



INDEPENDENT AUDITOR'S REPORT

Arlington Police Department



FEBRUARY 24TH, 2026
RAMPART AUDIT LLC

Audit Overview and Recommendations

Dear Arlington City Council and Chief Gerads:

We have audited the body-worn camera (BWC) program of the Arlington Police Department (APD) for the two-year period ended 12/31/2025. Minnesota Statute §13.825 mandates that any law enforcement agency operating a portable recording system (PRS)¹ program obtain an independent, biennial audit of its program. This program and its associated data are the responsibility of the Arlington Police Department. Our responsibility is to express an opinion on the operations of this program based on our audit.

On January 16, 2026, Rampart Audit, LLC (Rampart) met with Chief Glenn Gerads, who provided information about APD'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 APD's recordkeeping.

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

APD BWC Program Implementation and Authorization

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

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

Rampart previously audited APD's BWC program in 2024. As part of that audit, Chief Gerads advised us that APD's BWC program was already in place when he joined the agency in August of 2022. While he believed the program began operation sometime during the year 2020, he was unable to locate documentation to either confirm the exact start date, or to verify that the public notice and hearing requirements were met prior to the program's implementation.

At Rampart's recommendation, APD then conducted an after-the-fact public hearing to receive comments regarding the BWC program. Chief Gerads subsequently provided a copy of the hearing notice, which was posted on the Arlington Police Department page of the City of Arlington website. The

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

notice invited the public to submit comments about APD's BWC program electronically or via mail, or in person at a public hearing to be held during the July 1, 2024, Arlington City Council meeting. He also provided a copy of the minutes of the aforementioned meeting, documenting that public comments were solicited and a public hearing was held to discuss APD's BWC program.

Copies of these documents have been retained in Rampart's audit files. In our opinion, APD has taken appropriate after-the-fact steps to ensure the public was afforded an opportunity to comment on its BWC program.

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

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

APD BWC WRITTEN POLICY

As part of this audit, we reviewed APD'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 APD 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 were added as a result of 2023 legislation and will also be discussed separately below.

APD 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 APD'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 180 days." This exceeds the 90-day minimum retention period established in Minn. Stat. §13.825 Subd. 3(a) for all BWC data not subject to a longer retention period.

APD's BWC policy does not address retention periods for the data categories described in Minn. Stat. §13.825 Subd. 3(b). It does, however, incorporate by reference the General Records Retention Schedule for Minnesota Cities (GRRSMC). The GRRSMC specifies a retention period of one year for any reportable firearms discharge or any incident that results in a formal complaint against an officer. The GRRSMC prescribes a seven-year retention period for BWC data documenting "any incident in which force was used and supervisory review is completed according to department policy."

Prior to the completion of this report, APD furnished a revised BWC policy that includes the required retention period for the data categories listed in §13.825 Subd. 3(b). A copy of that revised policy is attached to this report as Appendix B.

The Retention of Recordings section of APD's BWC policy states: "[a]ll BWC recordings documenting an officer's use of deadly force must be maintained indefinitely. This is to include use of deadly force not resulting in the death of [a] subject," which satisfies the requirements of §13.825 Subd. 3(c).

This same section of APD's BWC policy addresses the requirement contained in §13.825 Subd. 3(d), specifying that when so requested, the requested BWC data will be maintained for an additional period of up to 180 days. We noted that this requirement was addressed in two separate paragraphs using similar but not identical language and setting slightly different retention requirements. We recommend removing one of these paragraphs in order to eliminate conflicts between the two.

APD's BWC policy also states that "[m]embers shall not alter, erase, or destroy any recordings before the end of the applicable records retention period," as described in Clause 2 of the Policy section of this report; however, it does not address any associated data or metadata. Prior to the completion of this report, APD submitted a revised BWC policy that addresses these additional elements.

APD employs Motorola V300 body-worn cameras and utilizes Motorola's CommandCentral cloud storage service. APD manages BWC data retention through automated retention settings in Motorola's VideoManager EL video management software. The retention period for each video is determined by the data classification assigned at the time of upload; however, this retention period can be adjusted as needed. Chief Gerads advised us that the upload process requires that the officer select a data category as a guard against the accidental loss of data.

APD's BWC policy states that "[e]ach Officer using a BWC is responsible for transferring or assuring the proper transfer of the data from his/her camera by the end of that Officer's shift," unless the officer is involved in an incident resulting in death or great bodily harm, in which case a supervisor is directed to take custody of the BWC and assume responsibility for transferring its data. The policy further states that "[o]fficers shall label the BWC data files at the time of video capture or transfer to storage..."

