442.18 Body Worn Camera Policy

INTRODUCTION

This General Order provides guidelines for the Saint Paul Police Department (SPPD) Body Worn Camera (BWC) system. This includes use of the BWC system, storage and retention, and review and dissemination of data. General Order 442.17 governs the In-Car Camera System (ICC). The rights and requirements of Minnesota Statutes section 13.825 are incorporated by reference into this policy and personnel should review and follow the current statute when there are policy conflicts or questions. (MN Statute 13.825)

SECTION 1. DEFINITIONS

A. Axon - The vendor selected by the department to provide BWCs and evidence.com, a cloud-based system for uploading, managing and storing BWC data.

B. Activate - To manually begin recording. Department BWCs do not automatically record. Officers must intentionally start the recording. If the camera is powered on prior to the activation of recording, it will create a 30-second buffer of video only.

C. BWC Quality Control Sergeant - Sergeant assigned to the technology unit responsible for auditing BWC use to confirm compliance with the requirements of this policy. General Order 442.19 governs the Quality Control Process.

D. Buffer - A vendor-configured component of the BWC that records 30 seconds of video only, without audio, prior to a BWC activation. The buffer records only when the BWC is powered on. Audio recording begins when an officer activates recording.

E. BWC Data - Audio and/or video data as defined by Minnesota Statute 13.825 collected by a department BWC.

F. BWC Data Technicians - Video management unit (VMU) and closed-circuit television (CCTV) staff trained in the operational use of BWCs, data copying methods, data storage and retrieval methods and procedures, and who possess a working knowledge of video forensics, evidentiary procedures and the MGDPA.

G. BWC Modes of Operation [Off, On-Buffering, On-Recording]

1) Off - The switch of the BWC is in the off position, indicated by the switch positioned towards the outside of the camera with no orange mark visible. The camera does not buffer or record in the off mode.

2) On - Buffering. The switch is positioned towards the center of the camera. An orange mark is visible. The camera is powered on, in standby mode, and buffering in a 30-second loop. The buffer records video only, no audio. The camera must typically be worn in the on-buffering position.

3) On - Recording. The BWC has been activated by the officer to record. Audio joins the buffer at the point the BWC is activated by the officer. Recording continues until the officer stops recording by returning the BWC to on-buffering mode or by turning the BWC off.

H. Categories - Labels given to BWC Data relating to predetermined retention schedules:

1) Misc./Equip Maint./ Training

2) Civil/ Morgan Plan

3) General Citizen Contact

4) Traffic Stop (Non-Arrest)

5) Squad Accident / AWI

6) Vehicle Pursuit

7) Arrest / Evidence / RRA

8) CSC

9) Investigation of a Death/Admin Hold

I. Critical Incident - Defined by General Order 246.09: Investigations - Incidents Where Serious Injury or Death Result during Police Custody in Involvement.

J. Deactivate - to stop recording.

K. Discretionary recording - when officers have the discretion to activate their BWC.

L. Evidence.com - A cloud-based system provided by Axon to upload, manage and store BWC data. Accounts, permissions and roles within evidence.com are administered by the technology unit.

M. ICC – In-Car Camera - See General Order 442.17.

N. Inventory control - The process whereby a BWC is issued to a specific officer and a collection of spare cameras is maintained. The radio shop will manage the overall inventory of all department BWCs and docking stations. The designated district or unit administrative sergeant is responsible for BWCs assigned to their district or unit and must report district BWC inventories to the radio shop.

O. MGDPA - Minnesota Government Data Practices Act defined by Minnesota State Statute chapter 13.

P. Memorandum of Understanding (MOU) – An agreement outlining the terms and conditions of any assignment or deputizing of Saint Paul Officers to a federal task force.

Q. Metadata - Information related to BWC data. This includes the date, time, case number, and name of the officer to whom the camera is assigned. Metadata also includes categorization of the video, which sets video retention. Officers may also add optional searchable notes as metadata.

R. Mandatory Recording - When the BWC must be activated under this policy.

S. Mute - Using the capability of the BWC to stop audio recording while continuing to record video.

T. Officer - the term officer is used generically throughout this policy for ease of reference. For unity of purpose it is important to note that within this policy "officer" refers to all sworn members of the Saint Paul Police Department who are issued a camera or authorized to wear one and who have been properly trained in its use.

U. Prohibited recording - When an officer is prohibited from recording under this policy. A recording may be prohibited in a situation (i.e.: interacting with a CSC victim) or in a physical location (i.e.: in a police facility). Inadvertent prohibited recordings will be managed by the video management unit.

V. Raid Gear Uniform - See General Order 202.04 Non-Uniformed Personnel-Classes and Rules.

W. Task Force Officer- A St. Paul Police officer assigned to a federal law enforcement agency as a federally deputized task force officer.

X. Technology Unit Commander - Oversees the technical aspects of the BWC program. This includes but is not limited to oversight of evidence.com, the video management unit, technology updates related to BWCs, Quality Control Process, as well as working with the Training Commander to ensure proper ongoing training of all officers assigned BWCs.

Y. Temporary Tactical Uniform: See General Order 202.04 Non-Uniformed Personnel-Classes and Rules.

Z. Training Unit Commander - Works with the Technology Unit Commander to ensure proper and ongoing training of officers related to BWCs.

AA. Video Management Unit (VMU) - Led by a sergeant and assigned under the technology unit. Responsible for BWC/ICC/CCTV data. Staffed with Data Release Technicians who possess a working knowledge of video forensics and evidentiary procedure. This unit will have responsibility for all BWC data released.

SECTION 2. OVERVIEW

This policy sets out guidelines governing the use of BWCs and administration of BWC Data. Compliance with this policy is mandatory. This policy recognizes 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.

BWC Data may be used for law enforcement purposes, internal review and use pursuant to this policy, or public access pursuant to the MGDPA and Minnesota Statutes section 626.8473.

SECTION 3. OPERATIONAL OBJECTIVES.

