Metro Transit PD Policy Manual

Body-Worn Cameras

451.1 PURPOSE AND SCOPE

The primary purpose of using body-worn cameras (BWCs) is to capture evidence arising from police encounters with the public. BWCs are a tool that is intended to enhance police-community relations, decrease complaints against officers, and assist in successful prosecution of crimes.

This policy sets forth guidelines governing the use of BWCs, as well as administering the resulting data as prescribed in state law. Compliance with these guidelines is mandatory. The Department recognizes that video cannot always show the entire scene and circumstances. This policy has been developed with the knowledge that some situations are tense, uncertain, and can evolve rapidly.

BWC data are not intended to replace detailed written reports and other forms of evidence.

This policy governs the use of BWCs in the course of official duties. It does not apply to or replace the use of mobile video ("dash cam") recording systems (MTPD Policy 446).

451.2 DEFINITIONS

The following phrases have special meanings as used in this policy:

- (a) CAD refers to the Computer-Aided Dispatch system used to manage the resources and details of a call for service.
- (b) **Citizen** is used as a general term and does not infer meaning upon immigration status of any kind.
- (c) **Cloud** is the storage model used for managing data. Data is then made available to appropriate parties using secure login credentials.
- (d) Critical incident refers to the definition detailed in MTPD Policy 310.1.1:
 - The use of deadly force by or against a Metro Transit police officer;
 - 2. Death or great bodily harm to a Metro Transit police officer;
 - 3. Death or great bodily harm to a person who is in the custody or control of a Metro Transit police officer; or
 - 4. Any action by a Metro Transit police officer that causes or is intended to cause death or great bodily harm.
- (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 confrontational, and a recording of the event would not yield information relevant to an ongoing investigation. Examples include, but are not limited to, assisting the public with directions, summoning a tow truck, or receiving generalized concerns.

- (g) **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.
- (h) MGDPA or Data Practices Act refers to the Minnesota Government Data Practices Act, Minn. Stat. § Ch. 13.825
- (i) **Officer** is used within this police as a general term referring to any authorized member of the Metro Transit Police Department, regardless of rank or assignment. This includes part-time sworn officers, full-time sworn officers, and non-sworn community service officers.
- (j) **Official duties**, for the purposes of this policy, means that the officer is on-duty and performing authorized law enforcement services on behalf of this agency.
- (k) Unintentionally recorded footage is a video recording that results from an officer's inadvertence 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 MTPD locker rooms, restrooms, and recordings made while officers were engaged in conversations of a non-business, personal nature.
- (I) **UOF** refers to Use of Force: when an officer uses any level force to gain compliance from a suspect.

451.3 EQUIPMENT ASSIGNMENT

Officers, as defined in 451.2(i), will use only Metro Transit Police Department-issued BWCs in the performance of official duties for this agency.

451.4 USAGE

451.4.1 WEARING AND OPERATING THE BWC

Officers who have been issued BWCs shall operate and use them in a manner consistent with this policy and training.

- (a) All officers, regardless of rank, are required to wear their BWC when they are on duty for the MTPD in the duty uniform appropriate to their assignment. At the discretion of the Chief of Police, an exception may be made in special circumstances.
- (b) Officers who are in the appropriate MTPD duty uniform but who are working off-duty and compensated by another entity should wear and use their BWC consistent with this policy.
- (c) Officers assigned to Ramsey County SWAT or another law enforcement agency should wear the MTPD-issued BWC unless otherwise agreed upon by that agency and the appropriate representative for the MTPD.
- (d) Officers should wear their BWCs at the location on their body and in the manner specified in training.

- (e) Officers shall conduct a function test of their BWCs at the beginning of each shift to make sure the devices are operating properly. The officer shall clearly state their name, badge number, and call sign.
- (f) Officers noting a malfunction during testing or at any other time shall promptly report the malfunction to their supervisor. The officer will also notify the Business Technology Unit via email. A supervisor will assign a spare BWC to the officer until such time that the malfunctioning equipment is repaired or replaced.