Chief Gerads advised us that the Motorola body-worn cameras utilize a physical docking station located at the Arlington Police Department.

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

APD BWC Data Destruction

As discussed above, APD's BWC data are stored on Motorola's cloud-based storage service, CommandCentral, with data retention and deletion schedules managed automatically through the VideoManager EL video management software based on the assigned data classification of each video.

Motorola describes its CommandCentral cloud service as CJIS compliant and notes that the service is routinely and automatically updated to maintain compliance.

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

APD BWC Data Access

Chief Gerads advised us that that all requests for BWC data from the public or media are made in writing using Arlington Police Department's BWC data request form, which can be submitted in-person, online or via email. This form is submitted to the Records Administrator. Requests are reviewed by Chief Gerads and, if approved, processed "in accordance with the MGDPA [Minnesota Government Data Practices Act] and other governing laws." Requests are primarily fulfilled via expiring internet link through CommandCentral, though USB media can also be used.

APD'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." Requests from other law enforcement agencies follow the same process described in the preceding paragraph. APD 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." Prosecutors and probation personnel follow the same procedure as other law enforcement personnel to request BWC data. Chief Gerads indicated that APD maintains verbal acknowledgments of any receiving agency's obligations under §13.825 Subd. 8, which include a requirement to maintain BWC data security. We recommend that APD consider obtaining such agreements in writing. Alternatively, when sending the internet link many agencies include a written disclaimer in the email reminding the receiving agency of its responsibilities to maintain BWC data security.

As discussed in Clauses 5 and 6 of the Policy section of this report, the Minnesota State Legislature in 2023 added specific access requirements related to BWC data that document deadly force incidents, and specified that these requirements must be included in the agency's BWC policy. These requirements are addressed in the Release of Audio/Video Recordings section of APD's BWC policy.

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

APD BWC Data Classification

APD's BWC Policy 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. APD BWC Policy also identifies certain categories of BWC data that are public.

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

APD BWC Internal Compliance Verification

The Compliance section of APD's BWC policy states that "[s]upervisors shall monitor for compliance with this policy," while the Department Use of Data section of the policy states that "[a]t least once a month, the Chief of Police will randomly review BWC usage by each Officer to ensure compliance with this policy. The Chief of Police will submit their findings and put information into a quarterly report that will be forwarded to the City Council," practices that Chief Gerads confirmed. All such reviews are logged in the VideoManager EL software. In addition, all access to BWC data is logged and supervisory personnel are able to monitor such access.

The Policy section of APD's BWC policy states that "[i]t is the policy of this Department to authorize and require the use of Department issued BWC's [sic]... and to administer BWC data as provided by law." The Use and Documentation section states that "[o]fficers will use only Department issued BWC's [sic] in the performance of official duties for this Department or when otherwise performing authorized law enforcement services as an employee of this Department."

As discussed in Clause 4 of the Policy section of this report, the 2023 legislative changes require that an agency's BWC policy must require that an officer assigned a BWC wear and operate the system in compliance with the agency's BWC policy while performing law enforcement activities under the command and control of another chief law enforcement officer or federal law enforcement official. This requirement is addressed in the Member Responsibilities section of APD's BWC policy.

The Compliance section of APD's BWC policy states: "The unauthorized access to or disclosure of BWC data may constitute misconduct and subject individuals to disciplinary action and criminal penalties pursuant to Minn. Stat. §13.09."

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

APD BWC Program and Inventory

APD possesses 4 Motorola V300 body-worn cameras, all of which are in regular use.

The APD 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 Member Responsibilities section of APD'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," as discussed in Clause 3 of the Policy section of this report. This same section of the policy requires that when a non-uniformed member uses a BWC outside of an authorized undercover capacity, he or she must "wear the recorder in a conspicuous manner when in use or otherwise notify persons that they are being recorded, whenever reasonably practicable." Because Minn. Stat. §626.8473 Subd. 3(b)(2) makes no distinction between uniformed and non-uniformed personnel in establishing the requirement that a BWC be worn "at or above the mid-line of the waist," it is our opinion that this requirement must apply to all personnel when using a BWC.

Prior to the completion of this report, APD submitted a revised BWC policy that addresses this issue.