Operational objectives include the list below:

- Use of best practices in the rapidly evolving field of law enforcement
- Enhance officer and public safety
- Enhance officers' ability to document and review statements and actions for reporting requirements and for courtroom preparation
- Promote transparency, accountability, and build community trust
- Collect evidence for use in criminal investigations and prosecutions
- Deter criminal activity and uncooperative behavior
- Aid in the documentation of statements and events during the course of an incident
- Provide additional information for training
- Assist in the investigation and reviewing of complaints

SECTION 4. ISSUANCE OF BODY-WORN CAMERAS (BWCs)

As determined by the Chief of Police, BWCs will be issued to all sworn officers.

SECTION 5. BWC USE BY OFFICERS

Officers must use the device according to this policy and as trained, and may not interfere with the proper functioning of the BWC. All sworn Officers are required to wear the BWC as described in this policy. Only Department issued and maintained body worn cameras may be used by officers.

A. Working on-duty, regular or overtime.

Officers must wear their BWC as part of the uniform when working on-duty (regular or overtime) and wearing the uniform of the day as defined by General Order 202.03 or raid gear or temporary tactical gear as defined by General Order 202.04.

B. Working off-duty in a uniform.

Officers must wear their BWC as part of the uniform when working off-duty in the uniform of the day as defined by General Order 202.03 or raid gear or temporary tactical gear as defined by General Order 202.04.

C. Plain clothes officer.

The supervisor of a plain clothes or undercover officer may dictate whether an on-duty officer will use a BWC when working in plain clothes. An officer in a plain clothes or undercover assignment must use an issued BWC when wearing the uniform of the day, raid gear or temporary tactical gear.

D. Task Force Officers

All St. Paul Police Officers assigned to a task force with federal law enforcement agencies are required to wear a BWC pursuant to G.O. 442.18, whether acting under authorization of their deputation or as a SPPD officer.

The Chief of Police or his/her designee may grant exemptions to this requirement. Additionally, Ordinance Disposal Unit (Bomb Squad) personnel are exempted from wearing a BWC over their protective gear when performing Bomb Squad functions under G.O. 463.01.

SECTION 6. INVENTORY CONTROL

The radio shop will manage the department inventory of BWC devices. The district or unit administrative sergeant will work with the radio shop for accurate accounting of BWCs assigned to district or unit personnel.

.

SECTION 7. BWC TESTING AND MECHANICAL FAILURES

Officers wearing a BWC must test the functioning of the BWC in accordance with their training at the beginning of each shift. Officers may not wear a BWC that fails the daily test. If an officer becomes aware of a BWC malfunction during their shift, they must exchange the BWC as soon as practically possible.

Regardless of whether a malfunctioning BWC is believed to contain evidence, all BWCs requiring repair must be treated as if they contain evidence. Malfunctioning BWCs will be turned into the property room. Officers with a malfunctioning BWC will:

- Contact a supervisor to facilitate obtaining a new BWC from the spares available to their district or unit.
- The supervisor will ensure that the new BWC is assigned to the officer in the Axon evidence.com system.
- The malfunctioning camera will remain assigned to the officer until all data has been uploaded from the malfunctioning camera as part of the repair process.

- Create a separate case number for Service to Body Camera (SBC).
- Complete an original report under the SBC case number describing:
  - The malfunctioning BWC serial number.
  - The new BWC serial number.
  - A brief description of the malfunction.
  - Whether the malfunctioning BWC is known or believed to contain data.
- Turn the malfunctioning BWC into a property locker or the property room following the same procedures applicable to all other evidence as outlined in General Order 439.02.

SECTION 8. BWC MOUNTS AND WEARING THE BWC

A. Mounts

a. Officers shall wear the BWC using one of the mounts provided by the department or available for purchase from Axon.com/buy.

b. Two magnetic mounts and a Z-clip mount are issued with the BWC. Officers may replace damaged or lost mounts or purchase additional at Axon.com/buy after creating an account at Axon.com/buy.

c. Mounts which have been damaged during the course of duty may be reimbursed per General Order 202.08.

d. Officers wishing to order additional mounts beyond the magnetic and Z-clip mounts will be reimbursed for up to 3 mounts per year from any available funds in the officer's uniform allowance.

B. Wearing the BWC

a. Officers must wear their BWC above the midline of their torso, facing forward, and unobstructed by any equipment or clothing (jacket, traffic vest, etc.). Officers shall not allow anything to obstruct the view of their BWC. Those officers issued the Axon Flex camera will mount the camera in accordance with their training, the camera facing forward to replicate the direction and view of the torso-mounted cameras.

b. BWCs must only be used for their intended operational objectives. During such use, it may be advantageous to temporarily remove the camera, including when

clearing a corner or attic or some other legitimate purpose. Any use of a BWC other than on an officer's uniform should be documented in a police report, or if a report is not otherwise necessary, CAD comments or citation notes.

SECTION 9. MANDATORY, DISCRETIONARY, AND PROHIBITED RECORDING

A. Mandatory Recording

Understanding that officers encounter tense, uncertain, and rapidly evolving situations, officers must activate their BWC at their earliest opportunity and before arriving on scene when recording is required by this policy.

Activating a BWC early, before an officer arrives on scene, allows an officer to safely turn on the BWC before reacting to or dealing with the circumstances of a particular call, incident, investigation or event. This also helps document important information from a view closer to that of the officer's perspective. Therefore, officers must activate their BWCs when preparing for or initiating any law enforcement action, when responding to any call or incident, and before arriving on scene in the following circumstances and conditions:

- When an officer is dispatched to or investigating any call or incident.
- When an officer is assisting another officer at a call or incident.
- When an officer is participating in any of the following police actions:
    - Any vehicle stop including traffic and investigative stops.
    - Vehicle pursuits.
    - Investigative stops of individuals.
    - Initiating any arrest.
    - All frisks and searches (e.g., suspect, vehicle, structure, physical area).
    - All strip searches must be conducted in accordance with General Order 409.08 and will only be audio recorded with the BWC.
    - When encountering or responding to resistance or aggression. See General Orders 246.00, 246.01.
    - When any situation becomes adversarial, including situations which are either verbally or physically adversarial
    - In-custody transports.

