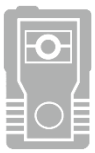
INDEPENDENT AUDITOR'S REPORT

Winthrop Police Department



OCTOBER 13TH, 2025

RAMPART AUDIT LLC

Audit Overview and Recommendations

Dear Winthrop City Council and Chief Anderson:

We have audited the body-worn camera (BWC) program of the Winthrop Police Department (WPD) for the two-year period ended 6/30/2025. 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 Winthrop Police Department. Our responsibility is to express an opinion on the operations of this program based on our audit.

On September 5, 2025, Rampart Audit, LLC (Rampart) met with Chief Logan Anderson, who provided information about WPD's BWC program policies, procedures and operations. As part of the audit, Rampart also conducted a sampling of BWC data to verify WPD's recordkeeping.

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

WPD BWC Program Implementation and Authorization

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

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

Chief Anderson advised Rampart that there was a discussion of WPD's proposed BWC policy during the January 23, 2023, Winthrop City Council meeting. Rampart was able to locate a copy of the Winthrop City Council meeting agenda for that date, which stated that a public reading of the proposed BWC policy was held. Rampart also located a copy of the minutes of the January 3, 2023, Winthrop City Council meeting, which documented the discussion of the proposed acquisition of a BWC system, as well as the council's approval to proceed. Copies of these documents have been retained in our files.

In reviewing this process, Chief Anderson determined that WPD had not taken steps to solicit public comment prior to the purchase or implementation of their BWC program. Rampart recommended that WPD post a notice inviting public comment and hold an after-the-fact public forum during an upcoming Winthrop City Council meeting to discuss the BWC program and policy. Chief Anderson provided documentation showing that a public notice was posted on the City of Winthrop Facebook page on 8/27/2025, inviting the public to review the BWC policy and provide comments either in writing via mail or email, or in person at the September 8, 2025, Winthrop City Council meeting.

[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 WPD, these terms may be used interchangeably in this report.

Rampart also located a copy of the agenda and minutes of the September 8, 2025, Winthrop City Council meeting. We noted that the BWC public hearing was listed on the agenda and that a copy of the BWC policy was included in the meeting minutes. Copies of these documents have been retained in our files.

In our opinion, while Winthrop Police Department did not meet the requirements of §626.8473 Subd. 2 prior to the implementation of their BWC program, they have taken appropriate remedial steps to address this oversight.

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 the BWC policy on the WPD webpage at the time of the audit. In our opinion, Winthrop Police Department is compliant with the requirements of §626.8473 Subd. 3(a).

WPD BWC WRITTEN POLICY

As part of this audit, we reviewed WPD's BWC policy, a copy of which is attached to this report as Appendix A.

Minnesota Statute §626.8473 Subd. 3(b) requires a written BWC policy to incorporate the following, at a minimum:

1. The requirements of section 13.825 and other data classifications, access procedures, retention policies, and data safeguards that, at a minimum, meet the requirements of chapter 13 and other applicable law;
2. A prohibition on altering, erasing or destroying any recording made with a peace officer's portable recording system or data and metadata related to the recording prior the expiration of the applicable retention period under section 13.825 Subdivision 3, except that the full, unedited, and unredacted recording of a peace officer using deadly force must be maintained indefinitely;
3. A mandate that a portable recording system be worn at or above the mid-line of the waist in a position that maximizes the recording system's capacity to record video footage of the officer's activities;
4. A mandate that officers assigned a portable recording system wear and operate the system in compliance with the agency's policy adopted under this section while performing law enforcement activities under the command and control of another chief law enforcement officer or federal law enforcement official;
5. A mandate that, notwithstanding any law to the contrary, when an individual dies as a result of a use of force by a peace officer, an involved officer's law enforcement agency must allow the deceased individual's next of kin, the legal representative of the deceased individual's next of kin, and the other parent of the deceased individual's child, upon their request, to inspect all portable recording system data, redacted no more than what is required by law, documenting the incident within five days of the request, with the following exception:
    - A law enforcement agency may deny a request if the agency determines that there is a compelling reason that inspection would interfere with an active investigation. If the agency denies access, the chief law enforcement officer must provide a prompt, written denial to the individual who requested the data with a short description of the compelling reason access was denied and must

provide notice that relief may be sought from the district court pursuant to section 13.82 subdivision 7;