The Use and Documentation section of APD's BWC policy states that "[o]fficers will use only Department issued BWC's in the performance of official duties for the Department or when otherwise performing authorized law enforcement services as an employee of this Department."

Chief Gerads advised us that he is able to determine the number of BWCs deployed in real-time through the Motorola VideoManager EL Cloud GPS feature. After-the-fact determinations would be based on the schedule and/or payroll data.

As of 2/11/2026, APD maintained a total of 3,378 GB of BWC data.

APD BWC Physical, Technological and Procedural Safeguards

APD BWC data are initially recorded to a hard drive in each officer's BWC. Data from each BWC is then uploaded to Motorola's CommandCentral Cloud Service via a physical docking station located at the APD office.

Officers have view-only access to their own data for report writing, trial preparation, data administration, investigatory purposes and other legitimate law enforcement purposes, as well as the ability to add or edit case numbers and titles.

BWC data is only destroyed via an automated process upon the expiration of the retention period defined for the specific data classification in the VideoManager EL software. There is no manual deletion of BWC data.

Enhanced Surveillance Technology

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

If APD 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 APD records.

Audit Conclusions

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

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

Rampart Audit, LLC

2/24/2026

APPENDIX A:

Policy

422

Arlington Police Department

Policy Manual

Portable Audio/Video Recorders

422.1 PURPOSE AND SCOPE

|state |

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 Arlington Police Department facility, undercover operations, wiretaps, or eavesdropping (concealed listening devices).

422.1.1 DEFINITIONS

|state | MODIFIED

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.

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

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

Records Retention Schedule: refers to the General Records Retention Schedule for Minnesota Cities.

Law Enforcement Related Information: means information captured or available for capture by use of a BWC that has evidentiary value because it documents events with respect to a stop, arrest, search, citation or charging decision.

Evidentiary Value: means that the information may be useful as proof in a criminal prosecution, related civil or administrative proceeding, further investigation of an actual or

suspected criminal act, or in considering an allegation against a law enforcement agency or Officer.

General Citizen Contact: means an informal encounter with a citizen that is not and does not become law enforcement-related or adversarial, and a recording of the event would not yield information relevant to an ongoing investigation. Examples include, but are not limited to, assisting a motorist with directions, summoning a tow truck, or receiving generalized concerns from a citizen about crime trends in his or her neighborhood.

Adversarial: means a law enforcement encounter with a person that becomes confrontational, during which at least one person expresses anger, resentment, or hostility toward the other, or

at least one person directs toward the other, verbal conduct consisting of arguing, threatening, challenging, swearing, yelling, or shouting. Encounters in which a citizen demands to be recorded or initiates recording on his or her own are deemed adversarial.

Unintentional Recorded Footage: is a video recording that results from an Officer's inadvertence or neglect in operating the Officer's BWC, provided that no portion of the resulting recording has evidentiary value. Examples of unintentionally recorded footage include, but are not limited to, recordings made in police Department locker rooms, restrooms, and recordings made while Officers were engaged in conversations of a non-business, personal nature with the expectation that the conversation was not being recorded.

Official Duties: for purposes of this policy, means that the Officer is on duty and performing authorized law enforcement services on behalf of this Department.

422.2 POLICY

Best Practice

MODIFIED

It is the policy of this Department to authorize and require the use of Department issued BWC's as set forth below, and to administer BWC data as provided by law. This policy governs the use of BWC's in the course of official duties. It does not apply to the use of squad-based (dash-cam) recording systems. The Police Chief or their designee may supersede this policy by providing specific instructions for BWC use to individual Officers or providing specific instructions pertaining to particular events or specialized details. This policy is a living document and any changes to the BWC policy must be approved by the City Council.

422.3 USE AND DOCUMENTATION

Agency Content

- (a) Officers will use only Department issued BWC's in the performance of official duties for this Department or when otherwise performing authorized law enforcement services as an employee of this Department.
- (b) Officers who have been issued BWC's shall operate and use them in accordance with this policy. Officers shall conduct a function test of their issued BWC's at the beginning of each shift to make sure the devices are operating properly. Officers noting a malfunction during

testing or at any other time shall promptly report the malfunction to the Officer's Supervisor and obtain a functioning device as soon as reasonably practical.

- (c) Officers should wear their issued BWC's in an approved, conspicuous location on their body.
- (d) Officers must document BWC use, and non-use as follows:
 1. Whenever an Officer makes a recording, the existence of the recording shall be documented.
 2. If an event that is required to be recorded under this policy is not captured or only a part of the activity is captured, the Officer must document the circumstances and reasons for not recording in an incident report or CAD notes.