- Suspect interviews in the field, including in-custody interviews occurring in the field when the Miranda warning is required.
- When directed by a supervisor.
- While operating a vehicle under General Order 444.01 Emergency Runs.

If an officer is at a location or in any situation where an event occurs or develops where this policy mandates recording and their BWC is not already activated, the officer must activate the BWC as soon as activation is possible and safe.

B. Discretionary Recording

This policy does not describe every possible situation where the BWC may be activated. Beyond the mandated scenarios described above, an officer may activate the BWC when they believe it should be activated based on their training, experience, and judgement, except when recording is prohibited under this policy. If an officer is involved in a situation and they are unsure if the activation is mandatory, discretionary or prohibited, they should activate the BWC.

C. Prohibited Recording

- Interactions solely among other department employees when not actively investigating or assigned to a call or incident.
- Non-work-related activity.
- Within areas of a police facility restricted to personnel-only access, including roll call rooms, locker rooms, break rooms, and report rooms. BWCs should only record citizen contacts inside a police facility if relevant to an investigation or to comply with the Mandatory Recording situations described in this policy.
- When interacting with undercover officers or confidential informants, or persons providing information based on confidentiality, unless necessary for a law enforcement investigation or to comply with the Mandatory Recording situations described in this policy.
- During a work break.
- At any location where a reasonable expectation of privacy exists, such as a bathroom or locker room, unless necessary for a law enforcement investigation or to comply with the Mandatory Recording situations described in this policy.
- In patient care areas of a hospital, sexual assault treatment center, or other healthcare facility unless necessary for a law enforcement investigation or to comply with the Mandatory Recording situations described in this policy.

This policy recognizes that officers encounter tense, uncertain, and rapidly evolving situations regardless of location. Given this fact, officers may unintentionally create a prohibited recording or may intentionally record to comply with the Mandatory Recording

requirements of this policy. The VMU will manage all data recorded in scenarios which this policy prohibits.

Officers who are aware an undercover officer has been recorded on a BWC shall email the VMU with specific information at SPPD-VMU@ci.stpaul.mn.us. UC officers include those assigned to the narcotics unit, SIU, FBI Safe Street task force, etc.

Officers may also communicate any other information to the VMU regarding prohibited recordings or other BWC information by e-mail.

D. Victim or witness interviews must also be recorded, unless the officer becomes aware of the following:

- The identity of a victim or witness is protected by the MGDPA. Individuals whose identities are protected under the MGDPA include victims or alleged victims of criminal sexual conduct or sex trafficking.
- An officer may deactivate recording to protect the identity of someone afforded protection under the MGDPA, provided the request does not conflict with any other Mandatory Recording requirement under this policy.
- A victim or witness has requested the officer deactivate recording, provided the request does not conflict with any other Mandatory Recording requirement under this policy.

Officers should consider the totality of the circumstances before deactivating recording and determine the best approach for a particular circumstance. For example, deactivation may be the best option if the situation is not adversarial and a BWC inhibits a victim or witness from providing information. Nothing precludes an officer who has deactivated recording under these circumstances from reactivating it should mandatory recording circumstances emerge, or the officer chooses to reactivate recording in their discretion.

Deactivation under these circumstances must be documented in an incident report, or if no incident report is otherwise required it must be documented in CAD comments.

This policy recognizes officers cannot or will not always know of or have time or opportunity to account for protections afforded under the MGDPA. An officer may also intentionally record an individual with MGDPA protections, or any witness or victim who has requested recording be deactivated, in order to comply with other sections of this policy. Compliance with the other Mandatory Recording requirements under this policy is the higher priority.

The VMU provides the final review to ensure appropriate management of data and compliance with the MGDPA.

Officers may communicate any information to the VMU regarding witness/victim recordings or BWC information by e-mail at SPPD-VMU@ci.stpaul.mn.us.

SECTION 10. FAILURE TO RECORD

Officer and public safety are the department's highest priorities. If an officer is unable to activate his or her BWC before one of the mandatory recording scenarios described in this policy, the BWC must be activated as soon as it is possible and safe.

Facts surrounding a failure to record must be reported to a supervisor and documented in an incident report, or if no incident report is required it must be documented in CAD comments. The supervisor notification should be made prior to the officer clearing the call, unless exigent circumstances exist. The officer must also submit a BWC self-reporting form prior to clearing the call, unless exigent circumstances exist. This form will record information about situations involving a failure to record and delayed activations.

If an officer is involved in a critical incident and they were unable or failed to record a mandatory record incident, any stated reason for the failure to record will be documented by an investigator assigned to the incident.

Officers involved in a critical incident who are not required to write a report are encouraged to provide any information as to their inability or failure to activate the BWC to the investigator under procedures outline in General Order 246.09 Critical Incident Policy, Responsibilities of Involved Employees.

SECTION 11. MUTING

Transparency is a critical component of the trust and partnership that the St Paul Police Department maintains with our community. As such, muting is not authorized.

SECTION 12. WHEN RECORDING MAY BE DEACTIVATED

The rights and requirements of Minnesota Statutes section 13.825 are incorporated by reference into this policy and personnel should review and follow the current statute when there are policy conflicts or questions. (MN Statute 13.825)

Once activated, the BWC must remain on-recording until the incident has concluded; meaning it is reasonable to believe that all arrests are made, arrestees transported, and suspect interviews are completed, unless or until:

1) The incident or event is of such duration that recording is deactivated to conserve power or storage capacity and the officer is not directly involved in activity relating to the incident or event.

2) In a Critical Incident, the supervisor has ordered deactivation – As per G.O. 246.09 Critical Incidents.

3) Deactivation is reasonable and necessary to protect the safety of the officers or others.

4) Deactivation is approved or ordered by a supervisor.

5) BWCs may be deactivated during non-enforcement activities, such as waiting for a tow truck or protecting accident scenes.

6) At search warrant scenes, the cameras may be deactivated once the entry is complete and the scene is safe. This deactivation can **only** occur after all occupants are removed from the warrant location. If removing all occupants is not possible or reasonable, at a minimum the cover officer(s) will have their BWC on. The remaining searching officers may deactivate their BWC's. The BWC does not replace the officer's obligation for photographs of the warrant scene, highlighted under policy 447.

