



INDEPENDENT AUDITOR'S REPORT

Plainview Police Department



JUNE 6TH, 2024
RAMPART AUDIT LLC

Audit Overview and Recommendations

Dear Plainview City Council and Chief Timm:

We have audited the body-worn camera (BWC) program of the Plainview Police Department (PPD) for the two-year period ended 2/14/2024. Minnesota Statute §13.825 mandates that any law enforcement agency operating a portable recording system (PRS)¹ program obtain an independent, biennial audit of its program. This program and its associated data are the responsibility of the Plainview Police Department. Our responsibility is to express an opinion on the operations of this program based on our audit.

On February 26, 2024, Rampart Audit LLC (Rampart) met with Chief Jason Timm, who provided information about PPD's BWC program policies, procedures and operations. Also present was police technical specialist Andrea McGraw, who is involved in the day-to-day operations of the BWC program. 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 PPD's recordkeeping.

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

PPD 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 Timm identified documentation showing that the public notification, comment and meeting requirements had been satisfied prior to the implementation of PPD's BWC program on January 5, 2022. Specifically, Chief Timm identified the following:

1. City of Plainview October 12, 2021, Meeting Minutes
2. Facebook Police Department post December 9, 2021
3. Facebook City of Plainview post December 9, 2021

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 PPD, these terms may be used interchangeably in this report.

4. City of Plainview December 14, 2021, Meeting Agenda Posted on Facebook and the city website
5. City of Plainview December 14, 2021, Meeting Notes

Rampart was able to obtain copies of each of the items Chief Timm identified. The October 12, 2021, Plainview City Council Meeting minutes included quotes for the Getac BWC system ultimately implemented by PPD, as well as discussion about the necessity of such systems. We noted that the December 9, 2021, City of Plainview Facebook post was a share of Plainview PD's post on that same date, which described the agency's intent to implement a body-worn camera program and invited the public to submit comments via mail or email, or in person at the December 14, 2021, Plainview City Council Meeting. We noted that the December 14, 2021, Meeting Agenda included an item titled "Police Department Body Worn Camera Public Comment," while the corresponding Meeting Notes described Chief Timm's presentation to the city council, which included the public hearing and public comment requirements prior to implementation.

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

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

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

PPD BWC WRITTEN POLICY

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

PPD BWC Data Retention

Plainview Police Department's BWC policy states that: "[a]ll recordings shall be retained for a period consistent with the requirements of the organization's records retention schedule but in no event for a period less than 90 days." PPD's records retention policy also specifies a minimum retention period of 90 days; however, Chief Timm advised Rampart that all BWC recordings are retained for a minimum of six months.

Minn. Stat. §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. PPD's records retention schedule addresses each of these categories of data and assigns the statutorily-required retention period.

PPD's records retention schedule also addresses the requirement contained in Minn. Stat. §13.825 Subd. 3(d) that an agency retain BWC recordings for an additional period of up to 180 days when so requested in writing by a data subject.

PPD's BWC policy states that "[m]embers shall not alter, erase, or destroy any BWC recordings before the end of the applicable records retention period." In our opinion, this satisfies the requirements of Clause 2 of the Policy section noted above.

PPD currently employs Getac body-worn cameras, though Chief Timm advised us that the agency is planning to switch to Axon body-worn cameras due to issues with the battery life of the Getac cameras. All BWC data are stored on iCrimeFighter's cloud service.

PPD manages BWC data retention automatically, based on the data classification assigned to each video at the time of upload. If an officer fails to assign a data classification, the default retention period is 90 days.

PPD's BWC policy states that each officer using a BWC "should download, tag or mark the recordings in accordance with procedure and document the existence of the recording in any related case report." Chief Timm advised that PPD utilizes both an automated upload feature as well as physical docking capabilities.

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

PPD BWC Data Destruction

As discussed above, Plainview Police Department's BWC data are stored on iCrimeFighter's cloud-based service, with data retention and deletion schedules managed automatically based on the assigned data classification of each video.

iCrimeFighter is hosted on Amazon Web Services (AWS) GovCloud. AWS describes its GovCloud service as offering "secure cloud solutions that comply with... the DOJ's [Department of Justice] Criminal Justice

Information Systems (CJIS) Security Policy...” as well as providing further detail about specific security protocols available to its customers.