Supervisors shall review these reports and initiate any corrective action deemed necessary.

- (e) The Department will maintain the following records and documents relating to BWC use, which are classified as public data:
 1. The total number of BWC's owned or maintained by the Department.
 2. A daily record of the total number of BWC's deployed and used by Officers.
 3. The total amount of recorded BWC data collected and maintained.
 4. This policy, together with the Records Retention Schedule.
 5. An accounting of when the Police Chief allows for any deviation of the policy, as described in section 422.3, will be mentioned in the quarterly report to the City Council as found in section 422.10 (a).

422.4 COORDINATOR

state

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.
 1. These procedures should include the process to obtain written authorization for access to non-public data by APO 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 Arlington 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 Arlington 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 Arlington 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.

422.5 MEMBER PRIVACY EXPECTATION

Best Practice

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.

422.6 MEMBER RESPONSIBILITIES

State MODIFIED

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.

Members are required to 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.

422.7 ACTIVATION OF THE AUDIO/VIDEO RECORDER

Best Practice

MODIFIED

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.

422.7.1 CESSATION OF RECORDING

Best Practice

MODIFIED

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 conversations with other officers/deputies, during conversations with legal counsel and during significant periods of inactivity such as report writing or other breaks from direct participation in the incident.

422.7.2 SURREPTITIOUS RECORDINGS

State

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.

422.7.3 EXPLOSIVE DEVICE

Best Practice

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.

422.7.4 DOWNLOADING AND LABELING DATA

Agency Content

- (a) Each Officer using a BWC is responsible for transferring or assuring the proper transfer of the data from his/her camera by the end of that Officer's shift. However, if the Officer is involved in a shooting, in-custody death, or other law enforcement activity resulting in death or great bodily harm, a Supervisor or investigator shall take custody of the Officer's BWC and assume responsibility for transferring the data from it.
- (b) Officers shall label the BWC data files at the time of video capture or transfer to storage and should consult with a Supervisor if in doubt as to the appropriate labeling.
- (c) In addition, staff shall flag each file as appropriate to indicate that it contains information about data subjects who may have rights under the MGDPA limiting disclosure of information about them before the file is disseminated. These individuals include:
 1. Juvenile witnesses, if the nature of the event or activity justifies protecting the identity of the witness;
 2. Mandated reporters;
 3. Individuals who called 911, and services subscribers whose lines were used to place a call to the 911 system;

4. Victims of, and witnesses to crimes, if the victim or witness has requested not to be identified publicly;
 5. When the video is clearly offensive to common sensitivities;
 6. Informants;
 7. Undercover Officers;
 8. Vulnerable adults who are victims of maltreatment;
 9. Victims of child abuse or neglect;
 10. Victims and alleged victims of criminal sexual conduct and/or sex trafficking;
 11. Juveniles who are, or may be delinquent or engaged in criminal acts;

 12. Other individuals whose identities the Officer believes may be legally protected from public disclosure.
 13. Officers and employees who are the subject of an inquiry related to the events captured on video;
 14. Individuals who make complaints about violations with respect to the use of real property;
- (d) Labeling and flagging designations may be corrected or amended based on additional information.

422.7.5 ADMINISTERING ACCESS TO BWC DATA

Agency Content

- (a) **Data Subjects:** Under Minnesota law, the following are considered data subjects for purposes of administering access to BWC data:
1. Any person or entity whose image or voice is documented in the data.
 2. The Officer who collected the data.
 3. Any other Officer whose voice or image is documented in the data, regardless of whether that Officer is or can be identified by the recording.
- (b) **BWC Data is Presumptively Private:** BWC recordings are classified as private data about the data subjects unless there is a specific law that provides differently. As a result:
1. BWC data pertaining to people is presumed private, as is BWC data pertaining to businesses or other entities.
 2. Some BWC data is classified as confidential (see c below).
 3. Some BWC data is classified as public (see d below).
- (c) **Confidential Data:** BWC data that is collected or created as part of an active criminal investigation is confidential. This classification takes precedence over the "private" classification listed above and the "public" classifications listed below.
- (d) **Public Data:** The following BWC data is public:

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

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

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

1. An individual shall be 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 Department would otherwise be prohibited by law from disclosing to the person seeking access, such as portions that would reveal identities protected by Minn. Stat. § 13.82, subd. 17.
2. Unless the data is part of an active investigation, an individual data subject shall be provided with a copy of the recording upon request, but subject to the following guidelines on redaction:
 - (a) Data on other individuals in the recording who do not consent to the release must be redacted.
 - (b) Data that would identify undercover Officers must be redacted.
 - (c) Data on other Officers who are not undercover, and who are on duty and engaged in the performance of official duties, may not be redacted.