An officer's decision to deactivate recording in a situation that would otherwise be recorded under this policy must be documented verbally on the camera before deactivation. That decision must also be noted in an incident report, or if no incident report is otherwise required the decision must be documented in CAD comments. The report or CAD comments must include factors considered in the decision to deactivate the camera off.

BWCs may also be deactivated after the officer has arrived on scene, assessed and stabilized the call, and if the officer reasonably believes there is no longer necessary audio or visual evidence to capture and that none of the circumstances requiring activation will likely occur.

Nothing in this section is intended to discourage an officer from recording during non-enforcement situations when in his or her judgement the recording may be beneficial.

SECTION 13. WEARING A BWC INSIDE A COURT BUILDING

The rights and requirements of Minnesota Statutes section 13.825 are incorporated by reference into this policy and personnel should review and follow the current statute when there are policy conflicts or questions. (MN Statute 13.825)

Ramsey County District Court order dated February 17, 2017, states that "Only law enforcement personal may have body cameras in a courtroom. These Electronic Devices may be powered on but must be kept and operated only in silent mode. Any authorized use of these Electronic Devices must not distract the proceedings pursuant to the Rules of Decorum. In addition, voice communication and the recording of pictures, video or audio are prohibited in courtrooms unless specifically approved by the presiding judge or judicial officer pursuant to Rule 4.02 of the Rules of General Practice."

This court order does not preclude an officer responding to an incident in the courthouse from recording as required by this policy.

SECTION 14. DUTY TO NOTIFY PERSONS OF BWC RECORDING

The rights and requirements of Minnesota Statutes section 13.825 are incorporated by reference into this policy and personnel should review and follow the current statute when there are policy

conflicts or questions. (MN Statute 13.825)

If an individual asks an officer if a BWC is on or recording, research and experience shows the best practice is to tell individuals they are being recorded. While not required by law (MN Statute 626A.02, subdivision 2), the Saint Paul Police Department strongly encourages officers to tell people that they are being recorded, unless the officer believes that disclosure would result in a safety issue for the officer or public.

Section 13.04, subdivision 2, does not apply to collection of body worn camera data.

SECTION 15. DATA CATEGORIZATION AND DEPARTMENT-ISSUED PHONES

A. Categorization

All data collected by BWCs is subject to statutory requirements and may also be considered evidence. The timely and accurate categorization of data is vitally important to determine the retention of data. Officers must ensure all BWC recordings are assigned a case number and correct category by the end of their next duty shift. Officers should contact a supervisor with any questions about appropriate categorization. Officers should assign as many of the following categories as are applicable to each file:

CATEGORY	RETENTION PERIOD
**Misc./Equip Maint./Training	1 year
Civil/Morgan Plan	1 year
General Citizen Contact	1 year
None	1 year
Traffic Stop (Non-Arrest)	1.5 years
Squad Accident/AWI	3 years
Vehicle Pursuit	6 years
Arrest/Evidence/RRA	7 years
CSC	9 years
Investigation of a Death/Admin Hold	No Expiration
Pending Review	No Expiration
*Officer Discharge of a Firearm	No Expiration

*Excludes training and killing of an animal that is sick, injured or dangerous.

B. **Training videos created as a part of the recruit academy will be retained for a minimum of 90 days and may be purged with the authorization from the Chief of Police or his/her designee.BWC recording may be retained for as long as reasonably necessary for possible evidentiary or exculpatory use

related to the incident with respect to which the data were collected.

C. CAD/RMS Integration

The CAD/ RMS integration is a feature of the system that will attempt to add a case number and a category to videos recorded by the officer. The CAD/RMS integration data that contains the time a call was dispatched to an officer and the time the officer cleared the call, will be compared to that officer's video in evidence.com. Where there is a match, the integration will add the case number and category to the video. Officers should be aware of instances where they are not assigned to a call at the time a recording is started, as these must be manually updated.

The CAD/RMS integration process only occurs after video has been uploaded to evidence.com. Officers are responsible for verifying that the CAD/RMS integration has updated the recordings with the correct case numbers and categories. Officers shall review their own recordings (using the evidence.com "My Evidence" page) to ensure that every recording they made has a case number and proper category. This shall be done no less than one time per work week.

Officers are responsible for ensuring that the data captured on their BWC is categorized and the correct CN attached to said data. Utilizing audit and search features of evidence.com, supervisors are responsible for ensuring data uploaded by subordinates has been categorized.

Officers shall manually update any call type of Previous Case Number (PCN) with the appropriate related case number and category. Often officers are assigned to a PCN call type in CAD while recovering a stolen car, following up on another call, or arresting someone on a pc pickup. The evidence relates to the original case and needs to be manually updated in order to be visible to investigators and prosecutors. The CAD/RMS integration is unable to properly update these call types.

D. Department Issued cell phones

Officers issued a department cell phone may categorize data in the field using the Axon View application.

Department issued cell phones are subject to General Order 236.02 Internet Access and E-mail.

Officers may use the camera and video features of their department issued cellphones for scene photography and other legitimate law enforcement purposes as trained. Refer to General Order 440.00 Digital Evidence and 424.01 Photograph, Audio and Video Recordings.

No personal devices may be used to update BWC data.

SECTION 16. UPLOADING DATA

All BWC data is subject to statutory requirements for retention and dissemination. Data captured on the BWC may also be evidentiary. Officers are responsible for ensuring the case number and correct category are attached to their videos.

All officers will upload BWC data daily when they are working regular duty, overtime or in an off-duty capacity. The department recognizes that officers may create BWC data during off-duty or overtime situations and will not have immediate access to upload the data. If an officer has recorded evidentiary data relating to an arrest and/or a Response to Resistance or Aggression (RRA), the officer must upload the BWC prior to end of their shift. If an officer is working in an off-duty or overtime capacity and has BWC data related to something other than an arrest and/or RRA, the officer should upload the data no later than the end of the officer's next regular shift.