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

PPD BWC Data Access

Chief Timm advised us that that all requests from the public, media or other law enforcement agencies are made to him in writing, normally via email. PPD’s BWC policy states that requests for BWC data shall be processed “in accordance with the MGDPA [Minnesota Government Data Practices Act] and other governing laws.” Upon Chief Timm’s reviewal and authorization, Administrator McGraw is responsible for completing the request. BWC data is provided to the recipient on DVD.

As discussed in Clauses 5 and 6 of the Policy section of this report, the Minnesota State Legislature in 2023 added specific access requirements related to BWC data that document deadly force incidents, and specified that these requirements must be included in the agency’s BWC policy. At the time of our audit, PPD had not revised its BWC policy to address these requirements.

PPD’s BWC policy also 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.” PPD maintains a copy of each such request it receives. In addition, BWC data “shall be made available to prosecutors, courts, and other criminal justice entities as provided by law.” Chief Timm indicated that PPD obtains a written acknowledgment of the receiving agency’s obligations under §13.825 Subd. 7 and Subd. 8, which include a requirement to maintain BWC data security. The Plainview City Attorney and Wabasha County Attorney also submit email requests for BWC data via email and receive video via DVD.

In our opinion, PPD’s written BWC policy is compliant with respect to the applicable data access requirements, with the following exceptions:

1. The BWC policy must state 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, unless 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.

2. The BWC policy must state 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.

These requirements were newly added in 2023 by the Minnesota State Legislature. Prior to the issuance of this report, PPD submitted a revised BWC policy that addresses the exceptions noted above. In our opinion, this revised BWC policy is compliant with respect to the applicable data access requirements.

PPD BWC Data Classification

PPD's BWC Policy states that "BWC data is presumptively private," and further states that "BWC recordings are classified as private data about the data subjects unless there is a specific law that provides differently." Active criminal investigation data are classified as confidential. PPD BWC Policy also identifies certain categories of BWC data that are public.

As noted in the preceding section, prior to the issuance of this report, PPD submitted a revised BWC policy that addresses the changes the Minnesota State Legislature made in 2023 regarding BWC data documenting incidents involving the use of deadly force. In our opinion, this revised policy is compliant with respect to the applicable data classification requirements.

PPD BWC Internal Compliance Verification

The PPD BWC Review of Recorded Media section states that BWC recordings may be reviewed "[b]y a supervisor as part of internal audits and reviews as required by Minn. Stat. §626.8473."

Chief Timm advised us that Administrator McGraw conducts a random review of BWC recordings to ensure compliance with policy. Logs are maintained of all such reviews.

PPD's BWC policy states that "[p]rior to going into service, uniformed members will be responsible for making sure that they are equipped with a portable recorder issued by the Department, and that the recorder is in good working order..."

The 2023 legislative changes require that an agency's BWC policy must specify that an officer assigned a BWC must 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. While the wording in PPD's BWC policy appears to be sufficiently broad to cover such scenarios, we recommend adding language to make this requirement explicit.

Prior to the issuance of this report, PPD submitted a revised version of their BWC policy adding the language described in the preceding paragraph. A copy of the revised policy is attached to this report as Appendix B.

Section 403.7 Prohibited Use of Audio/Video Recorders contains language stating that “[m]embers are prohibited from using personally owned recording devices while on-duty without the express consent of the XXX.” Chief Timm advised us that no personally-owned devices are permitted for use as BWCs, and that each officer has an agency-issued cellular phone that could be utilized as a BWC in an emergency. This passage appears to be an artifact of the standard Lexipol policy. We strongly recommend removing it and adding language specifically prohibiting the use of personally-owned devices as BWCs.

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

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

PPD BWC Program and Inventory

PPD currently possesses nine (9) Getac body-worn cameras, though, as noted earlier in this report, plans are in place to transition to Axon BWCs in the future.

The PPD 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.

PPD’s BWC policy states that “[u]niformed members should wear the recorder in a conspicuous manner at or above the mid-line of the waist.” This satisfies the requirement described in Clause 3 of the Policy section of this report.

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

As of the audit date, February 6, 2024, PPD maintained approximately 909.16 GB of BWC data.