6. A mandate that, when an individual dies as a result of a use of force by a peace officer, an involved officer's law enforcement agency shall release all portable recording system data, redacted no more than required by law, documenting the incident no later than 14 days after the incident, unless the chief law enforcement officer asserts in writing that the public classification would interfere with an ongoing investigation, in which case the data remain classified by section 13.82 subdivision 7;
7. Procedures for testing the portable recording system to ensure adequate functioning;
8. Procedures to address a system malfunction or failure, including requirements for documentation by the officer using the system at the time of a malfunction or failure;
9. Circumstances where recording is mandatory, prohibited, or at the discretion of the officer using the system;
10. Circumstances under which a data subject must be given notice of a recording;
11. Circumstances under which a recording may be ended while an investigation, response, or incident is ongoing;
12. Procedures for the secure storage of portable recording system data and the creation of backup copies of the data; and
13. Procedures to ensure compliance and address violations of the policy, which must include, at a minimum, supervisory or internal audits and reviews, and the employee discipline standards for unauthorized access to data contained in section 13.09.

In our opinion, the WPD BWC policy is compliant with respect to clauses 7 – 11.

Due to their complexity and interrelatedness, clauses 1 and 12 are discussed separately below. Clause 13 is also discussed separately.

Clauses 2 – 6 are newly added as a result of 2023 legislation and will also be discussed separately below.

WPD 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.

WPD currently follows the General Records Retention Schedule for Minnesota Cities (GRRSMC), but also addresses the categories above separately within its BWC policy:

Part 1 of the Data Retention subsection of WPD's BWC policy states: "All BWC data shall be retained for a minimum period of 90 days. There are no exceptions for erroneously recorded or non-evidentiary data," which satisfies the requirements of §13.825 Subd. 3(a).

Part 2 of the Data Retention section of WPD's BWC policy states:

> Data that documents 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 data documenting the use of force by a peace officer that results in substantial bodily harm must be retained for a minimum period of one year.

Part 4 of the Data Retention subsection of WPD's BWC policy states: "[d]ata documenting circumstances that have given rise to a formal inquiry against an officer must be retained according to the department's record retention schedule." We noted that this language differs from the "formal complaint" standard specified in the GRRSMC, and is also not addressed in the secondary retention schedule included in WPD's BWC policy. While it is our opinion that this constitutes a broader standard that would incorporate all formal complaints as well as additional inquiries, we recommend that WPD revise the language of this section to clarify that data documenting circumstances that have given rise to a formal complaint against an officer shall be retained for a minimum period of one year.

Part 3 of the Data Retention subsection of WPD's BWC policy states: "[d]ata that documents the use of deadly force by a peace officer, or force of a sufficient type or degree to require a use of force report or supervisory review must be retained indefinitely."

With the exception discussed above relating to the clarity of Part 4, these passages meet or exceed the requirements of §13.825 Subd. 3(b) and Subd. 3(c).

Prior to the issuance of this report, WPD submitted a revised BWC policy that states explicitly that "BWC data documenting circumstances that have given rise to a formal complaint against an officer shall be retained for a minimum period of one year." A copy of the revised policy is attached to this report as Appendix B.

Part 7 of the Data Retention subsection of WPD's BWC policy states: "Upon written request by a BWC data subject, the Department shall retain a recording pertaining to that subject for an additional time period requested by the subject of up to 180 days…" This satisfies the requirements of §13.825 Subd. 3(d).

Part 2 of the Data Security Safeguards subsection of WPD's BWC policy states:

> Officers shall not intentionally edit, alter, or erase any BWC recording made with a peace officer's portable recording system or data and metadata related to the recording prior 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.

This satisfies the requirement discussed in Clause 2 of the Policy section of this report, which states that a BWC policy must prohibit altering, erasing or destroying any recording made with a peace officer's portable recording system, as well as associated data or metadata, prior to the expiration of the applicable retention period.

Winthrop Police Department currently employs WatchGuard V300 BWCs, utilizes WatchGuard's Evidence Library Cloud storage service and manages BWC data retention through automated settings in WatchGuard's video management software. The retention period for each video is determined by the event type assigned at the time of upload; however, this retention period can be adjusted as needed. Chief Anderson advised us that in the event an officer fails to assign a category to a BWC recording, the default retention period is two years to avoid the accidental loss of data.

The Downloading and Labeling Data section of WPD's BWC policy requires that: "Each officer is responsible for transferring or assuring the proper transfer of the data from his/her camera to the Motorola Solutions cloud by the end of that officer's shift." It also states: "Officers shall label the BWC data files at the time of video capture or transfer to storage."

