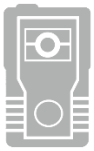
INDEPENDENT AUDITOR'S REPORT

Duluth Police Department



OCTOBER 27TH, 2026

RAMPART AUDIT LLC

Audit Overview and Recommendations

Dear Duluth City Council and Chief Ceynowa:

We have audited the body-worn camera (BWC) program of the Duluth Police Department (DPD) for the two-year period ended 7/14/2026. Minnesota Statute §13.825 mandates that any law enforcement agency operating a portable recording system (PRS)[1] program obtain an independent, biennial audit of its program. This program and its associated data are the responsibility of the Duluth Police Department. Our responsibility is to express an opinion on the operations of this program based on our audit.

On August 13, 2026, Rampart Audit LLC (Rampart) met with Lt. Joel Olejnicak and Digital Evidence Technician Erik Isakson, both of whom provided information about DPD'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 DPD's recordkeeping.

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

DPD 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 Duluth Police Department's BWC program in 2024. As part of that audit, DPD personnel advised us that while Duluth PD's BWC program was implemented in 2014, which predates the public comment and public hearing requirements, and it was unclear whether any sort of public hearing was held at that time. DPD personnel provided documentation showing that in April of 2016 Duluth PD solicited stakeholder feedback regarding its ongoing BWC program. This documentation included letters of support for the BWC program's continuation from the Duluth City Attorney's Office, the St. Louis County Attorney's Office, the Public Defender's Office, the All Nations Indigenous Center, the Cross-Cultural Alliance of Duluth and the Duluth Citizen Review Board. In addition, Lt. Olejnicak

[1] It should be noted that Minnesota statute uses the broader term "portable recording system" (PRS), which includes body-worn cameras. While DPD uses both body-worn cameras and, in limited instances, helmet-mounted cameras, the terms body-worn camera and portable recording system may be used interchangeably in this report.

advised us that DPD's BWCs are a recurring topic of discussion at the monthly Civilian Review Board meetings.

Minn. Stat. §626.8473 Subd. 2 does not contain language grandfathering existing BWC programs at the time of the statute's implementation. While it is our opinion that Duluth Police Department has taken substantial steps toward fulfilling the requirements outlined in statute, Rampart recommends that Duluth PD hold an after-the-fact public hearing and solicit public feedback to ensure these requirements are fully satisfied.

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 DPD's BWC policy on the Police Department page of the City of Duluth' website. In our opinion, Duluth Police Department is compliant with the requirements of §626.8473 Subd. 3(a).

DPD BWC WRITTEN POLICY

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

DPD BWC Data Retention

Minn. Stat. §13.825 Subd. 3(a) establishes a minimum retention period of 90 days for all BWC data not subject to a longer retention period, while §13.825 Subd. 3(b) requires that the following categories of BWC data be retained for a minimum period of one year:

1) any reportable firearms discharge;
2) any use of force by an officer that results in substantial bodily harm; and
3) any incident that results in a formal complaint against an officer.

Meanwhile, Subd. 3(c) requires that any portable recording system data documenting a peace officer's use of deadly force must be maintained indefinitely. Finally, Subd. 3(d) requires that an agency retain BWC recordings for an additional period of up to 180 days when so requested in writing by a data subject.

The Data Retention section of Duluth Police Department's BWC policy states that: "[a]ll portable recording system data shall be retained for a minimum period of 90 days. There are no exceptions for

erroneously recorded or non-evidentiary data." This section also includes the required retention period for each of the individual data categories listed above, except for incidents that result in a complaint against an officer. We noted that this category was included in the previous version of DPD's BWC policy with the correct retention period. It appears to have been omitted when the policy was updated. Prior to the completion of this report, DPD provided an updated version of its BWC policy, which addresses this omission. A copy of the BWC policy that was in force at the time of our audit is attached to this report as Appendix A, while a copy of the revised BWC policy is attached as Appendix B.

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

As discussed in Clause 2 of the Policy section of this report, a BWC policy must prohibit "altering, erasing or destroying any recording made with a peace officer's portable recording system or data and metadata related to the recording prior the expiration of the applicable retention period under section 13.825 Subdivision 3." While DPD's BWC policy includes most of the retention periods for specific data categories described in statute, it does not contain an explicit prohibition of the activities described in Clause 2 of this report, nor does the policy address associated data or metadata as required by Minn. Stat. §626.8473 Subd. 3(b)(1).