PPD BWC Physical, Technological and Procedural Safeguards

PPD BWC data are initially recorded to a hard drive in each officer’s BWC. The Getac cameras are capable of wireless uploading, though PPD also maintains a physical docking station as a backup. BWC data are uploaded to iCrimeFighter’s cloud-based storage service. In the event an officer fails to label a video, the default retention period is permanent to avoid the accidental loss of data.

Officers have view-only access to their own data for report writing, trial preparation, data administration, investigatory purposes and other legitimate law enforcement purposes. All BWC data access is logged automatically and available for audit purposes.

Enhanced Surveillance Technology

PPD currently employs BWCs with only standard audio/video recording capabilities. While PPD currently has plans to replace their Getac cameras with Axon body-worn cameras, 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 PPD 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 PPD records.

Audit Conclusions

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

Daniel E. Gazelka

Daniel E. Gazelka

Rampart Audit LLC

06/06/2024

APPENDIX A:

Policy 403 Plainview Police Department Law Enforcement Policy Manual Copyright Lexipol, LLC 2024/01/25, All Rights Reserved. Published with permission by Plainview Police Department Portable Audio/Video Recorders - 1 Portable Audio/Video Recorders 403.1 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, hand-held, or integrated into portable equipment. This policy does not apply to mobile audio/video recordings, interviews, or interrogations conducted at any Plainview Police Department facility, undercover operations, wiretaps, or eavesdropping (concealed listening devices). 403.1.1 DEFINITIONS Definitions related to this policy include: 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. 403.2 POLICY The Plainview 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. 403.3 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. 1. 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 procedures comply with requirements of the Minnesota Government Data Practices Act (MGDPA) and other applicable laws (Minn. Stat. § 13.01 et seq.) (see the Protected Information and the Records Maintenance and Release policies). 2. The coordinator should work with the Custodian of Records to identify recordings that must be retained for a specific time frame under Minnesota law (e.g., firearm discharges, certain use of force incidents, formal complaints). (b) Establishing procedures for accessing data and recordings. Plainview Police Department Law Enforcement Policy Manual Portable Audio/Video Recorders Copyright Lexipol, LLC 2024/01/25, All Rights Reserved. Published with permission by Plainview Police Department Portable Audio/Video Recorders - 2 1. These procedures should include the process to obtain written authorization for access to non-public data by PPD 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 marking events. (e) Establishing an inventory of portable recorders including: 1. Total number of devices owned or maintained by the Plainview Police Department. 2. Daily record of the total number deployed and used by members and, if applicable, the precinct or district in which the devices were used. 3. Total amount of recorded audio and video data collected by the devices and maintained by the Plainview Police Department. (f) Preparing the biennial audit required by Minn. Stat. § 13.825, Subd. 9. (g) Notifying the Bureau of Criminal Apprehension (BCA) in a timely manner when new equipment is obtained by the Plainview Police Department that expands the type or scope of surveillance capabilities of the department's portable recorders. (h) Ensuring that this Portable Audio/Video Recorders Policy is posted on the Department website. 403.4 MEMBER PRIVACY EXPECTATION All recordings made by members on any department-issued device at any time or while acting in an official capacity of this department, regardless of ownership of the device, shall remain the