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

WPD BWC Data Destruction

As discussed above, WPD utilizes WatchGuard's cloud-based storage service, Evidence Library Cloud, with data retention and deletion schedules managed automatically based on the assigned data classification of each video. Motorola, which acquired WatchGuard in 2019, describes its BWC cloud storage services as CJIS compliant as required by Minnesota Statute §13.825 Subd. 11(b), with the service 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, WPD's BWC policy is compliant with the applicable data destruction requirements.

WPD BWC Data Access

The Administering Access to BWC Data section of WPD's BWC policy states: "Officers shall refer members of the media or public seeking access to BWC data to the Administrative Manager, who shall process the request in accordance with the MGDPA and other governing laws." Chief Anderson, advised us, however, that such requests are submitted to either the chief or the assistant chief of police.

Chief Anderson advised us that requests from the public or members of the media are submitted using a printed data request form. He reviews the request and, if approved, either he or the assistant chief process it as described in the BWC policy, with the requester receiving an email link through the WatchGuard Cloud storage service.

WPD BWC data is shared with other law enforcement agencies "only for legitimate law enforcement purposes that are documented in writing at the time of the disclosure." All such requests are made in writing. The chief or assistant chief review each request and, if approved, all officers are able to share BWC data. Existing verbal agreements between WPD and other area law enforcement agencies address data classification, destruction and security requirements, as specified in §13.825 Subd. 8(b). The same process is used for requests from prosecutors. Requests are fulfilled via secure internet link through the WatchGuard Cloud service.

We recommend that copies of these requests be maintained for audit purposes. We also recommend that WPD obtain a written acknowledgment of the receiving agency's responsibilities under §13.825 Subd. 8(b), or include a reminder of those responsibilities as part of any correspondence with the receiving agency. Prior to the issuance of this report, Chief Anderson furnished a screenshot showing that a written reminder of these responsibilities had been added to the email that accompanies each BWC internet link.

As discussed in Clauses 5 and 6 of the Policy section of this report, the Minnesota State Legislature in 2023 added specific access requirements related to BWC data that document deadly force incidents, and specified that these requirements must be included in the agency's BWC policy. These requirements are addressed in the Access to BWC data by non-employees subsection of the Administering Access to Body Worn Camera Data section of WPD's BWC policy.

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

WPD BWC Data Classification

The Administering Access to BWC Data section of WPD'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," and identifies those circumstances in which BWC data are instead classified as either confidential or public.

As discussed in the preceding section of this report, WPD's BWC policy addresses the requirements discussed in Clauses 5 and 6 of the Policy section of this report, which include the public classification of BWC data documenting an officer's use of deadly force.

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

WPD BWC Internal Compliance Verification

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

The Agency Use of Data section of the WPD BWC policy states:

> At least once a month or as soon as practicable, the Police Chief will randomly review BWC usage by each full-time officer or part-time officer that has worked in the previous month to ensure compliance with this policy.

Chief Anderson advised us that WPD maintains a written record of the videos that are reviewed as part of these internal audits, as well as documenting the nature of each review in the WatchGuard Evidence Library software.

The Use and Documentation section of WPD's BWC policy states: "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," and: "Officers who have been issued BWC's shall operate and use them in accordance with this policy."

In addition, this section of the policy states: "While under the command and control of another chief law enforcement officer or federal law enforcement official, officers issued a BWC shall wear it in accordance with policy."

While it is our opinion that these passages collectively satisfy the requirements described in Clause 4 of the Policy section of this report, we recommend that WPD revise the wording quoted in the preceding

paragraph to clarify that an officer shall not only wear but also operate his or her BWC in accordance with WPD's BWC policy when acting under the command and control of another chief law enforcement officer or federal law enforcement official.

Prior to the issuance of this report, WPD submitted a revised BWC policy that addresses the recommendation in the preceding paragraph.

In our opinion, WPD's revised BWC policy meets the compliance and disciplinary requirements specified in §626.8473 Subd. 3(b)(3) and (12).

WPD BWC Program and Inventory

WPD currently possesses five (5) Motorola/WatchGuard V300 body-worn cameras.

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

While WPD does not maintain a separate log of BWC deployment or use, Chief Anderson advised us that because each patrol officer wears a BWC while on duty, the number of BWC units deployed each shift can be determined based on a review of WPD payroll records. In addition, the WatchGuard Evidence Library Cloud service has a GPS function that displays the location of a deployed BWC. BWC use would be determined based on the creation of BWC data.