We noted that this requirement was addressed in the BWC policy DPD provided as part of our 2024 audit, and appears to have been omitted when the policy was updated. Prior to the submission of this report, DPD provided an updated version of its BWC policy, which addresses this omission.

DPD employs Axon 4 body-worn cameras and utilizes Axon's Cloud Service storage (Evidence.com) and manages BWC data retention through automated retention settings in Axon's video management software. The retention period for each video is determined by the data classification assigned at the time of upload; however, this retention period can be adjusted by command staff or evidence personnel as needed. If an officer fails to assign a data classification, the default retention period is 90 days.

The Data Retention section of DPD's BWC policy states that:

> Employees are responsible for transferring portable recording system data to the video storage server by the end of their shift. In cases involving a shooting or any incident resulting in death or great bodily harm, a supervisor or investigator shall take custody of the portable recording system and ensure the data is properly secured, transferred, and retained.

Lt. Ojenicak advised us that the Axon body-worn cameras utilize physical docking stations located at the Duluth Police Department.

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

DPD BWC Data Destruction

As discussed above, DPD utilizes Axon's Evidence.com for storage, with retention periods determined based on the classification assigned to BWC data.

Axon certifies that its Cloud Service is compliant with the Federal Bureau of Investigation's Criminal Justice Information System Security Division Policy as required by Minnesota Statute §13.825 Subd. 11(b). Data destruction is achieved through automated deletion and overwriting, with storage devices

sanitized (overwritten three or more times or degaussed) or physically destroyed upon being removed from service.

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

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

DPD BWC Data Access

The Access by Non-Employees subsection of the Data Access and Disclosure section of DPD's BWC policy states: "[a]n individual should be allowed to review portable recording system data about themselves and other data subjects in the recording," but restricts access to data that are part of an active investigation, or for which disclosure would otherwise be prohibited. This section of the policy also states: "[u]nless the data is part of an active investigation, an individual data subject shall be provided with a copy of the recording upon request, subject to redaction."

Duluth Police Department personnel advised us that that all requests for BWC data from the public or media are made in writing. Requests can be made online or in person using DPD's police data request form. Requests are processed by one of the Data Release Coordinators unless redaction is required, in which case the Digital Evidence Technician processes it. BWC video is provided to members of the public via 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. A review of Part D of the Access by Non-Employees subsection of Duluth PD's BWC policy shows that DPD has incorporated these requirements into its BWC policy.

Requests for BWC data from other law enforcement agencies are primarily submitted to the Data Release Coordinator; however, lieutenants may process requests involving serious incidents. BWC is normally shared with other law enforcement agencies who use Axon through the "case sharing" function, while non-Axon customers receive an email containing a secure Evidence.com internet link.

Rampart recommends requiring that all requests for BWC video from other law enforcement agencies be made in writing.

The Authorized Disclosure portion of DPD's BWC policy states that "[p]ortable recording system 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." In addition, "[p]ortable recording system data shall be made available to prosecutors, courts, and other criminal justice entities as provided by law." DPD personnel advised us that both the Duluth City Attorney's Office (DCAO) and St. Louis County Attorney's Office (SLCAO) have direct access to BWC recordings through the case sharing portal; however, while the DCAO personnel will normally download BWC data themselves as needed, DPD

investigators normally include BWC data as part of the case submission process for cases to be prosecuted by SLCAO.

DPD personnel advised us that each "case share" or access email from Evidence.com contains a written reminder of the receiving agency's §13.825 Subd. 7 and Subd. 8 obligations, a practice that Rampart recommends.

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

DPD BWC Data Classification

Minn. Stat. §13.825 Subd. 2 defines BWC data as "private data on individuals or nonpublic data," subject to a series of exceptions that result in alternate classifications for specific types of BWC data. While DPD's BWC policy outlines data practices and access procedures that are consistent with such classifications and also notes that "the department may make any data classified as confidential, protected nonpublic, or private accessible to any person, agency, or the public" in certain circumstances, the policy does not explicitly identify BWC data as presumptively private or nonpublic. Although not a required element of a BWC policy, Rampart recommends including information about BWC data classifications in the policy to enhance clarity.

As noted in the preceding section, Duluth PD has incorporated the changes the Minnesota State Legislature made in 2023 regarding BWC data documenting incidents involving the use of deadly force, including the requirement that, subject to limited redaction and certain exceptions, such BWC data be released to the public no later than 14 days after the incident.