451.4.2 DOCUMENTING USE

Officers must document BWC use and non-use as follows:

- (a) If enforcement action is taken, the existence of the recording shall be documented in the related report, citation, or CAD call, whichever is the highest level of documentation for the circumstance.
- (b) Every recording will be classified in the BWC software according to the categories listed in 451.7.3, whether or not a report or citation has been issued (e.g., when a fare inspection warning is given, the recording will be categorized as "Call for Service/Public Contact").
- (c) Whenever an officer fails to record an activity that is required to be recorded under this policy or captures only a part of the activity, the officer must notify their supervisor immediately, as well as document the circumstances and reasons for not recording in an incident report. Supervisors shall review these reports and initiate any corrective action deemed necessary.

451.5 GENERAL GUIDELINES FOR RECORDING

451.5.1 ACTIVATING BWCS

Officers shall activate their BWCs prior to arrival and as soon as practicable when participating in any police actions including, but not limited to:

- (a) Vehicle or person stops (e.g., citations for fare evasions).
- (b) Pursuits.
- (c) Arrests.
- (d) Transports (jail, detox, hospital, etc.).
- (e) Searches (e.g., vehicle, person, structure).
- (f) In-the-field suspect, victim, and witness interviews and interrogations.
- (g) Any police-citizen contacts that become confrontational.
- (h) Holding a perimeter on a crime scene.
- (i) Engaging in crowd control or civil unrest.

451.5.2 EXCEPTIONS TO ACTIVATION

Officers need not activate their BWCs when it would be unsafe, impossible, or impractical to do so; however, such instances of not recording when otherwise required must be documented as specified in the Usage guideline 451.4.2(a).

451.5.3 PUBLIC NOTIFICATION

Officers have no affirmative duty to inform people that a BWC is being operated or that the individuals are being recorded. Officers may make announcements at their discretion.

451.5.4 CONCLUDING RECORDINGS

Once activated, the BWC should remain on until the incident has concluded. For purposes of this section, conclusion of an incident has occurred when any arrests have been made, arrestees or other persons have been transported, and all witnesses and victims have been interviewed. Recording may cease if an officer is simply waiting for a tow truck or in other similar situations.

- (a) If the recording is discontinued while an investigation, response, or incident is ongoing, officers shall state the reasons aloud for ceasing the recording on camera before deactivating their BWC. Officers will also document their reason(s) in an incident report.
- (b) If circumstances change, officers shall reactivate their BWC as required by this policy to capture information having evidentiary value.

Officers who are assigned to crime scene perimeter safety will keep their BWC activated until they have cleared from the scene, unless otherwise instructed by a supervisor or investigator.

Officers monitoring protests or engaged in crowd control or civil unrest (MTPD Policy 474: First Amendment Assemblies) will keep their BWC activated until they are relieved from live action for a break or end-of-shift.

451,5,5 BLOCKING CAMERA AND MUTING AUDIO

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

451.5.6 RECORDING AGENCY PERSONNEL

Notwithstanding any other provision in this policy, officers shall not use their BWCs to record other agency personnel during non-enforcement related activities, such as during 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.

451.6 SPECIAL GUIDELINES FOR RECORDING

451.6.1 OTHER REASONS FOR ACTIVATION

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

- (a) To use their BWCs 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 BWCs to take recorded statements from persons believed to be victims of or witnesses to crimes as well as persons suspected of committing crimes, considering the needs of the investigation and the circumstances pertaining to the victim, witness, or suspect.

451.6.2 TRANSPORTING SUSPECTS AND OTHER SUBJECTS

Officers shall use both their BWCs and squad-based audio/video systems to record the transportation and physical transfer of persons in their custody to hospitals, detox and mental health care facilities, juvenile detention centers, and jails.

- (a) Officers should cease recording once the transfer of custody is complete unless jail policy indicates otherwise.
- (b) Officers should not record once inside medical facilities (detox, hospitals, or mental health facilities) in order to protect HIPAA rights.
- (c) If an officer feels that the situation may escalate or become confrontational, the BWC may be activated as appropriate.