(f) **Access by Peace Officers and Law Enforcement Employees:** No employee may have access to the Department's BWC data except for legitimate law enforcement or data administration purposes.

1. Officers may access and view stored BWC video only when there is a business need for doing so, including the need to defend against an allegation of misconduct or substandard performance. Additionally, Officers may review video footage of a

typical law enforcement incident in which they were involved prior to preparing a report, giving a statement, or providing testimony about the incident. The exception will be Officer involved shootings or other critical incidents. The Department will abide by the investigative protocols established by the Minnesota Bureau of Criminal Apprehension that Officers will not typically be allowed to view BWC or squad camera footage prior to giving their statement. There may be isolated situations where this will be allowed. This decision will be made on a case-by-case basis.

2. Department personnel shall document their reasons for accessing stored BWC data at the time of each access. Department personnel are prohibited from accessing BWC data for non-business reasons and from sharing the data for non-law enforcement related purposes, including, but not limited to, uploading BWC data recorded or maintained by this agency to public and social media websites.
 3. Employees seeking access to BWC data for non-business reasons may make a request for it in the same manner as any member of the public.
- (g) **Other Authorized Disclosures of Data:** Officers may display portions of BWC footage to witnesses as necessary for purposes of investigation as allowed by Minn. Stat. § 13.82, subd. 15, as may be amended from time to time. Officers should generally limit these displays in order to protect against the incidental disclosure of individuals whose identities are not public. Protecting against incidental disclosure could involve, for instance, showing only a portion of the video, showing only screen shots, muting the audio, or playing the audio but not displaying video. In addition:
1. BWC data may be shared with other law enforcement agencies only for legitimate law enforcement purposes that are documented in writing at the time of the disclosure.
 2. BWC data shall be made available to prosecutors, courts, and other criminal justice entities as provided by law.

422.8 DATA SECURITY SAFEGUARDS

Agency Content

- (a) Personally owned devices, including, but not limited to, computers and mobile devices, shall not be programmed or used to access or view agency BWC data.
- (b) Officers shall not intentionally edit, alter, or erase any BWC recording.
- (c) As required by Minn. Stat. § 13.825, subd. 9, as may be amended from time to time, this Department shall obtain an independent biennial audit of its BWC program.

422.9 PROHIBITED USE OF AUDIONIDEO RECORDERS

Best Practice

MODIFIED

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.

Recordings shall not be used by any member for the purpose of embarrassment, harassment or ridicule.

422.10 DEPARTMENT USE OF DATA

Agency Content

- (a) At least once a month, the Chief of Police will randomly review BWC usage by each Officer to ensure compliance with this policy. The Chief of Police will submit their findings and put the information into a quarterly report that will be forwarded to the City Council.
- (b) In addition, supervisors and other assigned personnel may access BWC data for the purposes of reviewing or investigating a specific incident that has given rise to an inquiry or concern about Officer misconduct or performance.
- (c) Nothing in this policy limits or prohibits the use of BWC data as evidence of misconduct or as a basis for discipline.
- (d) Officers should contact their Supervisors to discuss retaining and using BWC footage for training purposes. Officer objections to preserving or using certain footage for training will be considered on a case-by-case basis. Field Training Officers may utilize BWC data with trainees for the purpose of providing coaching and feedback on the trainees' performance.

422.11 RETENTION OF RECORDINGS

State MODIFIED

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 180 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). The retention period for these written requests will be 180 days (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).

If a subject of the data submits a written request to the law enforcement agency to retain the recording beyond the applicable retention period for possible evidentiary or exculpatory use related to the circumstances under which the data were collected, the law enforcement agency shall retain the recording for an additional time period requested by the subject of up to 180 days and notify the requester that the recording will then be destroyed unless a new request is

made under this paragraph.

All BWC recordings documenting an officer's use of deadly force must be maintained indefinitely. This is to include use of deadly force not resulting in the death of subject.