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

DPD BWC Internal Compliance Verification

The Compliance section of the DPD BWC policy states that "[s]upervisors shall monitor for compliance with this policy," while the Data Access and Disclosure section states that "[s]upervisors should review portable recording system usage by each employee to ensure compliance with this policy," though the policy does not specify a quantity or frequency of reviews. Lt. Ojenicak advised us that supervisors review use-of-force incidents and complaints, and also conduct random spot checks of BWC usage and access.

Rampart recommends that Duluth PD add language to their BWC policy requiring supervisors to conduct reviews or internal audits on a regular basis. All access to BWC data is logged in the Axon Evidence software, and supervisory reviews should include monitoring of such access.

The Purpose section of DPD's BWC policy states:

> The purpose of this policy is to ensure the proper use of portable recording systems. The primary purpose of using these portable recording systems is to capture evidence arising from department employee encounters with citizens. Such systems also serve to enhance

transparency and accountability by providing an objective record of law enforcement interactions.

The Maintenance and Use of Portable Recording Systems section of DPD's BWC policy states that "[e]mployees may only use department-issued portable recording systems in the performance of official duties for the department or when otherwise performing authorized law enforcement services as an employee of the 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 is addressed in the Maintenance and Use of Portable Recording Systems section of DPD's BWC policy: "[o]fficers who are working under the command and control of another chief law enforcement officer or federal law enforcement official and who are assigned a portable recording system must operate the device in compliance with this policy."

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

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

DPD BWC Program and Inventory

DPD currently possesses 183 Axon 4 body-worn cameras, of which 180 are assigned to individual officers and three (3) are held as spares. Lt. Olejnicak noted that these counts will vary as staffing levels change.

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

As discussed in Clause 3 of the Policy section of this report, the 2023 legislative changes require that an agency's BWC policy must specify that a BWC be worn at or above the mid-line of the waist. The Maintenance and Use of Portable Recording Systems section of DPD's BWC policy states: "[a] body worn camera system must be worn at or above the midline of the waist at a position that maximizes the recording system's capacity to record video coverage of the employee's activities."

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

As of August 13, 2026, DPD maintained 177,629 BWC videos.

DPD BWC Physical, Technological and Procedural Safeguards

DPD BWC data are initially recorded to a hard drive in each officer's BWC. Data from each BWC is then uploaded to Axon's Evidence.com Cloud Service via a physical docking station located at the Police Department.

Officers have view-only access to their own data for report writing, trial preparation, data administration, investigatory purposes and other legitimate law enforcement purposes, as well as the ability to add or edit case numbers and titles. Officers also have the ability to view non-restricted videos created by other personnel; however, all BWC data access is logged automatically and available for audit purposes.

Enhanced Surveillance Technology

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

Audit Conclusions

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



Rampart Audit LLC

10/27/2026

APPENDIX A:

DULUTH POLICE DEPARTMENT POLICY MANUAL

Portable Recording Systems

Policy #: 3.5.11
Effective Date: 5/18/2026

I. PURPOSE

The purpose of this policy is to ensure the proper use of portable recording systems. The primary purpose of using these portable recording systems is to capture evidence arising from department employee encounters with citizens. Such systems also serve to enhance transparency and accountability by providing an objective record of law enforcement interactions. The department authorizes the use of department-issued portable recording systems, and this policy sets forth guidelines governing the use of body worn and helmet cameras, and the management of the resulting data.

II. DEFINITIONS

DATA SUBJECTS – any person or entity whose image or voice is documented in the data; the officer who collected the data; or 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.

PORTABLE RECORDING SYSTEM (BODY WORN CAMERA OR TRT HELMET CAMERA) - a device worn by a department employee that is capable of both video and audio recording of the employee's activities and interactions with others or collecting digital multimedia evidence as part of an investigation.

III. GUIDELINES

A. Maintenance and Use of Portable Recording Systems

1. An employee may only use a portable recording system issued and maintained by the department to document the employee's work-related activities while on duty.

2. Employees may only use department-issued portable recording systems in

the performance of official duties for the department or when otherwise performing authorized law enforcement services as an employee of the department.

3. Uniformed officers who are working patrol, traffic enforcement, special assignment or details, or department authorized off-duty employment shall

use a body worn camera unless permission has been granted by a supervisor to deviate from this policy.