Chief Anderson was unable to determine the amount of retained BWC data WPD had at the time of the audit. After consulting with WatchGuard, he subsequently advised us that WPD had 1166 retained BWC "events" as of 9/05/2025.

WPD BWC Physical, Technological and Procedural Safeguards

WPD BWC data are initially recorded to an internal hard drive in each officer's BWC. Those files are then uploaded automatically to WatchGuard's Evidence Library cloud service when the officer physically docks his or her BWC at the Winthrop Police Department office.

Officers have view-only access to their own BWC data for report writing, trial preparation and other legitimate law enforcement purposes. All such access is logged and can be reviewed by WPD supervisors.

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 Use and Documentation section of WPD's BWC policy states: "Officers should wear their issued BWC's in an approved, conspicuous location on their body at or above the midline of the waist to maximize the recording capabilities of the officers [sic] activities." We recommend that WPD replace "should" with "shall" in the preceding passage to clarify that this location is mandatory.

Prior to the issuance of this report, WPD submitted a revised BWC policy that addresses the recommendation in the preceding paragraph.

Enhanced Surveillance Technology

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

If WPD should obtain such enhanced technology in the future, Minnesota Statute §13.825 Subd. 10 requires notice to the Minnesota Bureau of Criminal Apprehension within 10 days. This notice must include a description of the technology and its surveillance capability and intended uses.

Data Sampling

Rampart selected a random sample of 132 calls for service from which to review any available BWC recordings. It should be noted that not every call will result in an officer activating his or her BWC. For example, an officer who responds to a driving complaint but is unable to locate the suspect vehicle would be unlikely to activate his or her BWC. It should also be noted that because the audit covers a period of two years, while most BWC data is only required to be retained for 90 days, there is a significant likelihood that the sample population will include 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 WPD records.

Audit Conclusions

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

Rampart Audit, LLC

10/13/2025

APPENDIX A:

Winthrop Police Department

Policy # 17

Body Worn Cameras

17.1 INTRODUCTION

It is our mission to provide superior law enforcement services through the advancement of technology. To further achieve this goal, body-worn cameras will be used for the purpose of documenting evidence and accurately capturing contacts between members of the department and the public. The Winthrop Police Department is committed to the utilization of body-worn cameras as a means to reach this goal.

17.2 PURPOSE

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

17.2.1 DEFINITIONS

Definitions related to this policy include:

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

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

(c) **Records Retention Schedule:** refers to the General Records Retention Schedule for Minnesota Cities.

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

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

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

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

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

(h) **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.

(i) **Official Duties:** for purposes of this policy, means that the officer is on duty and performing authorized law enforcement services on behalf of this department.

17.3 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 Administrator.

17.4 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 above the mid-line of the waist to maximize the recording capabilities of the officers activities.

(d) Officers must document BWC use, and non-use as follows:

1. Whenever an officer makes a recording, the existence of the recording shall be documented.

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 agency.

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 17.3, will be mentioned in the quarterly report to the City Administrator as found in section 17.10 (a).

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

17.5 GENERAL GUIDELINES FOR RECORDING

(a) Officers shall activate their BWC's when anticipating that they will be involved in, become involved in, or witness other officers of this agency involved in a pursuit, motor vehicle stops, stop of a motorist or pedestrian, search, seizure, arrest, use of force, adversarial contact, and during other activities likely to yield information having evidentiary value. However, officers need not activate their cameras when it would be unsafe, impossible, or impractical to do so, but such instances of not recording when otherwise required must be documented as specified in the Use and Documentation guidelines, section 17.4 (d)(2) (above).

(b) Any member assigned to a non-uniformed position (Investigators, DTF, Training) may carry an approved BWC at any time the member believes the device may be useful. School Resource Officers (SRO) shall carry their BWC while working in their capacity as an SRO.

(c) Officers have discretion to record or not record general citizen contacts.

(d) Officers have no affirmative duty to inform people that a BWC is being operated or that the individuals are being recorded.

(e) Once activated, the BWC should continue recording until the conclusion of the incident or encounter, or until it becomes apparent that additional recording is unlikely to capture information having evidentiary value. The officer having charge of a scene shall likewise direct the discontinuance of recording when further recording is unlikely to capture additional information having evidentiary value. If the recording is discontinued while an investigation, response, or incident is ongoing, officers shall state the reasons for ceasing the

recording on camera before deactivating their BWC. If circumstances change, officers shall reactivate their cameras as required by this policy to capture information having evidentiary value.

(f) Officers shall not intentionally block the BWC's audio or visual recording functionality to defeat the purposes of this policy.