422.11.1 RELEASE OF AUDIONIDEO RECORDINGS

Best Practice

MODIFIED

Requests for the release of audio/video recordings shall be processed in accordance with the Records Maintenance and Release Policy.

- (a) 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.

- (b) 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.

422.11.2 ACCESS TO RECORDINGS

|state|

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

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.

422.12 IDENTIFICATION AND PRESERVATION OF RECORDINGS

|state|

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.

422.13 REVIEW OF RECORDED MEDIA FILES

state |

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).

422.14 ACCOUNTABILITY

|state |

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

422.15 COMPLIANCE

Agency Content

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

Agency Content

422.16 CONCLUSION

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

APPENDIX B:

Policy

422

Arlington Police Department Policy Manual

Law Enforcement Policy

Portable Audio/Video Recorders

422.1 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 Arlington Police Department facility, undercover operations, wiretaps, or eavesdropping (concealed listening devices).

422.1.1 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.

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

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

Records Retention Schedule: refers to the General Records Retention Schedule for Minnesota Cities.

Law Enforcement Related Information: means information captured or available for capture by use of a BWC that has evidentiary value because it documents events with respect to a stop, arrest, search, citation or charging decision.

Evidentiary Value: means that the information may be useful as proof in a criminal prosecution, related civil or administrative proceeding, further investigation of an actual or suspected criminal act, or in considering an allegation against a law enforcement agency or Officer.

General Citizen Contact: means an informal encounter with a citizen that is not and does not become law enforcement-related or adversarial, and a recording of the event would not yield information relevant to an ongoing investigation. Examples include, but are not limited to, assisting a motorist with directions, summoning a tow truck, or receiving generalized concerns from a citizen about crime trends in his or her neighborhood.

Adversarial: means a law enforcement encounter with a person that becomes confrontational, during which at least one person expresses anger, resentment, or hostility toward the other, or at least one person directs toward the other, verbal conduct consisting of arguing, threatening, challenging, swearing, yelling, or shouting. Encounters in which a citizen demands to be recorded or initiates recording on his or her own are deemed adversarial.

Unintentional Recorded Footage: is a video recording that results from an Officer's inadvertence or neglect in operating the Officer's BWC, provided that no portion of the resulting recording has evidentiary value. Examples of unintentionally recorded footage include, but are not limited to, recordings made in police Department locker rooms, restrooms, and recordings made while Officers were engaged in conversations of a non-business, personal nature with the expectation that the conversation was not being recorded.

Official Duties: for purposes of this policy, means that the Officer is on duty and performing authorized law enforcement services on behalf of this Department.

422.2 POLICY

It is the policy of this Department to authorize and require the use of Department issued BWC's as set forth below, and to administer BWC data as provided by law. This policy governs the use of BWC's in the course of official duties. It does not apply to the use of squad-based (dash-cam) recording systems. The Police Chief or their designee may supersede this policy by providing specific instructions for BWC use to individual Officers or providing specific instructions pertaining to particular events or specialized details. This policy is a living document and any changes to the BWC policy must be approved by the City Council.

422.3 USE AND DOCUMENTATION

- a. Officers will use only Department issued BWC's in the performance of official duties for this Department or when otherwise performing authorized law enforcement services as an employee of this Department.
- b. Officers who have been issued BWC's shall operate and use them in accordance with this policy.

Officers shall conduct a function test of their issued BWC's at the beginning of each shift to make sure the devices are operating properly. Officers noting a malfunction during testing or at any other time shall promptly report the malfunction to the Officer's Supervisor and obtain a functioning device as soon as reasonably practical.

- c. Officers should wear their issued BWC's in an approved, conspicuous location on their body.
- d. Officers must document BWC use, and non-use as follows:
 - 1. Whenever an Officer makes a recording, the existence of the recording shall be documented.
 - 2. If an event that is required to be recorded under this policy is not captured or only a part of the activity is captured, the Officer must document the circumstances and reasons for not recording in an incident report or CAD notes. Supervisors shall review these reports and initiate any corrective action deemed necessary.
- e. The Department will maintain the following records and documents relating to BWC use, which are classified as public data:
 - 1. The total number of BWC's owned or maintained by the Department.
 - 2. A daily record of the total number of BWC's deployed and used by Officers.
 - 3. The total amount of recorded BWC data collected and maintained.
 - 4. This policy, together with the Records Retention Schedule.
 - 5. An accounting of when the Police Chief allows for any deviation of the policy, as described in section 422.3, will be mentioned in the quarterly report to the City Council as found in section 422.10 (a).