4. Plain clothes officers and/or officers working administrative assignments shall use a body worn camera for all search warrants, preplanned apprehensions and/or enforcement details, including traffic stops and person stops. Plain clothes officers may elect to use a body worn camera pursuant to the needs of a specific investigation or job duty, or when directed by a supervisor. If use of a body worn camera would be detrimental or compromise a plain-clothes operation, the use of a body worn camera would not be required with supervisor approval.

5. Officers who are working under the direction of another chief law enforcement officer or federal law enforcement official and who are assigned a portable recording system must operate the device in compliance with this policy.

6. Employees shall conduct a function test of their department-issued portable recording system(s) at the beginning of each shift. Employees noting a malfunction during testing or at any other time should promptly report the malfunction to a supervisor. Supervisors should take prompt action to address malfunctions and assign replacement equipment when necessary.

7. A body worn camera system must be worn at or above the midline of the waist at a position that maximizes the recording system's capacity to record video coverage of the employee's activities.

8. Employees shall not intentionally block the recording system's audio or visual recording functionality to defeat the purposes of this policy.

B. Portable Recording System Use

1. Employees shall activate their body worn cameras when anticipating that they will be involved in or become involved in a pursuit, investigative stop of a motorist or pedestrian, search, seizure, arrest, use of force, adversarial contact, and during other activities likely to yield information having evidentiary value. Employees need not activate their cameras when it would be unsafe, impossible, or impractical to do so.

2. Employees have discretion to record or not record any 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. Employees may decide to use their body worn cameras to record any citizen encounter if there is reason to

believe the recording would potentially yield information having evidentiary value, unless such recording is otherwise expressly prohibited.

3. Employees have no affirmative duty to inform people that a portable recording system is being operated or that the individuals are being recorded but may do so at any time.

4. Employees should be sensitive to the dignity of members of the public being recorded and exercise sound discretion to respect privacy by discontinuing recording when it reasonably appears that such privacy outweighs any legitimate interest in recording. Requests by members of the public to stop recording should be considered using these same criteria. Recording should resume when privacy is no longer at issue unless no longer required by another section of this policy. Employees should state the reason on camera before deactivating their recording device(s) and specify the circumstances in their report.

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

6. Employees should use their body worn camera to record their transportation and the physical transfer of persons in their custody to hospitals, detox, mental health facilities, or another agency's detention facility, but otherwise should not record inside these facilities unless necessary to document criminal activity, use of force, or an adversarial encounter.

7. Employees shall not use their portable recording system(s) to record non-work-related activity. Employees shall not use their portable recording system(s) to record other department personnel during non-enforcement related activities, such as before or after shift time, in locker rooms or restrooms, during breaks, during other private conversations or within areas of the department restricted to personnel-only, unless recording is authorized as part of an administrative or criminal investigation.

8. Once activated, the portable recording system should continue recording until the conclusion of the incident or encounter, or until it becomes apparent that additional recording is unlikely to capture information having evidentiary value. An officer having charge of a scene may direct the discontinuance of recording when further recording is unlikely to capture

additional information having evidentiary value. If the recording is discontinued while an investigation, response or incident is ongoing, the employee should state the reasons for ceasing the recording on camera before deactivating the device. If circumstances change, employees shall reactivate their cameras as required by this policy to capture information having evidentiary value.

C. Documentation

1. Whenever an employee makes a recording it shall be documented in the incident report. If no report is written, the recording shall be noted in the Computer-Aided Dispatch (CAD) event.

2. If an employee fails to record an activity that is required to be recorded under this policy, or captures only part of the activity, the employee must document the reasons for not recording in the incident report, or if no report is written, in the CAD event. If an activity was not recorded due to a supervisor's directive, the circumstances shall be documented in the same manner.

D. Data Retention

1. Employees are responsible for transferring portable recording system data to the video storage server by the end of their shift. In cases involving a shooting or any incident resulting in death or great bodily harm, a supervisor or investigator shall take custody of the portable recording system and ensure the data is properly secured, transferred, and retained.

2. All portable recording system data shall be retained for a minimum period of ninety (90) days. There are no exceptions for erroneously recorded or non-evidentiary data. Other body worn camera data that is classified as non-evidentiary, becomes non-evidentiary, or is not maintained for training should be destroyed after ninety (90) days. Minn Stat. §13.825, subd. 3 (a).

3. All recordings 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, and recordings documenting the use of force by a peace officer that results in substantial bodily harm must be maintained for a minimum period of one (1) year. Minn. Stat. § 13.825, subd. 3(b)(1).

