing law enforcement activities under the command and control of another chief law enforcement officer or federal law enforcement official.

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

Any member assigned to a non-uniformed position or administrative position may carry an approved portable recording at any time the member believes that such a device may be useful.

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

Activation of the audio/video recorder:

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

- 1. All enforcement and investigative contacts including traffic stops and field interviews.
- 2. Self-initiated activity.
- 3. Any contact that may or has the potential to become adversarial.

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

At no time is a member expected to jeopardize their safety to activate a portable recorder.

Stopping of Recording:

Once activated a portable recorder should remain on until the incident is complete. Recordings may be stopped during inactivity from the incident.

Surreptitious Recordings:

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

Prohibited Use of Audio/Video Recorders:

Members may not use department-issued portable recorders for personal use. Members shall not use devices for embarrassment, harassment, or ridicule.

Members are not allowed to use personally owned portable recording devices.

Retention of Recordings:

- a. 90 days minimum for ALL video, including accidental or test recordings
- b. 1 year a) reportable firearms discharge (i.e., any discharge not for training or dispatching an injured animal); b) use of force by an officer resulting in substantial bodily harm; c) a formal complaint is made against an officer related to the incident.
- c. "Indefinite" data documenting an officer's use of deadly force.
- d. Up to an additional 180 days (beyond the scheduled expiration date) when so requested in writing by a data subject.
- e. CGPD explicitly prohibit "altering, erasing, or destroying any recording made with a peace officer's portable recording system or data or metadata related to the recording prior to the expiration of the applicable retention period.

Release of Recordings:

Unless for purposes and or authorization from the courts, the release of all recordings will only be done following Minnesota Private Data Request laws (Minn. Stat. 13). All recordings are considered private.

Confidential recordings: All recordings collected as part of a criminal investigation is confidential. Outside of court proceedings or court orders, this information will not be released.

Public recordings: Following are examples of public information unless sealed by the courts.

- 1. Recordings documenting the discharge of a firearm by a peace officer in the course of their duties, other than for training or dispatching an animal that is sick, injured, or dangerous.
- 2. Recordings to document the use of force by a peace officer resulting in bodily harm.
- 3. Recording that a subject requests to be made accessible to the public, subject to redaction. Recording of any subject, other than a peace officer, who has consented to public release must be redacted.
- 4. Any recording of undercover officers must be redacted.

- 5. Any person captured in a recording may have access to the recording. If the individual requests a copy of the recording and does not have consent of other non-law enforcement individuals captured on the recording, the identity of those individuals must be blurred or obscured sufficiently to render the subject unidentifiable before release. The identity of on-duty peace offices may not be obscured unless their identity is protected under Minn. Stat. 13.82, Subd. 17.
- 6. If another provision of the Data Practices Act classifies data as private or otherwise not public, the data retains that other classification. An example of this would be the protection of certain victims, witnesses, and others (Minn Stat. 13.82 subd. 17).

Access to Recordings by Non-Employees:

All requests by non-employees, media, or the public seeking access to BWC recordings are to be directed to the Chief of Police who shall process the request following Minn. Stat. 13 Data Practices laws.

Death Resulting from Use of Force-Release of Public Data:

Notwithstanding section Minn. Stat. 13.82, Subd 7, when an individual dies as a result of a use of force by a peace officer, an involved officer's law enforcement agency must allow the following individuals, upon their request, to inspect all portable recording system data, redacted no more than what is required by law, documenting the incident within five days of the request, subject to paragraph (c) and (d):

- 1. The deceased individual's next of kin;
- 2. The legal representative of the deceased individual's next of kin; and
- 3. The other parent of the deceased individual's child.
- (c) A law enforcement agency may deny a request to inspect portable recording system data under paragraph (b) if the agency determines that there is a compelling reason that inspection would interfere with an active investigation. If the agency denies access under the paragraph, the chief law enforcement officer must provide a prompt, written denial to the individual in paragraph (b) who requested the data with a short description of the compelling reason access was denied and must provide notice that relief may be sought from the district court according to section 13.82, subdivision 7.
- (d) When an individual dies as a result of a use of force by a peace officer, an involved officer's law enforcement agency shall release all portable recording system data, redacted no more than what is required by law, documenting the incident no later than 14 days after the incident, unless the chief law enforcement officer asserts in writing that the public classification would interfere with an ongoing investigation, in which case the data remain classified by section 13.82, subdivision 7.

Identification and Preservation of Recordings:

All downloads from the device will be done by the Chief of Police and marked in such a way that the information will be easily found if needed. Marking may include the following:

- 1. Criminal or civil matter.
- 2. Non-disclosure request by the victim, witness, or complainant.
- 3. Potential dangers if the recording is released.
- 4. Disclosure be a violation of someone's privacy
- 5. Medical or mental health information is contained.
- 6. Disclosure may compromise an undercover officer or confidential informant.
- 7. The recording or portions of the recording may be protected under the Minnesota Data Practices Act.

Review of Recorded Media Files:

Members may review their recordings as a resource when writing their reports or before testing in court proceedings. However, members are not allowed to keep personal copies of the recordings. Also, members are not to use the fact that there is a recording to write a less detailed report.

Recorded files may be reviewed as part of an internal audit and review (Minn. Stat 626.8473).

Recorded files may be reviewed as part of a personnel complaint, administrative investigation, or criminal investigation by the Chief of Police.

According to lawful process or by court personnel who are otherwise authorized to review evidence in a related case.

By the media with permission of the Chief of Police as long as no other data practice issues are subject to the review.

In compliance with the Minnesota Data Practices Act request, if permitted or required by the Act, including according to Minn. Stat. 13.82, Subd. 15.

The Chief of Police will review the recordings of each device randomly periodically and also audit history and compare information detailed in written reports.

Use of BWC while acting under the directions of another law enforcement entity:

Officers will follow their own agency's BWC policy when acting under the command and control of another CLEO or federal officer.

Sharing of BWC material with other law enforcement agencies:

BWC data is shared with other LE agencies only for legitimate purposes that are documented in writing at the time of the request. Prior to sharing any BWC data, Prior to the release of any WC material CGPD will recieve a written request and will retain a record of that written request, as well as documenting in some fashion the receiving agency's acknowledgment that they are, essentially, required to treat any BWC they receive from CGPD as if it were their own BWC data.

Any member who violates any part of this policy is subject to discipline action and/or criminal prosecution.