

Metropolitan Transit Police Department

# 451: Use of Body-Worn Cameras Policy

Drafted for Public Review & Comment

# Table of Contents

451.1 PURPOSE & SCOPE
451.2 DEFINITIONS
451.3 EQUIPMENT ASSIGNMENT
451.4 USAGE
451.5 GENERAL GUIDELINES FOR RECORDING
451.6 SPECIAL GUIDELINES FOR RECORDING
451.7 UPLOADING AND CLASSIFYING DATA7
451.8 ADMINISTERING ACCESS TO BWC DATA
451.9 DATA SECURITY SAFEGUARDS 11
451.10 AGENCY USE OF DATA 12
451.11 DATA RETENTION
451.12 COMPLIANCE

### 451.1 PURPOSE & 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:
  - a. The use of deadly force by or against a Metro Transit police officer;
  - b. Death or great bodily harm to a Metro Transit police officer;
  - c. Death or great bodily harm to a person who is in the custody or control of a Metro Transit police officer; or

- d. Any action by a Metro Transit police officer that causes or is intended to cause death or great bodily harm.
- e) Duty Uniform is the uniform in compliance with MTPD Uniform Policy 1046
- f) **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.
- g) **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.
- h) **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.
- i) **MGDPA or Data Practices Act** refers to the Minnesota Government Data Practices Act, Minn. Stat. Ch. 13.
- j) **Officer** is used within this policy as a general term referring to any sworn member of the Metro Transit Police Department, regardless of rank or assignment.
- k) **Official duties,** for purposes of this policy, means that the officer is on-duty and performing authorized law enforcement services on behalf of this agency.
- I) 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.
- m) **UOF** refers to Use of Force: when an officer uses any level of force to gain compliance from a suspect.

#### **451.3 EQUIPMENT ASSIGNMENT**

451.3.1 Full-time and part-time officers will use only department-issued BWCs in the performance of official duties for this agency.

#### 451.4 USAGE

- 451.4.1 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 in on duty for the MTPD in the duty uniform appropriate to their assignment. and on duty for the Metro Transit Police Department. At the discretion of the Chief of Police, an exception may be made in special circumstances.
  - b. Officers who are in the appropriate 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 should wear their BWCs at the location on their body and in the manner specified in training.
  - d. 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.
  - e. Officers noting a malfunction during testing or at any other time shall promptly report the malfunction to their supervisor and will notify the Business Technology Unit via email. A spare BWC will be assigned to the officer for such time that the malfunctioning equipment is repaired or replaced.

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

- a. Whenever an officer makes a recording, the existence of the recording shall be documented in the related report or citation.
- 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 "Traffic/Person Stop – No Citation").
- 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 Officers shall activate their BWCs prior to arrival or as soon as practicable when participating in any police actions including, but not limited to:

- a. Motorist 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.
- 451.5.2 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(b).
- 451.5.3 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 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 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 BWCs as required by this policy to capture information having evidentiary value.
- 451.5.5 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 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 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 and 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 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 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 BWCs shall be deactivated in order to protect the identities of undercover officers and confidential informants. Officers shall include their reason for deactivating the BWC in their written report.
- 451.6.5 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 CLASSIFYINGING DATA

- 451.7.1 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 Officers may use the department-issued smartphone 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 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. Arrest: In-custody arrest of a person.
  - b. **Assist other Agency (AOA):** Footage captured while assisting another law enforcement agency.
  - c. **Crash Investigation:** Footage related to any crash-related investigation (private motor vehicle or Metro Transit vehicle).
  - d. **Death:** Any investigation into a death, including but not limited to fatal crashes and homicides.

- e. **DWI:** Footage showing evidence of DWI-related offenses.
- f. Flee: Footage showing a motor vehicle pursuit.
- g. Information: Any community contact of interest.
- h. **Internal Investigation:** Related to a complaint against an officer, whether initiated by the public or within the department.
- i. **Investigative:** Any community contact of interest related to an investigation. This may include, but is not limited to, footage that captures possible suspects or witnesses.
- j. No Event: System checks and unintentional recordings.
- k. Officer Assault: Footage of any assault on a police officer.
- I. **Transport:** Footage documenting the transportation of person(s) from one location to another including, but not limited to, jail, detox, hospital, or other facility.
- m. Traffic/Person Stop Citation: Any traffic or person stop that results in a citation being issued.
- n. **Traffic/Person Stop No Citation:** Any traffic or person stop that does not result in a citation.
- o. Training: An event that could assist in department training.
- p. Use of Force: Force used to gain compliance from a suspect.

#### 451.8 ADMINISTERING ACCESS TO BWC DATA

- 451.8.1 Under Minnesota Statutes § 13.825, subd. 4, the following are considered data subjects for purposes of administering 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 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.
- 451.8.3 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.
- 451.8.4 The following BWC data is public:
  - 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 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:
  - 1. 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 Officers, MTPD employees, and Council staff:

- 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 nonbusiness reasons may make a request for it to Records Unit. Data will be provided in compliance with the MGDPA.
- 451.8.7 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.
- 451.8.8 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 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 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 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 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 Officers shall not intentionally edit, alter, or erase any BWC recording. 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 may consult with the General Manager of Metro Transit and the Regional Administrator of the Metropolitan Council as part of the decisionmaking process to the release of BWC recording(s).

#### 451.10 AGENCY USE OF DATA

- 451.10.1 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 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 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 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-bycase 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 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
Arrest	In-custody arrest of a person.	2 years
Assist Other Agency	Footage captured while assisting	90 days
(AOA)	another law enforcement agency.	
Crash Investigation	Footage related to any crash- related investigation (private motor vehicle or Metro Transit vehicle).	2 years
Death	Any investigation of a death, including but not limited to fatal crashes and homicides.	25 years
DWI	Footage showing evidence of DWI- related offenses.	2 years
Flee	Footage showing a motor vehicle pursuit.	2 years
Information	Any community contact of interest.	90 days
Internal Investigation	Related to a complaint against an officer, whether initiated by the public or within the department.	90 days
Investigative	Any community contact of interest related to an investigation. This may include, but is not limited to, footage that captures possible suspects or witnesses.	90 days
No Event	System checks and unintentional recordings.	90 days
Officer Assault	Footage of any assault on a police officer.	6 years
Transport	Transportation of person(s) from one location to another including, but not limited to, jail, detox, hospital, or other facility.	90 days
Traffic – Citation	Any traffic stop that results in a citation being issued.	2 years
Traffic – No Citation	Any traffic stop that does not result in a citation.	90 days

Training	An event that could assist in	90 days
	department training.	
Use of Force	Force used to gain compliance	6 years
	from a suspect.	

- 451.11.2 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 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. At the time that the request is made, 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 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. The total number of BWCs owned or maintained by MTPD;
  - b. A daily record of the total number of BWCs actually deployed and used by officers and which Command they were used in; and
  - c. The total amount of recorded BWC data collected and maintained.

#### 451.12 COMPLIANCE

Supervisors shall monitor for compliance with this policy.

- 451.12.1 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 follow the policy and procedure as outlined in this document may result in discipline up to and including termination.
- 451.12.3 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 The MTPD will post this policy to the department's website.

# PUBLIC COMMENT DRAFT