property of the Department. Members shall have no expectation of privacy or ownership interest in the content of these recordings. 403.5 MEMBER RESPONSIBILITIES Prior to going into service, uniformed members will be responsible for making sure that they are equipped with a portable recorder issued by the Department, and that the recorder is in good working order (Minn. Stat. § 13.825). If the recorder is not in working order or the member 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 wear the recorder in a conspicuous manner at or above the mid-line of 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 may carry an approved portable recorder at any time the member believes that such a device may be useful. Unless conducting a lawful recording in an authorized undercover capacity, non-uniformed members should wear the recorder in a conspicuous manner when in use or otherwise notify persons that they are being recorded, whenever reasonably practicable. Plainview Police Department Law Enforcement Policy Manual Portable Audio/Video Recorders Copyright Lexipol, LLC 2024/01/25, All Rights Reserved. Published with permission by Plainview Police Department Portable Audio/Video Recorders - 3 When using a portable recorder, the assigned member shall record their name, employee number, and the current date and time at the beginning and the end of the shift or other period of use, regardless of whether any activity was recorded. This procedure is not required when the recording device and related software captures the user's unique identification and the date and time of each recording. Members should document the existence of a recording in any report or other official record of the contact, including any instance where the recorder malfunctioned or the member deactivated the recording (Minn. Stat. § 626.8473). Members should include the reason for deactivation. 403.6 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 any time the member believes it would be appropriate or valuable to record an incident. The recorder should be activated in any of the following situations: (a) All enforcement and investigative contacts including stops and field interview (FI) situations (b) Traffic stops including, but not limited to, traffic violations, stranded motorist assistance and all crime interdiction stops (c) Self-initiated activity in which a member would normally notify Dispatch (d) Any other contact that becomes adversarial after the initial contact in a situation that would not otherwise require recording Members should remain sensitive to the dignity of all individuals being recorded and exercise sound discretion to respect privacy by discontinuing recording whenever it reasonably appears to the member that such privacy may outweigh any legitimate law enforcement interest in recording. Requests by members of the public to stop recording should be considered 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 his/her safety in order to activate a portable recorder or change the recording media. However, the recorder should be activated in situations described above as soon as reasonably practicable. 403.6.1 CESSATION OF RECORDING Once activated, the portable recorder should remain on continuously until the member reasonably believes that his/her direct participation in the incident is complete or the situation no longer fits the criteria for activation. Recording may be stopped during significant periods of inactivity such as report writing or other breaks from direct participation in the incident. Plainview Police Department Law Enforcement Policy Manual Portable Audio/Video Recorders Copyright Lexipol, LLC 2024/01/25, All Rights Reserved. Published with permission by Plainview Police Department Portable Audio/Video Recorders - 4 403.6.2 SURREPTITIOUS RECORDINGS

Minnesota law permits an individual to surreptitiously record any conversation in which one party to the conversation has given his/her permission (Minn. Stat. § 626A.02). Members of the Department may surreptitiously record any conversation during the course of a criminal investigation in which the member reasonably believes that such a recording will be lawful and beneficial to the investigation. Members shall not surreptitiously record another department member without a court order unless lawfully authorized by the Chief of Police or the authorized designee.

403.6.3 EXPLOSIVE DEVICE Many portable recorders, including body-worn cameras and audio/video transmitters, emit radio waves that could trigger an explosive device. Therefore, these devices should not be used where an explosive device may be present.

403.7 PROHIBITED USE OF AUDIO/VIDEO RECORDERS Members are prohibited from using department-issued portable recorders and recording media for personal use and are prohibited from making personal copies of recordings created while on duty or while acting in their official capacity. Members are also prohibited from retaining recordings of activities or information obtained while on-duty, whether the recording was created with department-issued or personally owned recorders. Members shall not duplicate or distribute such recordings, except for authorized legitimate department business purposes. All such recordings shall be retained at the Department. Members are prohibited from using personally owned recording devices while on-duty without the express consent of the XXX. Any member who uses a personally owned recorder for department related activities shall comply with the provisions of this policy, including retention and release requirements and should notify the on-duty supervisor of such use as soon as reasonably practicable. Recordings shall not be used by any member for the purpose of embarrassment, harassment or ridicule.

403.8 RETENTION OF RECORDINGS All recordings shall be retained for a period consistent with the requirements of the organization's records retention schedule but in no event for a period less than 90 days. If an individual captured in a recording submits a written request, the recording shall be retained for an additional time period. The coordinator should be responsible for notifying the individual prior to destruction of the recording (Minn. Stat. § 13.825). Members shall not alter, erase, or destroy any recordings before the end of the applicable records retention period (Minn. Stat. § 626.8473).

Plainview Police Department Law Enforcement Policy Manual Portable Audio/Video Recorders Copyright Lexipol, LLC 2024/01/25, All Rights Reserved. Published with permission by Plainview Police Department

Portable Audio/Video Recorders - 5

403.8.1 RELEASE OF AUDIO/VIDEO RECORDINGS Requests for the release of audio/video recordings shall be in accordance of policy

403.8.2 "Access to Recordings.

403.8.2 ACCESS TO RECORDINGS Except as provided by Minn. Stat. § 13.825, Subd. 2, audio/video recordings are considered private or nonpublic data.

A. Data subjects. Under Minnesota law, the following are considered data subjects for purposes of administering access to BWC data: (a) Any person or entity whose image or voice is documented in the data. (b) The officer who collected the data. (c) Any other officer whose voice or image is documented in the data, regardless of whether that officer is or can be identified by the recording.