(g) In documented circumstances on the BWC audio, Officers who wish to discuss additional steps regarding the circumstances of a given law enforcement encounter; with fellow law enforcement officers or officers of the court, they have the discretion to temporarily and manually mute the audio recording function to do so, so long as the following happen:

1. Officers must manually mute the device.
2. The device is not muted for longer than necessary to complete the discussion with other Law Enforcement Officers or Officers of the Court.

(h) Notwithstanding any other provision in this policy, officers shall not use their BWC's to record other agency personnel during non-enforcement related activities, such as pre- and post-shift time in locker rooms, during meal breaks, or during other private conversations, unless recording is authorized as part of an administrative or criminal investigation.

17.6 SPECIAL GUIDELINES FOR RECORDING

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

(a) To use their BWC's to record any police-citizen encounter if there is reason to believe the recording would potentially yield information having evidentiary value, unless such recording is otherwise expressly prohibited.

(b) To use their BWC's to take recorded statements from persons believed to be victims of and witnesses to crimes, and persons suspected of committing crimes, considering the needs of the investigation and the circumstances pertaining to the victim, witness, or suspect.

In addition,

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

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

(e) Many portable recorders, including BWC's 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.

17.7 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.

1. Traffic Warning
2. Traffic Citation
3. Traffic Accident
4. Agency Assist
5. Animal Complaint
6. Arrest
7. Assault/Domestic
8. Agency/Motorist Assist
9. Burglary/Theft
10. Civil Issue
11. Drugs
12. DWI
13. Medical
14. Suspicious Activity
15. Test
16. Warrant
17. Welfare Check

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

(d) Labeling and flagging designations may be corrected or amended based on additional information.

17.8 ADMINISTERING ACCESS TO BWC DATA

(a) **Data subjects:** Under Minnesota law, the following are considered data subjects for purposes of administering access to BWC data:

1. Any person or entity whose image or voice is documented in the data
2. The officer who collected the data
3. Any other officer whose voice or image is documented in the data, regardless of whether that officer is or can be identified by the recording

(b) **BWC data is presumptively private:** BWC recordings are classified as private data about the data subjects unless there is a specific law that provides differently. As a result:

1. BWC data pertaining to people is presumed private, as is BWC data pertaining to businesses or other entities
2. Some BWC data is classified as confidential (see c below)
3. Some BWC data is classified as public (see d below)

(c) **Confidential data:** BWC data that is collected or created as part of an active criminal investigation is confidential. This classification takes precedence over the "private" classification listed above and the "public" classifications listed below.

(d) **Public data:** The following BWC data is public:

1. Data documenting the discharge of a firearm by a peace officer in the course of duty, other than for training or the killing of an animal that is sick, injured, or dangerous
2. Data that documents the use of force by a peace officer that results in substantial bodily harm
3. Data that a data subject requests to be made accessible to the public, subject to redaction. Data on any data subject (other than a peace officer) who has not consented to the public release must be redacted 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 Administrative Manager, 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:
    i. If the data was collected or created as part of an active investigation.
    ii. To portions of the data that the agency would otherwise be prohibited by law from disclosing to the person seeking access, such as portions that would reveal identities protected by Minn. Stat. § 13.82, subd. 17.
2. Unless the data is part of an active investigation, an individual data subject shall be provided with a copy of the recording upon request, but subject to the following guidelines on redaction:
    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.
3. In the event that an individual dies as a result of a use of force by a peace officer, an involved officer's law enforcement agency must allow the following individuals, upon their request, to inspect all portable recording system data, redacted no more than what is required by law, documenting the incident within five days of the request.
    i. the deceased individual's next of kin;
    ii. the legal representative of the deceased individual's next of kin; and
    iii. the other parent of the deceased individual's child.
    iv. A law enforcement agency may deny a request if the agency determines that there is a compelling reason that inspection would interfere with an active investigation. If the agency denies access, the chief law enforcement officer must provide a prompt, written denial to the individual who requested the data with a short description of the compelling reason access was denied and must provide notice that relief may be sought from the district court pursuant to section 13.82, subdivision 7;
4. In the event that an individual dies as a result of a use of force by a peace officer, an involved officer's law enforcement agency shall release all portable recording system data, redacted no more than what is required by law,

documenting the incident no later than 14 days after the incident, unless the chief law enforcement officer asserts in writing that the public classification would interfere with an ongoing investigation, in which case the data remain classified by section 13.82, subdivision 7;

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

1. Officers may access and view stored BWC video only when there is a business need for doing so, including the need to defend against an allegation of misconduct or substandard performance. 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. Agency personnel shall document their reasons for accessing stored BWC data at the time of each access. Agency personnel are prohibited from accessing BWC data for non-business reasons and from sharing the data for non-law enforcement related purposes, including but not limited to uploading BWC data recorded or maintained by this agency to public and social media websites.