422.4 COORDINATOR

The Chief of Police or the authorized designee should designate a coordinator responsible for (Minn. Stat.

§ 626.8473; Minn. Stat. § 13.825):

- 1. 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).
- 2. Establishing procedures for accessing data and recordings.
 - 1. These procedures should include the process to obtain written authorization for access to

non-public data by APO members and members of other governmental entities and agencies.

3. Establishing procedures for logging or auditing access.
4. Establishing procedures for transferring, downloading, tagging, or marking events.
5. Establishing an inventory of portable recorders including:
 1. Total number of devices owned or maintained by the Arlington 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 Arlington Police Department.
6. Preparing the biennial audit required by Minn. Stat. § 13.825, Subd. 9.
7. Notifying the Bureau of Criminal Apprehension (BCA) in a timely manner when new equipment is obtained by the Arlington Police Department that expands the type or scope of surveillance capabilities of the department's portable recorders.
8. Ensuring that this Portable Audio/Video Recorders Policy is posted on the Department website.

422.5 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.

422.6 MEMBER RESPONSIBILITIES

Prior to going into service, 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. Members should wear the recorder 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 at or above the mid- line of the waist and notify persons that they are being recorded, whenever reasonably practicable (Minn. Stat. § 626.8473).

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.

Members are required to 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.

422.7 ACTIVATION OF THE AUDIONIDEO 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.

422.7.1 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 conversations with other officers/deputies, during conversations with legal counsel and during significant periods of inactivity such as report writing or other breaks from direct participation in the incident.

422.7.2 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.

422.7.3 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.

422.7.4 DOWNLOADING AND LABELING DATA

- a. Each Officer using a BWC is responsible for transferring or assuring the proper transfer of the data from his/her camera by the end of that Officer's shift. However, if the Officer is involved in a shooting, in-custody death, or other law enforcement activity resulting in death or great bodily harm, a Supervisor or investigator shall take custody of the Officer's BWC and assume responsibility for transferring the data from it.
- b. Officers shall label the BWC data files at the time of video capture or transfer to storage and should consult with a Supervisor if in doubt as to the appropriate labeling.
- c. In addition, staff shall flag each file as appropriate to indicate that it contains information about data subjects who may have rights under the MGDPA limiting disclosure of information about them before the file is disseminated. These individuals include:
 1. Juvenile witnesses, if the nature of the event or activity justifies protecting the identity of the witness;
 2. Mandated reporters;

3. Individuals who called 911, and services subscribers whose lines were used to place a call to the 911 system;
 4. Victims of, and witnesses to crimes, if the victim or witness has requested not to be identified publicly;
 5. When the video is clearly offensive to common sensitivities;
 6. Informants;
 7. Undercover Officers;
 8. Vulnerable adults who are victims of maltreatment;
 9. Victims of child abuse or neglect;
 10. Victims and alleged victims of criminal sexual conduct and/or sex trafficking;
 11. Juveniles who are, or may be delinquent or engaged in criminal acts;
 12. Other individuals whose identities the Officer believes may be legally protected from public disclosure.
 13. Officers and employees who are the subject of an inquiry related to the events captured on video;
 14. Individuals who make complaints about violations with respect to the use of real property;
- d. Labeling and flagging designations may be corrected or amended based on additional information.

422.7.5 ADMINISTERING ACCESS TO BWC DATA

- a. **Data Subjects:** Under Minnesota law, the following are considered data subjects for purposes of administering access to BWC data:
 1. Any person or entity whose image or voice is documented in the data.
 2. The Officer who collected the data.
 3. Any other Officer whose voice or image is documented in the data, regardless of whether that Officer is or can be identified by the recording.
- b. **BWC Data is Presumptively Private:** BWC recordings are classified as private data about the data subjects unless there is a specific law that provides differently. As a result:
 1. BWC data pertaining to people is presumed private, as is BWC data pertaining to businesses or other entities.
 2. Some BWC data is classified as confidential (see c below).
 3. Some BWC data is classified as public (see below).
- c. **Confidential Data:** BWC data that is collected or created as part of an active criminal investigation is confidential. This classification takes precedence over the "private" classification listed above and the "public" classifications listed below.

d. **Public Data:** The following BWC data is public:

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

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

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

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

f. **Access by Peace Officers and Law Enforcement Employees:** No employee may have access to the Department's BWC data except for legitimate law enforcement or data administration purposes.