451.6.3 COURTROOMS

BWCs should be worn but not powered on when in a courtroom or associated areas, unless circumstances indicate otherwise. A courthouse policy regarding recording devices will supersede this policy when appropriate. This does not include an officer who is responding to a call for service for an incident inside a court facility.

451.6.4 PROTECTED PERSONS

BWCs shall be deactivated in order to protect the identities of undercover officers and confidential informants. For security reasons, officers do not need to verbally state the reason for deactivation, but shall document their reason for deactivating the BWC in their written report.

451.6.5 VICTIM AND WITNESS STATEMENTS

An officer may choose to turn off the BWC if its operation is inhibiting a victim or witness from giving a statement. Officers should use good judgment and discretion in activating/deactivating BWCs when dealing with sensitive calls and vulnerable victims (sexual assault or child abuse, for example). Officers shall include their reason for deactivating the BWC in their written report.

451,7 UPLOADING AND CLASSIFYING DATA

451.7.1 END OF SHIFT

Each officer using a BWC is responsible for uploading the data from their BWC at the end of that officer's shift.

(a) If the officer is involved in a critical incident, the Business Technology Unit shall take custody of the camera from the officer and work in conjunction with the investigating

agency to upload any BWC data and to preserve the chain of custody. The camera will be inventoried as evidence until the investigating agency or the prosecuting office releases it. In the interim, the officer will be issued a spare BWC pending the return of their original hardware.

451.7.2 SMARTPHONE INTEGRATION

Officers may use the department-issued smartphone in order to access BWC data to flag, categorize, and otherwise manage video while in the field. Policy related to department-issued phones is found under MTPD Policy 702.

451.7.3 CATEGORIZATION

Officers will ensure that the categories on the BWC data files are accurate and include the case number prior to uploading the data. If in doubt, they should consult with a supervisor as to the appropriate categorizing. Officers should assign as many of the following categories as are applicable to each file:

- (a) **Academy:** For use by recruit academy staff and recruits only.
- (b) Administrative Hold: Data related to an Internal Affairs investigation.
- (c) Arrest/Investigative/Evidence: Data related to an in-custody arrest, investigation, or evidence thereof.
- (d) Call for Service/Public Contact: Data related to a general call for service or community contact of interest.
- (e) Critical Incident: Data related to a critical incident as defined in MTPD Policy 310.
- (f) **Death or CSC Investigation:** Data related to any investigation involving a homicide or criminal sexual conduct (CSC).
- (g) **Motor Vehicle Flee/Use of Force:** Data related to a motor vehicle pursuit or use of force incident.
- (h) **Test/Accidental/Non-Evidentiary**: Data that is a test, accidental, or has no evidentiary value.
- (i) Traffic/Accident Investigation: Data related to a traffic stop or crash investigation.

451.8 ADMINISTERING ACCESS TO BWC DATA

451.8.1 DATA SUBJECTS

Under Minnesota Statutes § 13.825, subd. 4, the following are considered data subjects for purposes of managing public access to BWC data:

- (a) Any person or entity whose image or voice is documented in the data.
- (b) The officer who collected the data.
- (c) Any other officer whose voice or image is documented in the data, regardless of whether that officer is or can be identified by the recording.

451.8.2 PUBLIC OR CONFIDENTIAL DATA

BWC recordings are classified as private data about the data subjects unless there is a specific law that provides differently. However, some BWC data is classified as confidential or public as addressed below (451.8.4).

451.8.3 DATA IN ACTIVE INVESTIGATIONS

BWC data that is collected or created as part of an active criminal investigation is confidential. This classification takes precedence over the "private" and "public" classifications.

451.8.4 PUBLIC DATA

- (a) Data documenting the discharge of a firearm by a peace officer in the course of duty, other than for training or the killing of an animal that is sick or injured.
- (b) Data that documents the use of force by a peace officer that results in substantial bodily harm.
- (c) Data that a data subject requests to be made accessible to the public, subject to redaction. Data on any data subject (other than a peace officer) who has not consented to the public release must be redacted if practicable. In addition, any data on undercover officers or confidential informants must be redacted.
- (d) However, if another provision of the Data Practices Act classifies data as private or otherwise not public, the data retains that other classification. For instance, data that reveals protected identities under the MGDPA (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.