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

(g) **Other authorized disclosures of data:** Officers may display portions of BWC footage to witnesses as necessary for purposes of investigation as allowed by Minn. Stat. § 13.82, subd. 15, as may be amended from time to time. Officers should generally limit these displays in order to protect against the incidental disclosure of 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.

17.9 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 agency shall obtain an independent biennial audit of its BWC program.

17.10 AGENCY USE OF DATA

(a) At least once a month, the Police Chief will randomly review BWC usage by each officer to ensure compliance with this policy.

(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.

17.11 DATA RETENTION

(a) All BWC data shall be retained for a minimum period of 90 days. There are no exceptions for erroneously recorded or non-evidentiary data.

(b) Data documenting the discharge of a firearm by a peace officer in the course of duty, other than for training or the killing of an animal that is sick, injured, or dangerous, must be maintained for a minimum period of one year.

(c) Data that documents the use of deadly force by a peace officer, or force of a sufficient type or degree to require a use of force report or supervisory review must be retained according to the department's record retention schedule.

(d) Data documenting circumstances that have given rise to a formal inquiry against an officer must be retained according to the department's record retention schedule.

(e) Other data having evidentiary value shall be retained for the period specified in the Records Retention Schedule. When a particular recording is subject to multiple

retention periods, it shall be maintained for the longest applicable period.

(f) Subject to Part g (below), all other BWC footage that is classified as non-evidentiary, becomes classified as non-evidentiary, or is not maintained for training shall be destroyed after 90 days.

(g) Upon written request by a BWC data subject, the Department shall retain a recording pertaining to that subject for an additional time period requested by the subject of up to 180 days. The Department will notify the requestor at the time of the request that the data will then be destroyed unless a new written request is received.

(h) The Department shall maintain an inventory of BWC recordings having evidentiary value.

(i) The Department will post this policy, together with its Records Retention Schedule, on its website.

17.12 COMPLIANCE

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

17.14 CONCLUSION

The use of this technology will add a higher level of transparency of the professional services provided by Winthrop 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.

Logan Anderson

Logan Anderson, Chief of Police
Winthrop Police Department

APPENDIX B:

17.1 INTRODUCTION & POLICY

It is our mission to provide superior law enforcement services through the advancement of technology. To further achieve this goal, body-worn cameras will be used for the purpose of documenting evidence and accurately capturing contacts between members of the department and the public. The Winthrop Police Department is committed to the utilization of body-worn cameras as a means to reach this goal.

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 Administrator and/or City Council.

17.2 PURPOSE

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

17.3 DEFINITION

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

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

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

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

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

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

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

h) **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.

i) **Official Duties**: for purposes of this policy, means that the officer is on duty and performing authorized law enforcement services on behalf of this department.

17.4 PROCEDURE

a) USE AND DOCUMENTATION

1) 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.

2) 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.

3) Officers shall wear their issued BWC's in an approved, conspicuous location on their body above the mid-line of the waist to maximize the recording capabilities of the officers activities.
4) Officers must document BWC use, and non-use as follows:
   i) Whenever an officer makes a recording, the existence of the recording shall be documented.

   ii) 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.
   iii) 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 agency.
      (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 17.3, will be mentioned in the quarterly report to the City Administrator as found in section 17.10 (a).
   iv) While under the command and control of another chief law enforcement officer or federal law enforcement official, officers issued a BWC shall wear and operate it in accordance with policy.

b) GENERAL GUIDELINES FOR RECORDING

1) Officers shall activate their BWC's when anticipating that they will be involved in, become involved in, or witness other officers of this agency involved in a pursuit, motor vehicle stops, stop of a motorist or pedestrian, search, seizure, arrest, use of force, adversarial contact, and during other activities likely to yield information having evidentiary value. However, officers need not activate their cameras when it would be unsafe, impossible, or impractical to do so, but such instances of not recording when otherwise required must be documented as specified in the Use and Documentation guidelines, section 17.4 (d)(2) (above).
2) Any member assigned to a non-uniformed position (Investigators, DTF, Training) may carry an approved BWC at any time the member believes the device may be useful. School Resource Officers (SRO) shall carry their BWC while working in their capacity as an SRO.
3) Officers have discretion to record or not record general citizen contacts.
4) Officers have no affirmative duty to inform people that a BWC is being operated or

that the individuals are being recorded.