4. Portable recording system data must be maintained for at least one (1) year if a formal complaint is made against an officer related to the incident recorded. Minn Stat. § 13.825, subd. 3(b)(2).

5. The full, unedited, and unredacted recording of a peace officer using deadly force must be maintained indefinitely. Minn. Stat. § 13.825, subd. 3 (c).

6. Other data having evidentiary value shall be retained for the period specified in the applicable records retention schedule.

7. When a particular recording is subject to multiple retention periods, it shall be maintained for the longest applicable period.

8. Upon written request by a body worn camera data subject, the department shall retain a recording pertaining to that subject for an additional time period requested by the subject, up to one hundred eighty (180) days, pursuant to Minn. Stat. § 13.825, subd. 3. The department must notify the requestor at the time of the request that the data will then be destroyed unless a new written request for retention is received.

E. Data Access and Disclosure

1. Access by Employees

a. Employees may only access portable recording system data for legitimate law enforcement or data administration purposes.

b. Employees may access and view stored video only when there is a business need for doing so, including the need to defend against an allegation of misconduct or substandard performance. Employees 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.

c. Supervisors should review portable recording system usage by each employee to ensure compliance with this policy.

d. Supervisors and other assigned personnel may access portable recording system data for the purpose of reviewing or investigating a specific incident that has given rise to a complaint or concern about employee misconduct or performance.

e. Field training officers may utilize portable recording system data with trainees for the purposes of providing coaching and feedback on the trainee's performance.

f. Employees seeking access to portable recording system data for non-business reasons may make a request for it in the same manner as any member of the public.

2. Access by Non-Employees

a. An individual should be allowed to review portable recording system data about themselves and other data subjects in the recording, however access shall not be granted:

    i. If the data was collected or created as part of an active investigation; or

    ii. To portions of the data that the department would otherwise be prohibited by law from disclosing to the person seeking access.

b. Unless the data is part of an active investigation, an individual data subject shall be provided with a copy of the recording upon request, subject to redaction.

    i. Data on other individuals in the recording who do not consent to the release must be redacted.

    ii. Data that would identify undercover officers must be redacted.

    iii. 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.

c. Portable Recording System Data from Motor Vehicle Collisions

    i. A person entitled to a report of a collision, under Minn. Stat. § 169.09, subd. 13, must be provided with copies of unredacted data from all portable recording systems used in the collision investigation, including data on other individuals who are the subject of the recording. A request must be made in writing and accompanied by the accident report relating to the data.

    ii. The department shall notify the requester of the remedies and penalties applicable under Minn Stat. § 13.08 should the requester use or disseminate the data in an unauthorized manner. Minn. Stat. § 13.825, subd. 4.

    iii. The department may deny a request for unredacted portable recording system from a person entitled to a report of a motor vehicle collision, if:

a) The department determines there is a compelling reason that providing access to the data would interfere with an active investigation;

b) The data is clearly offensive to common sensibilities; or

c) The data is classified as not public by a provision of Minnesota Statute Chapter 13.

iv. If the department denies access, the department must provide a prompt, written reason for the denial to the individual who requested the data with a description of the compelling reason and must provide notice that relief may be sought from the district court under Minn. Stat. § 13.82, subd. 7. Minn. Stat. § 13.825, subd. 4.

d. Data Documenting Deadly Use of Force Incidents

i. When an individual dies as a result of the use of force by an officer employed by the department, the department shall release all body worn camera data documenting the incident, redacted no more than what is required by law, no later than fourteen (14) days after the incident, pursuant to Minn. Stat. § 13.825.

ii. As allowed by Minn. Stat. § 13.825, upon request, when an individual dies as a result of use of force by an officer, the department must allow the following individuals to view all body worn camera data, redacted no more than what is required by law, within five (5) days of the request:

a) The deceased individual's next of kin;

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

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

iii. The Chief may deny a request if the department determines that there is a compelling reason that viewing or releasing the video would interfere with an active investigation. If the Chief deems releasing portable recording system data within the mandated fourteen (14) day period would interfere with an ongoing investigation, the Chief must assert this in writing. If the department denies access to an eligible individual, the

Chief 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 Minn. Stat. § 13.82, subd. 7.

e. Pursuant to Minn. Stat. § 13.82, subd. 15, the department may make any data classified as confidential, protected nonpublic, or private accessible to any person, agency, or the public if the department determines that the access will aid the law enforcement process, promote public safety, or dispel widespread rumor or unrest.