For example: An officer working off-duty creates a video for an incident report or general citizen contact that does not result in an arrest or RRA. This officer should upload their video no later than their next scheduled shift.

An officer conducts a traffic stop on their way home that does not result in an arrest or RRA. This officer should upload their video no later than their next scheduled shift.

SECTION 17. CRITICAL OR SIGNIFICANT INCIDENTS

A. In the event of a Critical Incident all officers who are involved or who witness the incident shall turn off their BWCs only when instructed by a supervisor or investigator assigned to the incident. It is the responsibility of the scene supervisor to ensure compliance with this section.
    a. Note that General Order 246.09 Critical Incidents requires officers involved in a critical incident to give the first responding non-involved field supervisor a brief, factual, public safety statement of the event for the purpose of focusing the investigative efforts, which will include, but is not necessarily limited to assisting in identifying and locating suspects, victims, witnesses, evidence, and any other information deemed pertinent to public or officer safety.

B. All involved or responding officers must maintain custody of their BWC equipment until the forensic services unit or crime lab of the investigating agency takes custody of the equipment. In the event that an officer will be photographed as part of the investigation, the officer should leave their uniform intact, including BWC equipment, until photographs are completed. The department will ensure that all video is properly uploaded. Once all uploads are complete, BWC equipment will be returned to the officer, or their supervisor, unless the device itself is evidence beyond any data created by the BWC. If the BWC device is evidence it must be handled in the same manner as any other evidence.

C. In the event an outside agency crime lab or the forensic services unit does not respond to a Critical Incident, the supervisor must ensure BWC Data is properly uploaded before returning the BWC to the officer.

SECTION 18. PRIVATE, CONFIDENTIAL AND PUBLIC BWC DATA

All BWC data is the property of the department and is government data subject to the laws of the State of Minnesota.

Minnesota Statutes section 13.825, subdivision 2, defines BWC data as presumptively private data about the data subjects unless there is a specific law that makes the BWC data either confidential or public.

BWC data subjects are defined as:

- Any person or entity whose image or voice is documented in the data.
- The officer who collected the data.
- 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.

Confidential BWC data is collected or created as part of an active criminal investigation. Data is classified as confidential while the investigation is active. Inactive investigative data is classified according to rest of section 13.825.

Public BWC Data is defined as:

- Data documenting the discharge of a firearm by an officer in the course of duty, other than for training or the dispatching of an animal that is sick, injured, or dangerous.
- Data that documents the use of force by an officer resulting in substantial bodily harm. Substantial bodily harm is defined in Minnesota Statute section 609.02 as bodily injury which involves a temporary but substantial disfigurement, or which involves a temporary but substantial disfigurement, or which causes a temporary but substantial loss or impairment of the function of any bodily member or organ, or which causes a fracture of any bodily member.
- Data that a data subject requests to be made accessible to the public, subject to redaction. Data on any data subject (other than an officer) who has not consented to the public release must be redacted. In addition, data on undercover officers must be redacted.
- Data may be redacted, or access withheld to portions of data that are public, if those portions of data are clearly offensive to common sensibilities. A person seeking access to otherwise public data that have been withheld may bring an

action in district court to challenge this determination. The person bringing the action must give notice to the department and the subjects of the data. The department must give notice to any subjects of the data of which the department is aware and that were not provided notice by the person bringing the action for access. The rights of a defendant in a criminal proceeding to obtain access to body worn camera data are not affected by any determination by the department that the data are clearly offensive to common sensibilities.

- Data that documents the final disposition of a disciplinary action against a public employee.
- If another provision of the MGDPA classifies data as private or otherwise not public, that data retains the other MGDPA classification.

SECTION 19. ACCESS BY DATA SUBJECTS

A. As required by statute, an individual must be allowed to access BWC data about him/ herself as a subject of the recording, however access is not required under the following conditions:

- The data is collected or created as part of an active investigation.
- The data is restricted by law from disclosure to the person seeking access, such as portions that would reveal identities protected by Minnesota Statutes section 13.82, subdivision 17.

B. Unless the data is part of an active investigation, an individual data subject may request said video and must be provided with a copy of the recording redacted as follows:

- Data on other individuals in the recording who do not consent to the release must be redacted.
- The identities and activities of an on-duty peace officer engaged in an investigation or response to an emergency, incident or request for service may not be redacted unless the officer's identity is subject to protection under section 13.82, subdivision 17, clause (a) (when access to the data would reveal the identity of an undercover law enforcement officer).
- If a subject of the data submits a written request to retain the recording, the data must be retained for the period of time requested, up to an additional 180 days beyond the applicable retention period.
- VMU Sergeant will ensure the request is documented in Gov QA, adjust the

category retention period and notify the subject of the new expiration date. VMU Sergeant shall notify the requester that the recording will be destroyed when the requested time elapses (180 days) unless a new request is made.

SECTION 20. WHEN BWC DATA MAY BE WATCHED OR REVIEWED

A. Officers are authorized to access public and non-public (confidential or private) BWC data for legitimate law enforcement purposes, including but not limited to report writing. Nothing in this policy restricts an officer from reviewing data for law enforcement purposes, including for preparing to give a statement, preparing for court testimony or to respond to allegations of substandard performance or misconduct, excepting department policy under General Order 235.20 Administrative Lockdown.

B. BWC data may not be accessed or reviewed for the purpose of surveillance. Permitted use of BWC Data includes:

1) Case investigation.

An investigator assigned to a related criminal investigation may review BWC Data relevant to the investigation.

2) Incident debrief and performance review.

An officer's immediate supervisor may utilize an officer's BWC data for the purpose of coaching and providing feedback to the officer with the purpose of improving performance.

3) Response to Resistance or Aggression Review.

BWC data may be accessed as part of the department's review of officer response to resistance or aggression. Supervisors and department personnel who have the responsibility to review a response to resistance or aggression may access BWC data pertaining to the incident.

4) Pursuit review.

BWC data showing a vehicle pursuit may be accessed by supervisors and department personnel who have the responsibility to review the incident.

5) Accidents involving department vehicles.