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

5) Officers shall not intentionally block the BWC's audio or visual recording functionality to defeat the purposes of this policy.
6) In documented circumstances on the BWC audio, Officers who wish to discuss additional steps regarding the circumstances of a given law enforcement encounter; with fellow law enforcement officers or officers of the court, they have the discretion to temporarily and manually mute the audio recording function to do so, so long as the following happen:
   i) Officers must manually mute the device.
   ii) The device is not muted for longer than necessary to complete the discussion with other Law Enforcement Officers or Officers of the Court.
7) Notwithstanding any other provision in this policy, officers shall not use their BWC's to record other agency personnel during non-enforcement related activities, such as pre- and post-shift time in locker rooms, during meal breaks, or during other private conversations, unless recording is authorized as part of an administrative or criminal investigation.
8) There are no additional requirements to notify a data subject of a recording as Minnesota is a single party consent state.

c) SPECIAL GUIDELINES FOR RECORDING

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

1) To use their BWC's to record any police-citizen encounter if there is reason to believe the recording would potentially yield information having evidentiary value, unless such recording is otherwise expressly prohibited.
2) To use their BWC's to take recorded statements from persons believed to be victims of and witnesses to crimes, and persons suspected of committing crimes, considering the needs of the investigation and the circumstances pertaining to the victim, witness, or suspect.
3) Officers need not record persons being provided medical care unless there is reason to believe the recording would document information having evidentiary value. When responding to an apparent mental health crisis or event, BWC's shall be activated as

necessary to document any use of force and the basis for it, and any other information having evidentiary value, but need not be activated when doing so would serve only to record symptoms or behaviors believed to be attributable to the mental health issue.

Officers shall use their BWC's and squad-based audio/video systems to record their transportation and the physical transfer of persons in their custody to hospitals,

detox or mental health care facilities, juvenile detention centers, and jails, but otherwise should not record in these facilities unless the officer anticipates witnessing a criminal event, being involved in or witnessing an adversarial encounter or use-of-force incident.

4) Many portable recorders, including BWC's 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.

d) DOWNLOADING AND LABELING DATA

1) 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.
2) 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.
   i) Traffic Warning
   ii) Traffic Citation
   iii) Traffic Accident
   iv) Agency Assist
   v) Animal Complaint
   vi) Arrest
   vii) Assault/Domestic
   viii) Agency/Motorist Assist
   ix) Burglary/Theft
   x) Civil Issue
   xi) Drugs
   xii) DWI
   xiii) Medical
   xiv) Suspicious Activity
   xv) Test
   xvi) Warrant
   xvii) Welfare Check
3) 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:
   i) Victims and alleged victims of criminal sexual conduct and/or sex trafficking

ii) Victims of child abuse or neglect
iii) Vulnerable adults who are victims of maltreatment
iv) Undercover officers
v) Informants
vi) When the video is clearly offensive to common sensitivities
vii) Victims of, and witnesses to crimes, if the victim or witness has requested not to be identified publicly
viii) Individuals who called 911, and services subscribers whose lines were used to place a call to the 911 system
ix) Mandated reporters
x) Juvenile witnesses, if the nature of the event or activity justifies protecting the identity of the witness.
xi) Juveniles who are, or may be delinquent or engaged in criminal acts
xii) Individuals who make complaints about violations with respect to the use of real property
xiii) Officers and employees who are the subject of an inquiry related to the events captured on video
xiv) Other individuals whose identities the officer believes may be legally protected from public disclosure

4) Labeling and flagging designations may be corrected or amended based on additional information.

e) ADMINISTERING ACCESS TO BWC DATA

1) **Data subjects:** Under Minnesota law, the following are considered data subjects for purposes of administering access to BWC data:
   i) Any person or entity whose image or voice is documented in the data
   ii) The officer who collected the data
   iii) 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
2) **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:
   i) BWC data pertaining to people is presumed private, as is BWC data pertaining to businesses or other entities
   ii) Some BWC data is classified as confidential (see 3 below)
   iii) Some BWC data is classified as public (see 4 below)
3) **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.
4) **Public data:** The following BWC data is public:

i) 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
ii) Data that documents the use of force by a peace officer that results in substantial bodily harm
iii) 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.
iv) 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