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:

- (a) 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.
- (b) Data that

documents the use of force by a peace officer that results in substantial bodily harm. (c) 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. Data that documents the final disposition of a disciplinary action against a public employee. (d) 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. Plainview Police Department Law Enforcement Policy Manual Portable Audio/Video Recorders Copyright Lexipol, LLC 2024/01/25, All Rights Reserved. Published with permission by Plainview Police Department Portable Audio/Video Recorders - 6 E. Access to BWC data by non-employees. Officers shall refer members of the media or public seeking access to BWC data to , 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. 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: (a) Officers may access and view stored BWC video only when there is a business need for doing so, including the need to defend against an allegation of misconduct or substandard performance. Officers may review video footage of an incident in which they were involved prior to preparing a report, giving a statement, or providing testimony about the incident. (b) Agency personnel 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. (c) Employees seeking access to BWC data for non-business reasons may make a request for it in the same manner as any member of the public. 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, Plainview Police Department Law Enforcement Policy Manual Portable Audio/Video Recorders Copyright Lexipol, LLC 2024/01/25, All Rights Reserved. Published with permission by Plainview Police Department Portable Audio/Video Recorders - 7 (a) BWC data may be shared with other law enforcement agencies only for legitimate law enforcement purposes that are documented in writing at the time of the disclosure. All written requests shall be made through the requestor's government email. (b) BWC data

shall be made available to prosecutors, courts, and other criminal justice entities as provided by law. All requests must be in writing and shall be made through the requestor's government email. 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 the 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 prior to release. The identity of on-duty peace officers may not be obscured unless their identity is protected under Minn. Stat. § 13.82, Subd. 17.

403.9 IDENTIFICATION AND PRESERVATION OF RECORDINGS To assist with identifying and preserving data and recordings, members should download, tag or mark the recordings in accordance with procedure and document the existence of the recording in any related case report. A member should transfer, tag or mark recordings when the member reasonably believes: (a) The recording contains evidence relevant to potential criminal, civil or administrative matters. (b) A complainant, victim or witness has requested non-disclosure. (c) A complainant, victim or witness has not requested non-disclosure but the disclosure of the recording may endanger the person. (d) Disclosure may be an unreasonable violation of someone's privacy. (e) Medical or mental health information is contained. (f) Disclosure may compromise an under-cover officer or confidential informant. (g) The recording or portions of the recording may be protected under the Minnesota Data Practices Act. Any time a member reasonably believes a recorded contact may be beneficial in a non-criminal matter (e.g., a hostile contact), the member should promptly notify a supervisor of the existence of the recording.

403.10 REVIEW OF RECORDED MEDIA FILES When preparing written reports, members should review their recordings as a resource (see the Officer-Involved Shootings and Deaths Policy for guidance in those cases). However, members shall not retain personal copies of recordings. Members should not use the fact that a recording was made as a reason to write a less detailed report. Supervisors are authorized to review relevant recordings any time they are investigating alleged misconduct or reports of meritorious conduct or whenever such recordings would be beneficial in reviewing the member's performance.

Plainview Police Department Law Enforcement Policy Manual Portable Audio/Video Recorders Copyright Lexipol, LLC 2024/01/25, All Rights Reserved. Published with permission by Plainview Police Department Portable Audio/Video Recorders - 8 Recorded files may also be reviewed: (a) By a supervisor as part of internal audits and reviews as required by Minn. Stat. § 626.8473. (b) Upon approval by a supervisor, by any member of the Department who is participating in an official investigation, such as a personnel complaint, administrative investigation, or criminal investigation. (c) Pursuant to lawful process or by court personnel who are otherwise authorized to review evidence in a related case. (d) By media personnel with permission of the Chief of Police or the authorized designee. (e) In compliance with the Minnesota Data Practices Act request, if permitted or required by the Act, including pursuant to Minn. Stat. § 13.82, Subd. 15, and in accordance with the Records Maintenance and Release Policy. All recordings should be reviewed by the Custodian of Records prior to public release (see the Records Maintenance and Release Policy). Recordings that are clearly offensive to common sensibilities should not be publicly released unless disclosure is required by law or order of the court (Minn. Stat. § 13.82, Subd. 7; Minn. Stat. § 13.825, Subd. 2).