F. Authorized Disclosures

1. Officers may display portions of portable recording system footage to witnesses as necessary for purposes of investigation, as allowed by Minn. Stat. § 13.82, subd. 15. These displays should be limited in order to protect against the incidental disclosure of individuals whose identities are not public. Protecting against incidental disclosure could involve strategies such as showing only a portion of the video, showing only a screen shot of the footage, muting the audio, or playing the audio but not displaying the video.

2. Portable recording system 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.

3. Portable recording system data shall be made available to prosecutors, courts, and other criminal justice entities as provided by law.

G. Inventory and Records

1. The department shall maintain a written record of:

   a. The total number of recording devices owned or maintained by the department;

   b. A daily record of the total number of recording devices deployed and used by officers;

   c. The policies and procedures for use of portable recording systems; and

   d. The total amount of recorded audio and video data collected by the portable recording system and maintained by the department's retention schedule of the data, and the department's procedure for destruction of the data.

2. This information is public and shall be provided upon request.

H. Compliance

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

2. If data collected by a portable recording system is received from another law enforcement agency, the department must comply with all data classification, destruction, and security requirements of the recording agency.

3. The Chief or the Chief's designee should periodically review the efficacy of the body worn camera program, including review of this policy, to ensure it remains compliant with relevant laws and practices.

APPENDIX B:

DULUTH POLICE DEPARTMENT POLICY MANUAL

Portable Recording Systems

Policy #: 3.5.11

Effective Date: 5/18/2026

PURPOSE

The purpose of this policy is to ensure the proper use of portable recording systems. The primary purpose of using these portable recording systems is to capture evidence arising from department employee encounters with citizens. Such systems also serve to enhance transparency and accountability by providing an objective record of law enforcement interactions. The department authorizes the use of department-issued portable recording systems, and this policy sets forth guidelines governing the use of body worn and helmet cameras, and the management of the resulting data.

DEFINITIONS

DATA SUBJECTS – any person or entity whose image or voice is documented in the data; the officer who collected the data; or 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.

PORTABLE RECORDING SYSTEM (BODY WORN CAMERA OR TRT HELMET CAMERA) - a device worn by a department employee that is capable of both video and audio recording of the employee's activities and interactions with others or collecting digital multimedia evidence as part of an investigation.

GUIDELINES

Maintenance and Use of Portable Recording Systems

An employee may only use a portable recording system issued and maintained by the department to document the employee's work-related activities while on duty.

Employees may only use department-issued portable recording systems in the performance of official duties for the department or when otherwise performing authorized law enforcement services as an employee of the department.

Uniformed officers who are working patrol, traffic enforcement, special assignment or details, or department authorized off-duty employment shall use a body worn camera unless permission has been granted by a supervisor to deviate from this policy.

Plain clothes officers and/or officers working administrative assignments shall use a body worn camera for all search warrants, preplanned apprehensions and/or enforcement details, including traffic stops and person stops. Plain clothes officers may elect to use a body worn camera pursuant to the needs of a specific investigation or job duty, or when directed by a supervisor. If use of a body worn camera would be detrimental or compromise a plain-clothes operation, the use of a body worn camera would not be required with supervisor approval.

Officers who are working under the direction of another chief law enforcement officer or federal law enforcement official and who are assigned a portable recording system must operate the device in compliance with this policy.

Employees shall conduct a function test of their department-issued portable recording system(s) at the beginning of each shift. Employees noting a malfunction during testing or at any other time should promptly report the malfunction to a supervisor. Supervisors should take prompt action to address malfunctions and assign replacement equipment when necessary.

A body worn camera system must be worn at or above the midline of the waist at a position that maximizes the recording system's capacity to record video coverage of the employee's activities.

Employees shall not intentionally block the recording system's audio or visual recording functionality to defeat the purposes of this policy.

Portable Recording System Use

Employees shall activate their body worn cameras when anticipating that they will be involved in or become involved in a pursuit, investigative stop of a motorist or pedestrian, search, seizure, arrest, use of force, adversarial contact, and during other activities likely to yield information having evidentiary value. Employees need not activate their cameras when it would be unsafe, impossible, or impractical to do so.

Employees have discretion to record or not record any 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. Employees may decide to use their body worn cameras to record any citizen encounter if there is reason to believe the recording would potentially yield information having evidentiary value, unless such recording is otherwise expressly prohibited.

Employees have no affirmative duty to inform people that a portable recording system is being operated or that the individuals are being recorded but may do so at any time.