BWC data relating to department vehicle accidents may be disclosed to the Accident Review Board pursuant to General Order 640.07.

6) Quality Control Process

BWC data may be accessed as part of the BWC Quality Control Process - see G.O. 442.19.

7) Disclosure to Courts

a. BWC data relating to a criminal matter will be disclosed to the appropriate prosecuting authority.

b. BWC data may be further disclosed to court personnel as authorized by applicable rules of procedure and Minnesota Statutes sections 13.03, subdivision 6, and 13.825, subdivision 2 (d).

8) Training

a. Officers who become aware of BWC data that may contain training value should notify their supervisor. BWC data may be shown to staff for public safety training purposes.

b. The Training Unit Commander will communicate with any employees depicted in the BWC data prior to use of the data for training. The Training Unit Commander will evaluate and consider any objections of officers depicted in the data prior to use of the data. In all cases the training value of the data will be the focal point of any consideration for use as part of a training session.

c. Field Training Officers (FTOs) may utilize their own or their recruit's BWC data with their recruit for the purpose of providing coaching and feedback on the recruit's performance.

9) Evaluation of alleged misconduct.

a. Nothing in this policy limits or prohibits the use of BWC Data by the department to evaluate alleged misconduct or as a basis for discipline.

b. BWC data may be accessed by the internal affairs unit or any supervisor investigating a complaint of misconduct. A complaint of misconduct may include any allegation of improper procedure or misconduct, from an informal allegation or question to a formalized internal affairs complaint. Informal allegations or questions should be handled within the unit consistent with the chain of command. Formal complaints should follow the procedure outlined in General Order 230.00.

c. BWC data related to a formal complaint made against an officer during an internal investigation will temporarily be categorized as an Admin Hold under the Investigation of a Death/Admin Hold retention category.

10) Public Release.

Minnesota State Statute section 13.825, subdivision 2 defines instances in which BWC becomes public. Such data will be reviewed by the VMU prior to release.

The department will also at times release BWC data to the public with the goal of demonstrating:

1) Exceptional work done by officers on a daily basis.
2) Some of the challenges our officers face on a daily basis.
3) Things body cameras record and do not record.

The department may also release BWC data in the interest of public safety. Prior to release, all private data as defined by Minnesota Statute section 13.825, subdivision 2 will be redacted.

The Public Information Officer (PIO) will communicate with any employees depicted in the BWC data prior to public release under this section. The PIO will evaluate and consider any objections of employees depicted in the data prior to use of the data. The privacy and interests of all data subjects will be the focal point of all data released under this section.

C. Officers only have permissions in evidence.com to view data created by the BWC assigned to them. Officers needing to review data created by another officer's BWC may:

1) Ask the officer who created the data to show it.
2) Ask the officer who created the data to assign rights to view it in evidence.com.
3) Ask a supervisor to play it.

D. Critical Incidents and Review of Data.

Officer(s) involved in a Critical Incident may view and/or listen to BWC Data of the incident only after:

1) The officer has met with legal counsel or the Saint Paul Police Federation representative, if those entities are requested by the officer, and

2) The officer and legal counsel have met with the investigative entity or designee regarding the process for a Critical Incident set out in General Order 246.09.

SECTION 21. SHOWING BWC DATA WITH WITNESSES OR THE PUBLIC

Officers shall not share BWC recordings with any member of the public or any other employee, unless it is required for the official performance of their duties and consistent with all applicable laws.

Officers may show portions of BWC Data to witnesses as necessary for purposes of investigation as allowed by Minnesota Statutes section 13.82, subdivision 15 which states data may be shown to:

1) Aid the law enforcement process.

2) Promote public safety.

3) Dispel widespread rumor or unrest.

SECTION 22. COPYING OF BWC DATA

Copies of BWC data must be requested through the video management unit. Employees shall not copy or record BWC data with smart phones, video cameras, or by any other means.

SECTION 23. PROTECTION OF BWC DATA / AUDIT

BWC data will be protected in compliance with state law and this policy. To that end, the department will:

1) Restrict access to BWC data according to an authorized employee's access credentials.

2) Maintain an automated audit/electronic audit trail of the date, time, and person with regard to each access to data. All employees who access BWC Data via evidence.com will be required to document the reason for their access by adding a note describing their reason for accessing the data in the "notes" section of whatever data file is accessed.

   A note should usually be one of the following authorized reasons for review:

   - Report writing
   - Court
   - Internal affairs response
   - Case investigation
   - Debrief
   - RRA review
   - Pursuit review
   - Squad accident
   - Quality Control Process (QCP)

- Training
- FTO
- Complaint investigation
- VMU review

Any other reason not covered above should be specifically described.

SECTION 24. RELEASE TO THE PUBLIC

A. Only video management unit (VMU) staff or Internal Affairs Staff trained in data practice and the use of the system for copying such data are authorized to make copies of BWC data. The original data will be retained according to the retention schedule in this policy.

B. Copies made by VMU or IAU staff must be for lawful purposes including, but not limited to, data requests under the MGDPA, department purposes, criminal litigation and civil litigation.

C. Whenever a request for BWC data is made to the department by the media and the department intends to release the video, an email will be sent to all officers assigned to the associated CN in the CAD system, with a 24-hour advance notice of its release for all routine requests if possible.

D. The department may charge its actual cost for providing requested copies of data pursuant to Minnesota Statute sections 13.03 and 13.04.

SECTION 25. CASE NUMBERS AND DOCUMENTING EXISTENCE OF BWC DATA

A. All BWC data must be associated with a department case number to ensure accurate tracking of BWC data. Therefore, whether on- or off-duty, an officer who has created BWC data must ensure they have logged into the Computer Aided Dispatch system (CAD) with their employee (long) number. Then:

1) If a case number has not already been created to associate with the BWC data, the officer must call for a case number.

2) If a case number has already been created to associate with the BWC data, the officer must ensure they are assigned to that case number in the CAD.

3) If working off-duty or overtime or on-duty special detail (i.e. Xcel or CHS stadium, parade, etc.) and the situation for which the BWC data

was created does not require an independent case number, an officer may use the case number created when calling in for the off-duty job or created for the detail.