403.11 ACCOUNTABILITY Any member who accesses or releases recordings without authorization may be subject to discipline (per union contract), (see the Standards of Conduct and the Protected Information policies), (Minn. Stat. § 626.8473).

403.12 AGENCY AUDIT / COMPLIANCE The CLEO or designee will review BWC recordings of each recording device/officer randomly on a weekly basis. The CLEO or designee will randomly audit the history of BWC files to insure that no unauthorized

Rampart Audit, LLC

downloading or viewing took place. In the event of a violation, the violator will be disciplined in accordance to policy 403.11.

APPENDIX B:

Policy 403 Plainview Police Department Law Enforcement Policy Manual Portable Audio/Video Recorders 403.1 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, hand-held, or integrated into portable equipment. This policy does not apply to mobile audio/video recordings, interviews, or interrogations conducted at any Plainview Police Department facility, undercover operations, wiretaps, or eavesdropping (concealed listening devices).

403.1.1 DEFINITIONS Definitions related to this policy include: 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.

403.2 POLICY The Plainview 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.

403.3 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.
 1. 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 procedures comply with requirements of the Minnesota Government Data Practices Act (MGDPA) and other applicable laws (Minn. Stat. § 13.01 et seq.) (see the Protected Information and the Records Maintenance and Release policies).
 2. The coordinator should work with the Custodian of Records to identify recordings that must be retained for a specific time frame under Minnesota law (e.g., firearm discharges, certain use of force incidents, formal complaints).
- (b) Establishing procedures for accessing data and recordings. Copyright Lexipol, LLC 2024/05/08, All Rights Reserved. Published with permission by Plainview Police Department Portable Audio/Video Recorders - 193 Plainview Police Department Law Enforcement Policy Manual Law Enforcement Policy Manual Portable Audio/Video Recorders
1. These procedures should include the process to obtain written authorization for access to non-public data by PPD 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 marking events.
- (e) Establishing an inventory of portable recorders including:
 1. Total number of devices owned or maintained by the Plainview Police Department.
 2. Daily record of the total number deployed and used by members and, if applicable, the precinct or district in which the devices were used.
 3. Total amount of recorded audio and video data collected by the devices and maintained by the Plainview Police Department.
- (f) Preparing the biennial audit required by Minn. Stat. § 13.825, Subd. 9.
- (g) Notifying the Bureau of Criminal Apprehension (BCA) in a timely manner when new equipment is obtained by the Plainview Police Department that expands the type or scope of surveillance capabilities of the department's portable recorders.
- (h) Ensuring that this Portable Audio/Video Recorders Policy is posted on the Department website.

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

403.5 MEMBER

RESPONSIBILITIES All officers assigned a portable recording system shall wear and operate the system in compliance with the Plainview Police Department's 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 will be responsible for making sure that they are equipped with a portable recorder issued by the Department, and that the recorder is in good working order (Minn. Stat. § 13.825). If the recorder is not in working order or the member 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 wear the recorder in a conspicuous manner at or above the mid-line of 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 may carry an approved portable recorder at any time the member believes that such a device may be useful. Unless conducting a lawful recording in an authorized undercover capacity, non-uniformed members should wear the recorder in a conspicuous manner when in use or otherwise notify persons that they are being recorded, whenever reasonably practicable. When using a portable recorder, the assigned member shall record their name, employee number, and the current date and time at the beginning and the end of the shift or other period of use, regardless of whether any activity was recorded. This procedure is not required when the recording device and related software captures the user's unique identification and the date and time of each recording. Members should document the existence of a recording in any report or other official record of the contact, including any instance where the recorder malfunctioned or the member deactivated the recording (Minn. Stat. § 626.8473). Members should include the reason for deactivation.

403.6 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 any time the member believes it would be appropriate or valuable to record an incident. The recorder should be activated in any of the following situations: (a) All enforcement and investigative contacts including stops and field interview (FI) situations (b) Traffic stops including, but not limited to, traffic violations, stranded motorist assistance and all crime interdiction stops (c) Self-initiated activity in which a member would normally notify Dispatch (d) Any other contact that becomes adversarial after the initial contact in a situation that would not otherwise require recording. Members should remain sensitive to the dignity of all individuals being recorded and exercise sound discretion to respect privacy by discontinuing recording whenever it reasonably appears to the member that such privacy may outweigh any legitimate law enforcement interest in recording. Requests by members of the public to stop recording should be considered 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 his/her safety in order to activate a portable recorder or change the recording media. However, the recorder should be activated in situations described above as soon as reasonably practicable.