Employees should be sensitive to the dignity of members of the public being recorded and exercise sound discretion to respect privacy by discontinuing recording when it reasonably appears that such privacy outweighs any legitimate interest in recording. Requests by members of the public to stop recording should be considered using these same criteria. Recording should resume when privacy is no longer at issue unless no longer required by another section of this policy. Employees should state the reason on camera before deactivating their recording device(s) and specify the circumstances in their report.

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

Employees should use their body worn camera to record their transportation and the physical transfer of persons in their custody to hospitals, detox, mental health facilities, or another agency's detention facility, but otherwise should not record inside these facilities unless necessary to document criminal activity, use of force, or an adversarial encounter.

Employees shall not use their portable recording system(s) to record non-work-related activity. Employees shall not use their portable recording system(s) to record other department personnel during non-enforcement related activities, such as before or after shift time, in locker rooms or restrooms, during breaks, during other private conversations or within areas of the department restricted to personnel-only, unless recording is authorized as part of an administrative or criminal investigation.

Once activated, the portable recording system should continue recording until the conclusion of the incident or encounter, or until it becomes apparent that additional recording is unlikely to capture information having evidentiary value. An officer having charge of a scene may direct the discontinuance of recording when further recording is unlikely to capture additional information having evidentiary value. If the recording is discontinued while an investigation, response or incident is ongoing, the employee should state the reasons for ceasing the recording on camera before deactivating the device. If circumstances change, employees shall reactivate their cameras as required by this policy to capture information having evidentiary value.

Documentation

Whenever an employee makes a recording it shall be documented in the incident report. If no report is written, the recording shall be noted in the Computer-Aided Dispatch (CAD) event.

If an employee fails to record an activity that is required to be recorded under this policy, or captures only part of the activity, the employee must document the reasons for not recording in the incident report, or if no report is written, in the CAD event. If an activity was not recorded due to a supervisor's directive, the circumstances shall be documented in the same manner.

Data Management

The department shall comply with the requirements of Minn. Stat. § 13.825 and other data classifications, access procedures, retention policies, and data security safeguards that, at a minimum, meet the requirements of Ch. 13 and other applicable law.

Data Retention

Employees are responsible for transferring portable recording system data to the video storage server by the end of their shift. In cases involving a shooting or any incident resulting in death or great bodily harm, a supervisor or investigator shall take custody of the portable recording system and ensure the data is properly secured, transferred, and retained.

All portable recording system data shall be retained for a minimum period of ninety (90) days. There are no exceptions for erroneously recorded or non-evidentiary data. Other body worn camera data that is classified as non-evidentiary, becomes non-evidentiary, or is not maintained for training should be destroyed after ninety (90) days. Minn Stat. §13.825, subd. 3 (a).

All recordings 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, and recordings documenting the use of force by a peace officer that results in substantial bodily harm must be maintained for a minimum period of one (1) year. Minn. Stat. § 13.825, subd. 3(b)(1).

Portable recording system data must be maintained for at least one (1) year if a formal complaint is made against an officer related to the incident recorded. Minn Stat. § 13.825, subd. 3(b)(2).

~~The full, unedited, and unredacted recording of a peace officer using deadly force must be maintained indefinitely. Minn. Stat. § 13.825, subd. 3 (c).~~ Employees shall not alter, erase, or destroy any recording made with a peace officer's portable recording system, or any data or metadata related to the recording, prior to the expiration of the applicable retention period under Minn. Stat. § 13.825, subd. 3, except that the full, unedited, and unredacted recording of a peace officer using deadly force must be maintained indefinitely. Minn. Stat. § 626.8473, subd. 3(b)(1).

Other data having evidentiary value shall be retained for the period specified in the applicable records retention schedule.

When a particular recording is subject to multiple retention periods, it shall be maintained for the longest applicable period.

Upon written request by a body worn camera data subject, the department shall retain a recording pertaining to that subject for an additional time period requested by the subject, up to one hundred eighty (180) days, pursuant to Minn. Stat. § 13.825, subd. 3. The department must notify the requestor at the time of the request that the data will then be destroyed unless a new written request for retention is received.

Data Access and Disclosure

Access by Employees

Employees may only access portable recording system data for legitimate law enforcement or data administration purposes.

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

Supervisors should review portable recording system usage by each employee to ensure compliance with this policy.

Supervisors and other assigned personnel may access portable recording system data for the purpose of reviewing or investigating a specific incident that has given rise to a complaint or concern about employee misconduct or performance.