451.8.5 DATA REQUESTS FROM THE PUBLIC AND THE MEDIA

Officers and MTPD employees shall refer members of the media or public seeking access to BWC data to the MTPD's Records Unit, who shall process the request in accordance with the MGDPA and other governing laws. In particular:

- (a) An individual shall be allowed to review recorded BWC data about themselves and other data subjects in the recording, but access shall not be granted:
 - 1. If the data was collected or created as part of an active investigation
 - 2. 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. § 13.825, subd. 17.
- (b) Unless the data is part of an active investigation, an individual data subject shall be provided with a copy of the recording upon request, but subject to the following guidelines on redaction:
 - Data on other individuals in the recording who do not consent to the release must be redacted.
 - 2. Data that would identify undercover officers or confidential informants must be redacted.

3. 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.

451.8.6 VIEWING BWC DATA BY EMPLOYEES

- (a) Officers, MTPD employees, and Council employees may access and view stored BWC data only when there is a business need for doing so. Access is reasonably limited by the BWC's system permissions as granted by the Chief of Police or their designee. Reasons for access may include:
 - 1. When preparing reports or statements.
 - 2. By a supervisor investigating a specific act of officer conduct.
 - 3. By a supervisor to assess officer's compliance to policy.
 - 4. By appropriate department investigators as related to an official investigation such as a criminal act or personnel complaint.
 - 5. By an officer who is captured on the recording for a purpose related to his/her employment.
 - 6. To assess potential training value.
- (b) Officers will not be permitted to view body worn camera data prior to giving a statement when involved in a critical incident.
- (c) Officers and MTPD employees may access data in order to assess proper functioning of BWC system. Approved vendors with a clear reason, such as troubleshooting equipment or network infrastructure, may also access data in compliance with the MGDPA and in coordination with the Business Technology Unit.
- (d) Officers and MTPD employees shall document their reasons for accessing stored BWC data within the cloud-based platform.
- (e) Officers and MTPD employees are prohibited 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. Agency personnel shall not use any other recording device such as a smartphone to record a copy of the video.
- (f) Any Metropolitan Council employee who is seeking access to BWC data for non-business reasons may make a request for it to the Records Unit. Data will be provided in compliance with the MGDPA.

451.8.7 DISPLAYING BWC DATA DURING ACTIVE INVESTIGATIONS

Officers may display portions of BWC footage to witnesses as necessary for purposes of investigation as allowed by Minn. Stat. § 13.825, subd. 15. Officers should generally limit these displays in order to protect against the incidental disclosure of individuals whose identities are not public. Such purposes may include showing only a portion of the video, showing only screen shots, muting the audio, or playing the audio but not displaying video.

Metro Transit PD Policy Manual

Body-Worn Cameras

Officers may create and share screenshots of video for internal use only, but must have approval from a supervisor before doing so.

451.8.8 DATA SHARING WITH OTHER LAW ENFORCEMENT AGENCIES

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.

451.8.9 DATA SHARING WITH OTHER CRIMINAL JUSTICE ENTITIES

BWC data shall be made available to prosecutors, courts, and other criminal justice entities as provided by law. Data that is shared under these circumstances will be documented in the BWC software and in the records management system.

451.9 DATA SECURITY SAFEGUARDS

451.9.1 ENCRYPTION

Recorded video will be off-loaded from the device once docked at the end of the officer's shift. This dock is supplied by the vendor and provides for charging of the device. CJIS-level encryption standards will be met while data is being transferred to the cloud platform.

451.9.2 REDUNDANCY

Per the negotiated and signed contract, the system vendor is responsible for creating data redundancy and ensuring the survivability of data in the event of disaster.

451.9.3 SYSTEM SAFEGUARDS

Built-in system safeguards including user-based permissions, audit trail, viewing, and limitations on who can transfer copies of video files from the cloud are all part of the overall system configuration.