1. Officers may access and view stored BWC video only when there is a business need for doing so, including the need to defend against an allegation of misconduct or substandard performance. Additionally, Officers may review video footage of a typical law

enforcement incident in which they were involved prior to preparing a report, giving a statement, or providing testimony about the incident. The exception will be Officer involved shootings or other critical incidents. The Department will abide by the investigative protocols established by the Minnesota Bureau of Criminal Apprehension that Officers will not typically be allowed to view BWC or squad camera footage prior to giving their statement. There may be isolated situations where this will be allowed. This decision will be made on a case-by-case basis.

2. Department personnel shall document their reasons for accessing stored BWC data at the time of each access. Department personnel are prohibited from accessing BWC data for non-business reasons and from sharing the data for non-law enforcement related purposes, including, but not limited to, uploading BWC data recorded or maintained by this agency to public and social media websites.
 3. Employees seeking access to BWC data for non-business reasons may make a request for it in the same manner as any member of the public.
- g. **Other Authorized Disclosures of Data:** Officers may display portions of BWC footage to witnesses as necessary for purposes of investigation as allowed by Minn. Stat. § 13.82, subd. 15, as may be amended from time to time. Officers should generally limit these displays in order to protect against the incidental disclosure of individuals whose identities are not public. Protecting against incidental disclosure could involve, for instance, showing only a portion of the video, showing only screen shots, muting the audio, or playing the audio but not displaying video. In addition:
1. BWC data may be shared with other law enforcement agencies only for legitimate law enforcement purposes that are documented in writing at the time of the disclosure.
 2. BWC data shall be made available to prosecutors, courts, and other criminal justice entities as provided by law.

422.8 DATA SECURITY SAFEGUARDS

- a. Personally owned devices, including, but not limited to, computers and mobile devices, shall not be programmed or used to access or view agency BWC data.
- b. Officers shall not intentionally edit, alter, or erase any BWC recording.
- c. As required by Minn. Stat. § 13.825, subd. 9, as may be amended from time to time, this Department shall obtain an independent biennial audit of its BWC program.

422.9 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.

Recordings shall not be used by any member for the purpose of embarrassment, harassment or ridicule.

422.10 DEPARTMENT USE OF DATA

- a. At least once a month, the Chief of Police will randomly review BWC usage by each Officer to ensure compliance with this policy. The Chief of Police will submit their findings and put the information into a quarterly report that will be forwarded to the City Council.
- b. In addition, supervisors and other assigned personnel may access BWC data for the purposes of reviewing or investigating a specific incident that has given rise to an inquiry or concern about Officer misconduct or performance.
- c. Nothing in this policy limits or prohibits the use of BWC data as evidence of misconduct or as a basis for discipline.
- d. Officers should contact their Supervisors to discuss retaining and using BWC footage for training purposes. Officer objections to preserving or using certain footage for training will be considered on a case-by-case basis. Field Training Officers may utilize BWC data with trainees for the purpose of providing coaching and feedback on the trainees' performance.

422.11 RETENTION OF RECORDINGS

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). The retention period for these written requests will be 180 days (Minn. Stat. § 13.825).

Members shall not alter, erase, or destroy any recordings before the end of the applicable records retention period to include any associated data or metadata in accordance with (Minn. Stat. § 626.8473).

If a subject of the data submits a written request to the law enforcement agency to retain the recording beyond the applicable retention period for possible evidentiary or exculpatory use related to the circumstances under which the data were collected, the law enforcement agency shall retain the recording for an additional time period requested by the subject of up to 180 days and notify the requester that the recording will then be destroyed unless a new request is made under this paragraph.

All BWC recordings documenting an officer's use of deadly force must be maintained indefinitely. This is to include use of deadly force not resulting in the death of subject.

All of the following BWC data shall be retained for a minimum of one year in accordance with (Minn. Stat. § 13.825 Subd. 3(b)).

1. 1. Reportable firearm discharge
2. Use of force resulting in substantial bodily harm
3. Incident giving rise to a formal complaint against an officer

422.11.1 RELEASE OF AUDIONIDEO RECORDINGS

Requests for the release of audio/video recordings shall be processed in accordance with the Records Maintenance and Release Policy.

1. 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. 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.

422.11.2 ACCESS TO RECORDINGS

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

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.

422.12 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.

422.13 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).

422.14 ACCOUNTABILITY & COMPLIANCE

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

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

422.15 CONCLUSION

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