B. An officer not assigned to an incident in the CAD system, who arrives on scene and as per policy has activated their BWC, must notify dispatch of their arrival so they will be assigned to the incident in the CAD system.

C. Each officer completing a report and/or citation must document the existence of their BWC data in their report and/ or citation.

D. Documentation of BWC footage in a police report will be done using eForms. Officers will check yes or no in the section for "Has Body Camera Video". If yes is checked, they will then select yes or no with respect to whether the video was reviewed or not. Officers will also use eForms to document the existence of ICC video and what squad(s) have ICC video evidence. If an officer is not otherwise completing a report and/or citation for an incident, the existence of their BWC data must be documented in CAD via CAD comments.

E. Officers who unintentionally or accidentally create a recording may use the blanket CN of the year and 999999. For example, an inadvertent recording in 2020 should have in the ID field the CN 20999999.

SECTION 26. REPORT WRITING - DOCUMENTING BWC DATA CONTENT IN A NON-CRITICAL INCIDENT

A. To ensure the accuracy of reports and statements, officers may review audio and video data before making a report or statement.

B. Officers completing a report for an incident in which the BWC data was created are responsible to ensure the content of relevant BWC data is referenced in narrative form in their reports.

Additionally, a narrative report must describe

1) Reasons for failing to record when called for by this policy.

2) Whether officers have reviewed their BWC data before completing a report.

3) Whether the officer completing a report has reviewed the data of other BWCs.

4) The extent of review of any BWC data undertaken by an officer. Some examples of documentation of review:

- "I have not reviewed footage before completing this report."
- "I have conducted a full and detailed review of all data which could function as a transcript."
- "I have conducted a cursory review of video at fast speed without audio review."
- "The footage begins at 21:00:10 hours and ends at 21:20:00 hours. I have conducted a full and detailed review of portions (2105:05 to 2109:30)."

SECTION 27. BWC DATA RETENTION

BWC Data will be retained in accordance with the MGDPA, General Retention Schedule for Minnesota Cities, Ramsey County Evidence Retention Policy, court order, or applicable statute of limitations or preservation period. (The schedule is detailed in Section 15 of this policy)

All BWC Data not covered under the aforementioned provisions will be retained for a minimum period of 1 year, with the exception of those created and classified during the recruit training academy. There are no exceptions for erroneously recorded or non- evidentiary data.

Upon written request by a BWC Data subject, the department will 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. Subsequent requests will be evaluated and based on critical nature of the request may be approved by the Chief of Police or designee.

SECTION 28. HANDLING OF EVIDENCE

A. BWC Data will be handled as evidence and retained according to the applicable retention period of the categories assigned to the data.

B. When BWC Data contains evidence for a case, whether civil or criminal, that is being investigated by another agency, that agency will be provided a duplicate copy of the recording for a specified law enforcement purpose with the written approval of the Chief of Police or his or her designee.

SECTION 29. POLICY COMPLIANCE AND QUALITY CONTROL PROCESS.

Minnesota Statutes section 626.8473 requires that police departments put in place "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."

To meet these statutory requirements, all supervisors must monitor compliance with this policy.

The department has also created the position of BWC Quality Control Sergeant. The BWC Quality Control Sergeant will be assigned to the technology unit to verify compliance with this policy. G.O. 442.19 details the department's internal Quality Control Process for BWC.

Pursuant to G.O. 442.19, the department has also established the BWC Review Committee which is responsible for reviewing randomly selected videos for compliance with this BWC policy.

SECTION 30. TRAINING

Employees must complete the BWC training program before being issued or using a BWC. Ongoing training will be provided as determined by the Training Unit Commander.

SECTION 31. BWCs AND THE ICC SYSTEM

BWCs do not replace the ICC system. This policy does not replace the ICC policy. ICC continues to be governed by General Order 442.17 In-Car Camera Policy. However, officers wearing a BWC are exempt from the wireless microphone portion of the ICC policy.

SECTION 32. DISCOVERY OF POTENTIAL MISCONDUCT

The department encourages officers who witness or become aware of violations of department policy to immediately report said violation to their supervisor. If a civilian employee, an officer, or a sergeant reviewing BWC data observes a violation of department policy they should report the violation to their supervisor. A supervisor notified of such a violation shall take the appropriate actions based on the circumstances of the violation.

If a commander or chief reviewing BWC data observes a violation of department policy, they should take the appropriate actions based on the circumstances of the violation.

All who review BWC data shall focus their review on the reasons for which they are justified to do so.

SECTION 33. ACCESS TO SENSITIVE PERSONAL RECORDINGS

In the event of unintentional or inadvertent BWC recording, such as a personal conversation that captures sensitive personal information for which access should be restricted, an officer

may submit a written request via email to the VMU (SPPD-VMU@ci.stpaul.mn.us) which will restrict access to that portion of BWC data. The VMU sergeant will evaluate the request in conjunction with the Technology Unit Commander. If a restriction is placed on access to such data, that restriction will remain until the data is deleted according to the retention schedule of the data's category.

SECTION 34. SUMMARY OF VARIED REPORTING REQUIREMENTS

EVENT	POLICY REFERENCE	VERBAL NOTE IN BWC	REPORT, if written, or CAD COMMENTS	SUPERVISOR NOTIFICATION	VMU NOTIFICATION
Temporary removal of BWC from uniform, i.e. clearing an attic, etc.	Section 8. (B.) Wearing the BWC		X		
Recording an undercover officer	Section 9. (C.)				X
Officer deactivates recording due to MGDPA protections	Section 9. (D.)		X		
Officer deactivates recording due to victim or witness request	Section 9. (D.)		X		
Intentional or unintentional recordings under Prohibited Section of policy.	Section 9. (D.)				X
Any failure to record	Section 10.		X	X	
Stop or pause recording in a situation that would otherwise be recorded.	Section 12.	X	X		
Awareness of BWC data with training value	Section 20.			X	

SECTION 35. SECURITY ACCESS CONTROL PROCEDURES

A. Access to BWC recordings will be granted only to authorized users pursuant to this policy. It is the responsibility of authorized users to keep their username and password confidential. Accessing, copying, or releasing any recordings for other than legitimate law enforcement purposes is strictly prohibited, except as required by law.