Field training officers may utilize portable recording system data with trainees for the purposes of providing coaching and feedback on the trainee's performance.

Employees seeking access to portable recording system data for non-business reasons may make a request for it in the same manner as any member of the public.

Access by Non-Employees

An individual should be allowed to review portable recording system data about themselves and other data subjects in the recording, however access shall not be granted:

If the data was collected or created as part of an active investigation; or

To portions of the data that the department would otherwise be prohibited by law from disclosing to the person seeking access.

Unless the data is part of an active investigation, an individual data subject shall be provided with a copy of the recording upon request, subject to redaction.

Data on other individuals in the recording who do not consent to the release must be redacted.

Data that would identify undercover officers must be redacted.

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.

Portable Recording System Data from Motor Vehicle Collisions

A person entitled to a report of a collision, under Minn. Stat. § 169.09, subd. 13, must be provided with copies of unredacted data from all portable recording systems used in the collision investigation, including data on other individuals who are the subject of the recording. A request must be made in writing and accompanied by the accident report relating to the data.

The department shall notify the requester of the remedies and penalties applicable under Minn Stat. § 13.08 should the requester use or disseminate the data in an unauthorized manner. Minn. Stat. § 13.825, subd. 4.

The department may deny a request for unredacted portable recording system from a person entitled to a report of a motor vehicle collision, if:

The department determines there is a compelling reason that providing access to the data would interfere with an active investigation;

The data is clearly offensive to common sensibilities; or

The data is classified as not public by a provision of Minnesota Statute Chapter 13.

If the department denies access, the department must provide a prompt, written reason for the denial to the individual who requested the data with a description of the compelling reason and must provide notice that relief may be sought from the district court under Minn. Stat. § 13.82, subd. 7. Minn. Stat. § 13.825, subd. 4.

Data Documenting Deadly Use of Force Incidents

When an individual dies as a result of the use of force by an officer employed by the department, the department shall release all body worn camera data documenting the incident, redacted no more than what is required by law, no later than fourteen (14) days after the incident, pursuant to Minn. Stat. § 13.825.

As allowed by Minn. Stat. § 13.825, upon request, when an individual dies as a result of use of force by an officer, the department must allow the following individuals to view all body worn camera data, redacted no more than what is required by law, within five (5) days of the request:

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.

The Chief may deny a request if the department determines that there is a compelling reason that viewing or releasing the video would interfere with an active investigation. If the Chief deems releasing portable recording system data within the mandated fourteen (14) day period would interfere with an ongoing investigation, the Chief must assert this in writing. If the department denies access to an eligible individual, the Chief 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 Minn. Stat. § 13.82, subd. 7.

Pursuant to Minn. Stat. § 13.82, subd. 15, the department may make any data classified as confidential, protected nonpublic, or private accessible to any person, agency, or the public if the department determines that the access will aid the law enforcement process, promote public safety, or dispel widespread rumor or unrest.

Authorized Disclosures

Officers may display portions of portable recording system footage to witnesses as necessary for purposes of investigation, as allowed by Minn. Stat. § 13.82, subd. 15. These displays should be limited in order to protect against the incidental disclosure of individuals whose identities are not public. Protecting against incidental disclosure could involve strategies such as showing only a portion of the video, showing only a screen shot of the footage, muting the audio, or playing the audio but not displaying the video.

Portable recording system 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.

Portable recording system data shall be made available to prosecutors, courts, and other criminal justice entities as provided by law.

Inventory and Records

The department shall maintain a written record of:

The total number of recording devices owned or maintained by the department;

A daily record of the total number of recording devices deployed and used by officers;

The policies and procedures for use of portable recording systems; and

The total amount of recorded audio and video data collected by the portable recording system and maintained by the department's retention schedule of the data, and the department's procedure for destruction of the data.

This information is public and shall be provided upon request.

The department shall arrange for an independent, biennial audit of the portable recording system records to determine whether data are appropriately classified, how the data are used, and whether the data are destroyed as required by statute, and to verify compliance with all rules and regulations. Minn. Stat. § 13.825, subd 9 (a).

Compliance

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

If data collected by a portable recording system is received from another law enforcement agency, the department must comply with all data classification, destruction, and security requirements of the recording agency.

The Chief or the Chief's designee should periodically review the efficacy of the body worn camera program, including review of this policy, to ensure it remains compliant with relevant laws and practices.