403.6.1 CESSATION OF RECORDING Once activated, the portable recorder should remain on continuously until the member reasonably believes that his/her direct participation in the incident is complete or the situation no longer fits the criteria for activation. Recording may be stopped during significant periods of inactivity such as report writing or other breaks from direct participation in the incident. Copyright Lexipol, LLC 2024/05/08, All Rights Reserved.

Published with permission by Plainview Police Department Portable Audio/Video Recorders - 195 Plainview Police Department Law Enforcement Policy Manual Law Enforcement Policy Manual Portable Audio/Video Recorders 403.6.2 SURREPTITIOUS RECORDINGS Minnesota law permits an individual to surreptitiously record any conversation in which one party to the conversation has given his/her permission (Minn. Stat. § 626A.02). Members of the Department may surreptitiously record any conversation during the course of a criminal investigation in which the member reasonably believes that such a recording will be lawful and beneficial to the investigation. Members shall not surreptitiously record another department member without a court order unless lawfully authorized by the Chief of Police or the authorized designee. 403.6.3 EXPLOSIVE DEVICE Many portable recorders, including body-worn cameras and audio/video transmitters, emit radio waves that could trigger an explosive device. Therefore, these devices should not be used where an explosive device may be present. 403.7 PROHIBITED USE OF AUDIO/VIDEO RECORDERS Members are prohibited from using department-issued portable recorders and recording media for personal use and are prohibited from making personal copies of recordings created while on duty or while acting in their official capacity. Members are also prohibited from retaining recordings of activities or information obtained while on-duty, whether the recording was created with department-issued or personally owned recorders. Members shall not duplicate or distribute such recordings, except for authorized legitimate department business purposes. All such recordings shall be retained at the Department. Members are prohibited from using personally owned recording devices while on-duty without the express consent of the XXX. Any member who uses a personally owned recorder for department related activities shall comply with the provisions of this policy, including retention and release requirements and should notify the on-duty supervisor of such use as soon as reasonably practicable. Recordings shall not be used by any member for the purpose of embarrassment, harassment or ridicule. 403.8 RETENTION OF RECORDINGS See policy 802 for retention guidelines. 403.8.1 RELEASE OF AUDIO/VIDEO RECORDINGS Requests for the release of audio/video recordings shall be in accordance of policy 403.8.2 "Access to Recordings. 403.8.2 ACCESS TO RECORDINGS Except as provided by Minn. Stat. § 13.825, Subd. 2, audio/video recordings are considered private or nonpublic data. Copyright Lexipol, LLC 2024/05/08, All Rights Reserved. Published with permission by Plainview Police Department Portable Audio/Video Recorders - 196 Plainview Police Department Law Enforcement Policy Manual Law Enforcement Policy Manual Portable Audio/Video Recorders A. Data subjects. Under Minnesota law, the following are considered data subjects for purposes of administering access to BWC data: (a) Any person or entity whose image or voice is documented in the data. (b) The officer who collected the data. (c) Any other officer whose voice or image is documented in the data, regardless of whether that officer is or can be identified by the recording. 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: (a) 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. (b) Data that documents the use of force by a peace officer that results in substantial bodily harm. (c) 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. Data that documents the final disposition of a disciplinary action against a public employee. (d) 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 responsible authority/data practices designee], 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. Copyright Lexipol, LLC 2024/05/08, All Rights Reserved. Published with permission by Plainview Police Department Portable Audio/Video Recorders - 197 Plainview Police Department Law Enforcement Policy Manual Law Enforcement Policy Manual Portable Audio/Video Recorders 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: (a) Officers may access and view stored BWC video only when there is a business need for doing so, including the need to defend against an allegation of misconduct or substandard performance. Officers may review video footage of an incident in which they were involved prior to preparing a report, giving a statement, or providing testimony about the incident. (b) Agency personnel shall document their reasons for accessing stored BWC data in the program audit note file of the specific recording or written log 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. (c) Employees seeking access to BWC data for non-business reasons may make a request for it in the same manner as any member of the public. 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, (a) BWC data may be shared with other law enforcement agencies only for legitimate law enforcement purposes that are documented in writing at the time of the disclosure. All written requests shall be made through the requestor's government email and shall acknowledge their responsibilities under 13.825 Subd 7 and 8 in the email request. (b) BWC data shall be made available to prosecutors, courts, and other criminal justice entities as provided by law. All requests must be in writing and shall be made through the requestor's government email. Copyright Lexipol, LLC 2024/05/08, All Rights Reserved. Published with