f) Access to BWC data by non-employees: Officers shall refer members of the media or public seeking access to BWC data to the Administrative Manager, 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:
   i) If the data was collected or created as part of an active investigation.
   ii) To portions of the data that the agency would otherwise be prohibited by law from disclosing to the person seeking access, such as portions that would reveal identities protected by Minn. Stat. § 13.82, subd. 17.
2) Unless the data is part of an active investigation, an individual data subject shall be provided with a copy of the recording upon request, but subject to the following guidelines on redaction:
   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.
3) In the event that an individual dies as a result of a use of force by a peace officer, an involved officer's law enforcement agency must allow the following individuals, upon their request, to inspect all portable recording system data, redacted no more than what is required by law, documenting the incident within five days of the request.

i) the deceased individual's next of kin;
ii) the legal representative of the deceased individual's next of kin; and
iii) the other parent of the deceased individual's child.
iv) A law enforcement agency may deny a request if the agency determines that there is a compelling reason that inspection would interfere with an active investigation. If the agency denies access, the chief law enforcement officer must provide a prompt, written denial to the individual who requested the data with a short description of the compelling reason access was denied and must provide notice that relief may be sought from the district court pursuant to section 13.82, subdivision 7;

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

g) 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) Agency personnel shall document their reasons for accessing stored BWC data at the time of each access. Agency personnel are prohibited from accessing BWC data for non-business reasons and from sharing the data for non-law enforcement related purposes, including but not limited to uploading BWC data recorded or maintained by this agency to public and social media websites.
3) Employees seeking access to BWC data for non-business reasons may make a request for it in the same manner as any member of the public.

h) 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.

i) DATA SECURITY SAFEGUARDS

1) 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.
2) Officers shall not intentionally edit, alter, or erase any BWC recording made with a peace officer's portable recording system or data and metadata related to the recording prior the expiration of the applicable retention period under section 13.825 Subdivision 3, except that the full, unedited, and (b) unredacted recording of a peace officer using deadly force must be maintained indefinitely.
3) As required by Minn. Stat. § 13.825, subd. 9, as may be amended from time to time, this agency shall obtain an independent biennial audit of its BWC program.

j) AGENCY USE OF DATA

1) At least once a month or as soon as practicable, the Police Chief will randomly review BWC usage by each full-time officer or part-time officer that has worked in the previous month to ensure compliance with this policy.
2) 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.
3) Nothing in this policy limits or prohibits the use of BWC data as evidence of misconduct or as a basis for discipline.
4) 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.

k) DATA RETENTION

1) All BWC data shall be retained for a minimum period of 90 days. There are no exceptions for erroneously recorded or non-evidentiary data.

2) 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, and data documenting the use of force by a peace officer that results in substantial bodily harm must be retained for a minimum period of one year.
3) Data that documents the use of deadly force by a peace officer, or force of a sufficient type or degree to require a use of force report or supervisory review must be retained indefinitely.
4) BWC data documenting circumstances that have given rise to a formal complaint against an officer shall be retained for a minimum period of one year.
5) Other data having evidentiary value shall be retained for the period specified in the Records Retention Schedule. When a particular recording is subject to multiple retention periods, it shall be maintained for the longest applicable period.
6) Subject to Part g (below), all other BWC footage that is classified as non-evidentiary, becomes classified as non-evidentiary, or is not maintained for training shall be destroyed after 90 days.
7) Upon written request by a BWC data subject, the Department shall retain a recording pertaining to that subject for an additional time period requested by the subject of up to 180 days. The Department will notify the requestor at the time of the request that the data will then be destroyed unless a new written request is received.
8) The Department shall maintain an inventory of BWC recordings having evidentiary value.
9) The Department will post this policy, together with its Records Retention Schedule, on its website.

l) COMPLIANCE

1) 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.

m) CONCLUSION

1) The use of this technology will add a higher level of transparency of the professional services provided by Winthrop 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.

17.5 RETENTION SCHEDULE

Category	Retention
Uncategorized	2 Years
Animal Complaint	90 Days
Test	90 Days
Welfare Check	90 Days
Traffic Warning	90 Days
Civil Issue	90 Days
Medical	90 Days
Traffic Accident	1 Year
Traffic Citation	1 Year
Arrest	1 Year
Assault/Domestic	1 Year
Burglary/Theft	1 Year
DWI	1 Year
Suspicious Activity	1 Year
Warrant	1 Year
Drugs	1 Year
Agency/Motorist Assist	1 Year

Logan Anderson

Logan Anderson, Chief of Police
Winthrop Police Department