451.9.4 EDITING OR ALTERING DATA

Officers shall not intentionally edit or alter any BWC recording without a business reason for doing so (451.8.7). Officers will not intentionally erase any BWC recording outside of the retention schedule.

451.9.5 DATA REDACTION

Before releasing video to an individual, the general public, or the media, video may be redacted to protect identities, remove offensive portions, and other reasons as detailed in the Data Practices Act. In the event of a high-profile incident, the Chief of Police must consult with the General Manager of Metro Transit and the Regional Administrator of the Metropolitan Council as part of the decision-making process to the release of BWC recording(s).

451.10 AGENCY USE OF DATA

Metro Transit PD Policy Manual

Body-Worn Cameras

451.10.1 AUDIT

At reasonable intervals determined by the Chief of Police or their designee, members of the BWC Review Committee will review randomly selected video in order to ensure compliance with this policy and to identify any performance areas in which additional training or guidance is required.

451.10.2 PERSONNEL COMPLAINTS

Supervisors and other assigned personnel may access BWC data for the purposes of reviewing or investigating a specific incident that has given rise to a complaint or concern about officer misconduct or performance.

451.10.3 DISCIPLINE

Nothing in this policy limits or prohibits the use of BWC data as evidence of misconduct or as a basis for discipline.

451.10.4 TRAINING

Officers should contact the Training Unit to discuss retaining and using BWC footage for department-wide 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 also utilize BWC data with trainees for the purpose of providing coaching and feedback on the trainees' performance.

451.11 DATA RETENTION

451.11.1 RETENTION SCHEDULE

The table below shows the retention schedule for each video as classified. It represents the minimum amount of time that data should be preserved and is subject to change as needed.

CLASSIFICATION	DEFINITION	RETENTION
Academy	For use by Recruit Academy staff & recruits only.	2 years
Administrative Hold	Data related to an Internal Affairs investigation.	2 years
Arrest/Investigative/Evidence	Data related to an in-custody arrest, investigation, or evidence thereof.	2 years
Call for Service/Public Contact	Data related to a general call for service or community contact of interest.	90 days
Critical Incident	Data related to a critical incident as defined in MTPD Policy 310.	11 years
Death or CSC Investigation	Data related to any investigation of a death involving a homicide or criminal sexual conduct.	25 years

Metro Transit PD Policy Manual

Body-Worn Cameras

Motor Vehicle Flee/Use of Force Data related to a motor vehicle 6 years

pursuit or use of force.

Test/Accidental/Non-Evidentiary Data that is a test, accidental, or 90 days

has no evidentiary value.

Traffic/Accident Investigation Data related to a traffic stop or 2 years

crash investigation.

451.11.2 MULTIPLE RETENTION PERIODS

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.

451.11.3 REQUESTING RETENTION EXTENSIONS

Upon written request by a BWC data subject, the MTPD shall retain the data subject's recording for an additional time period as requested, up to 180 days. The MTPD will notify the requestor that the data will be destroyed after 180 days unless a new written request is received.

451.11.4 RECORDS

The department will maintain the following records and documents relating to BWC use, which are classified as public data, pursuant to the Data Practices Act:

- (a) 1. The total number of BWCs owned or maintained by MTPD;
 - 2. A daily record of the total number of BWCs actually deployed and used by officers and which Command they were used in; and
 - 3. The total amount of recorded BWC data collected and maintained.

451.12 COMPLIANCE

451.12.1 BIENNIAL AUDIT

As required by Minn. Stat. § 13.825, subd. 9, the MTPD shall obtain an independent biennial audit of its BWC program. The audit shall be conducted by the Metropolitan Council's Program Evaluation and Audit or an entity designated by Program Evaluation and Audit.

451.12.2 FAILURE TO COMPLY

Failure to follow the policy and procedure as outlined in this document may result in discipline up to and including termination.

451.12.3 UNAUTHORIZED ACCESS OR DISCLOSURE

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.

451.12.4 PUBLIC POSTING

The MTPD will post this policy to the department's website.