permission by Plainview Police Department Portable Audio/Video Recorders - 198 Plainview Police Department Law Enforcement Policy Manual Law Enforcement Policy Manual Portable Audio/Video Recorders 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 the 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 prior to release. The identity of on-duty peace officers may not be obscured unless their identity is protected under Minn. Stat. § 13.82, Subd. 17. H. Death Resulting from Force - Release of Public Data Notwithstanding section 13.82, subdivision 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 paragraphs (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 this 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 pursuant 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.

403.9 IDENTIFICATION AND PRESERVATION OF RECORDINGS To assist with identifying and preserving data and recordings, members should download, tag or mark the recordings in accordance with procedure and document the existence of the recording in any related case report. A member should transfer, tag or mark recordings when the member reasonably believes: (a) The recording contains evidence relevant to potential criminal, civil or administrative matters. (b) A complainant, victim or witness has requested non-disclosure. (c) A complainant, victim or witness has not requested non-disclosure but the disclosure of the recording may endanger the person. (d) Disclosure may be an unreasonable violation of someone's privacy. Copyright Lexipol, LLC 2024/05/08, All Rights Reserved. Published with permission by Plainview Police Department Portable Audio/Video Recorders - 199 Plainview Police Department Law Enforcement Policy Manual Law Enforcement Policy Manual Portable Audio/Video Recorders (e) Medical or mental health information is contained. (f) Disclosure may compromise an under-cover officer or confidential informant. (g) The recording or portions of the recording may be protected under the Minnesota Data Practices Act. Any time a member reasonably believes a recorded contact may be beneficial in a non-criminal matter (e.g., a hostile contact), the member should promptly notify a supervisor of the existence of the recording.

403.10 REVIEW OF RECORDED MEDIA FILES When preparing written reports, members should review their recordings as a resource (see the Officer-Involved Shootings and Deaths Policy for guidance in those cases). However, members shall not retain personal copies of recordings. Members should not use the fact that a recording was made as a reason to write a less detailed report. Supervisors are authorized to review relevant recordings any time they are investigating alleged misconduct or reports of meritorious

conduct or whenever such recordings would be beneficial in reviewing the member's performance. Recorded files may also be reviewed: (a) By a supervisor as part of internal audits and reviews as required by Minn. Stat. § 626.8473. (b) Upon approval by a supervisor, by any member of the Department who is participating in an official investigation, such as a personnel complaint, administrative investigation, or criminal investigation. (c) Pursuant to lawful process or by court personnel who are otherwise authorized to review evidence in a related case. (d) By media personnel with permission of the Chief of Police or the authorized designee. (e) In compliance with the Minnesota Data Practices Act request, if permitted or required by the Act, including pursuant to Minn. Stat. § 13.82, Subd. 15, and in accordance with the Records Maintenance and Release Policy. All recordings should be reviewed by the Custodian of Records prior to public release (see the Records Maintenance and Release Policy). Recordings that are clearly offensive to common sensibilities should not be publicly released unless disclosure is required by law or order of the court (Minn. Stat. § 13.82, Subd. 7; Minn. Stat. § 13.825, Subd. 2).

403.11 ACCOUNTABILITY Any member who accesses or releases recordings without authorization may be subject to discipline (per union contract), (see the Standards of Conduct and the Protected Information policies), (Minn. Stat. § 626.8473). Copyright Lexipol, LLC 2024/05/08, All Rights Reserved. Published with permission by Plainview Police Department Portable Audio/Video Recorders - 200 Plainview Police Department Law Enforcement Policy Manual Law Enforcement Policy Manual Portable Audio/Video Recorders

403.12 AGENCY AUDIT / COMPLIANCE The CLEO or designee will review BWC recordings of each recording device/officer randomly on a weekly basis. The CLEO or designee will randomly audit the history of BWC files to insure that no unauthorized downloading or viewing took place. In the event of a violation, the violator will be disciplined in accordance to policy 403.11.