B. BWC recordings will be accessed and copied from Evidence.com using department-approved equipment only for legitimate law enforcement purposes.

C. Any time a video is redacted for any purpose, the original of the un-redacted video shall also be kept.

D. Supervisors will monitor the BWC recorder system for compliance with this policy.

E. Officers must not attempt to intentionally edit, alter, or erase any BWC recording.

F. 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. The audit shall determine whether the data is being effectively managed according to Minnesota Statute 13.825 subd 9.

G. The department will maintain records showing the date and time BWC system data were collected and the applicable classification of the data.

H. The department will require in its vendor contracts that the vendor comply with the requirements of this policy and the FBI CJIS security policy, as amended, and that the vendor have in place sufficient security safeguards and policies to ensure appropriate protection of BWC data, including secure backups of BWC data. A portable recording system vendor that stores portable recording system data in the cloud must protect the data in accordance with the security requirements of the United States Federal Bureau of Investigation Criminal Justice Information Services Division Security Policy 5.4 or its successor version.

Security Access Control Procedure (Click to view document)

Outside Law Enforcement Agencies and Attorney Offices:

Shall use GovQA Request portal (www.stpaul.gov/datarequest) for the purposes of requesting BWC data. In doing so, they are required to fill out the SPPD Video Management Unit form "BWC Request for Data from Outside Agency". The form requires the following acknowledgement: "The recipient of body camera data acknowledges and agrees that they are required by law to fully comply with all requirements of Minnesota Statute section 13.825, subdivision 8, regarding data classification, destruction and security of portable recording system data received for a law enforcement purpose".

BWC data may not be shared with, disseminated to, sold to or traded with any other individual or entity unless explicitly authorized by this section or other applicable law, including explicitly Minnesota Statutes section 13.825, subdivision 7.

Roles by Job Level/Duty Chart:

The following SPPD and SPCAO personnel are granted roles/permissions in Evidence.com (cloud storage for BWC video) as indicated upon hire, transfer, promotion or demotion. All roles/permissions granted must have written permission from the Chief of Police or their designee. The corresponding HR Code (BWC Approval Letter) and Chief's approval are maintained by the SPPD HR Administrator.

HR Code	Evidence.com Role	Role Defined by Assignment
01	Camera Assignment Access	Personnel assigned to the Records Unit tasked with signing out spare BWCs
02	Officer	Personnel with the rank of Police Officer

03	SPCAO	Personnel working as an attorney or paralegal assigned to SPCAO criminal prosecution
04	Officer Trainer (Canine)	Personnel designated by the Canine Unit Commander as Canine Trainer
05	Training RRA Review	Personnel designated by the Training Unit Commander as a member of the Training Unit RRA Review
06	Supervisor Role	Personnel with the rank of Sergeant, Commander or Senior Commander NOT assigned to any of the following roles: • ADMIN ROLE • BWC REVIEW COMMITTEE ROLE • INTERNAL AFFAIRS ROLE • SUPERVISOR PLUS ROLE
07	Supervisor Plus Role	Personnel with the rank of Officer, Sergeant, Commander or Senior Commander assigned to any of the following units: • Gangs • Homicide/Robbery • Human Trafficking/Vice • MN Crimes Against Children • Narcotics • Special Investigations Unit (S.I.U.) • Safe Streets
08	BWC Review Committee	Personnel, of any rank, assigned to the BWC Review Committee
09	VMU CCTV	Personnel with the rank of Police Officer assigned to CCTV
10	VMU Technician	Personnel assigned to the Video Management Unit (VMU)
11	Internal Affairs	• Personnel with the rank of Commander or Sergeant, assigned to the Internal Affairs Unit • Office Assistant assigned to Internal Affairs
12	Chief	Personnel with the rank of Chief of Police, Assistant Chief or Deputy Chief
13	Admin	• Personnel with the rank of Sergeant, assigned to the Technology Unit • Personnel with the rank of Sergeant assigned to the Video Management Unit • Designated OTC Personnel
14	Super Admin	• Personnel with the rank of Sergeant, assigned to the Video Management Unit • Personnel with the rank of Commander, assigned to the Technology Unit

Axon roles and permissions checklist which defines each role's access in the evidence.com program is maintained by the Sergeant of VMU.

SECTION 36. Data Breach Policy and Procedures: Penalties (Minnesota State Statute 13.09)

Misuse or improper access to BWC data is subject to penalties under Minnesota Statute section 13.09.

(a) Any person who willfully violates the standards for unauthorized access to data or whose conduct constitutes the knowing unauthorized acquisition of nonpublic data, as defined in Section 13.055, subdivision 1, is guilty of a misdemeanor.
(b) Willful violation of Minnesota Statutes chapter 13, including any action subject to a criminal penalty under paragraph (a), by any public employee constitutes just cause for suspension without pay or dismissal of the public employee. See also General Orders 235.00 Data Practices and 236.00 Computer Security.

If there is a breach in security of BWC data maintained by the department, notifications will be made to those affected by the breach and an investigation started by the Property Crimes Administrators and the City of Saint Paul Office of Technology (OTC) staff as provided under Minnesota Statute 13.055.

A government entity that collects, creates, receives, maintains or disseminates private or confidential data on individuals must disclose any breach of the security of the data following discovery or notification of the breach. We will investigate crimes that occur in our jurisdiction and within our authority.

Data Breach Policy and Procedures

In the event of a body worn camera data breach, the City of Saint Paul Critical Security Incident Response Procedure will be followed (see Appendix A-G).

SECTION 37. Notification to the BCA

Within ten days of obtaining new surveillance technology that expands the type or scope of surveillance capability of a portable recording system device beyond video or audio recording, a law enforcement agency must notify the Bureau of Criminal Apprehension that it has obtained the new surveillance technology. The notice must include a description of the technology and its surveillance capability and intended uses. The notices are accessible to the public and must be available on the bureau's website.

January 28, 2022