# **Chaska Police Department**

	Date of Issue August 20, 1999		0 10 1 10		
			General Order 43		
	Effective Date	Annual Review Date		Subject	
	August 8, 2018	April			EQUIPMENT

#### 43.1 MCD Care and Use

#### 43.1.1 Definition

An MCD is a Mobile Computing Device in Police department vehicles to be used as tools to assist the user in carrying out their job duties. The system uses laptop computers to run routine database queries, (e.g. vehicle registrations and drivers license checks).

### 43.1.2 <u>Hardware</u>

Only authorized computers may be connected to the MCD system. When transporting the MCD unit outside the vehicle, the screen must be closed and latched.

#### 43.1.3 Software

Only department authorized software may be installed on the MCD.

### 43.1.4 Upkeep

The MCD should not be turned on in a vehicle, until the temperature inside the vehicle is comfortable for the driver.

The users of the MCD are responsible for keeping the MCD clean. The city will provide appropriate cleaning supplies.

#### 43.1.5 Trouble Reporting

Any loss, damage or malfunction of MCD related equipment shall be reported by the user to the supervisor on duty. Where deemed necessary, the MCD will be removed from the vehicle, and left in the police department for repair, with appropriate documentation.

## 43.1.6 Equipment Alterations

Only authorized personnel will make adjustments or repairs to the MCD. Unauthorized persons shall not repair, adjust, modify, disable or interrupt operations of any of the MCD equipment.

The basic settings of the computer are not to be changed by unauthorized persons. This includes the colors, fonts, and desktop settings.

#### 43.1.7 Prohibited Use

MCD shall not be used for any purpose that suggests any of the following:

- Discrimination on the basis of age, sex, marital status, race, creed, color, national origin, sensory, mental or physical handicap status.
- Sexual harassment.
- Copyright infringement.
- An employee's personal, political, or personal business interests.
- Any unlawful activity.

#### 43.1.8 Data Privacy

All MCD data is public information under the Minnesota Data Practices Act. This means that the media and general public may access it on demand. Employees shall not have any expectation of privacy when using the MCD.

#### 43.1.9 Messaging

The Sheriff's Office records all messaging on the MCD system. No vulgarity or profanity shall be transmitted through the system. The messages shall remain professional.

Supervisors will review messaging as directed by the Chief of Police

#### 43.1.10 Authorized Users

The MCD system is solely for official police business and only authorized employees shall operate the units. The user is responsible for transmissions made under their log on.

## 43.2 First Responder Defibrillation Protocol

A Defibrillation unit would be used under the following circumstances:

- 1. Chest Pains
- 2. Respiratory Distress
- 3. Massive Trauma
- 4. Acute CVA

#### FIRST RESPONDER DEFIBRILLATION PROTOCOL

#### 1. Establish Cardiac Arrest and start C.P.R.

- A. Ventilate with pocket mask connected to O2.
- B. Perform one or two-person C.P.R.
- 2. Connect Defibrillator to patient and follow protocol for the specific type of defibrillator being used.
- 3. If monitor shows a heart rhythm other than ventricular fibrillation and no shock is advised, keep the patient attached to the unit.
- 4. If monitor shown Ventricular Fibrillation and audible signals a "need for shock", proceed on per voice commands of the units.
- 5. Only certified Police/Ambulance Personnel will use the Defibrillation unit.
- 6. C.P.R. should not be delayed at any time for any reason to persons needing it.
- 7. The patient should be defibrillated in a stationary setting free of adverse weather conditions.
- Certified Personnel shall follow protocol for recording the actions of the specific defibrillator upon completion of use.

#### 43.3 Protective Equipment for First Responders

 Disposable gloves, gowns, masks, protective eyewear and other protective equipment should be worn when applicable to prevent transmission of infectious agents.

## 43.4 Body Worn Cameras

## 43.4.1 **Purpose**

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

## **43.4.2 Policy**

It is the policy of this department to authorize and require the use of department-issued BWCs as set forth below, and to administer BWC data as provided by law.

## 43.4.3 Scope

This policy governs the use of BWCs in the course of official duties. It does not apply to the use of squad-based (dash-cam) recording systems. The chief or chief's designee may supersede this policy by providing specific instructions for BWC use to individual officers, or providing specific instructions pertaining to particular events or classes of events, including but not limited to political rallies and demonstrations. The chief or designee may also provide specific instructions or standard operating procedures for BWC use to officers assigned to specialized details, such as carrying out duties in courts or guarding prisoners or patients in hospitals and mental health facilities.

# 43.4.4 Administrator Responsibilities

The BWC administrator (designated personnel authorized by the Chief of Police) are responsible for deleting media:

- **A.** Pursuant to a court order.
- **B.** In accordance with established records retention policies, including reclassifying all other media deemed to be of no evidentiary value.
- C. In instances where privacy issues are noted.

# 43.4.5 **Definitions**

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

- A. **MGDPA or Data Practices Act** refers to the Minnesota Government Data Practices Act, Minn. Stat. § 13.01, et seq.
- B. **Records Retention Schedule** refers to the General Records Retention Schedule for Minnesota Cities.
- C. 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.

- D. **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.
- E. **General citizen contact** means an informal encounter with a citizen that is not and does not become law enforcement-related or adversarial, and a recording of the event would not yield information relevant to an ongoing investigation. Examples include, but are not limited to, assisting a motorist with directions, summoning a tow truck, or receiving generalized concerns from a citizen about crime trends in his or her neighborhood.
- F. **Adversarial** means a law enforcement encounter with a person that becomes confrontational, during which at least one person expresses anger, resentment, or hostility toward the other, or at least one person directs toward the other verbal conduct consisting of arguing, threatening, challenging, swearing, yelling, or shouting. Encounters in which a citizen demands to be recorded or initiates recording on his or her own are deemed adversarial.
- G. **Unintentionally recorded footage** is a video recording that results from an officer's inadvertence or neglect in operating the officer's BWC, provided that no portion of the resulting recording has evidentiary value. Examples of unintentionally recorded footage include, but are not limited to, recordings made in station house locker rooms, restrooms, and recordings made while officers were engaged in conversations of a non-business, personal nature with the expectation that the conversation was not being recorded.
- H. **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.

# 43.4.6 <u>Use and Documentation</u>

- **A**. Officers may use only department-issued BWCs in the performance of official duties for this agency or when otherwise performing authorized law enforcement services as an employee of this department.
- **B.** Officers who have been issued BWCs shall operate and use them consistent with this policy. Officers shall conduct a function test of their issued BWCs at the beginning of each shift to make sure the devices are operating properly. Officers noting a malfunction during testing or at any other time shall promptly report the malfunction to the officer's supervisor and shall document the report in writing. Supervisors shall take prompt action to address malfunctions and document the steps taken in writing.
- C. Officers should wear their issued BWCs at the location on their body and in the manner specified in training. Any member assigned to a non-uniformed position may carry a approved BWC at any time the member believes that such a device may be useful, with the exception of a School Resource Officer performing their daily activities within their assigned school.

- **D.** Officers must document BWC use and non-use as follows:
- 1. Whenever an officer makes a recording, the existence of the recording shall be documented in an incident report or categorized appropriately within Evidence.com.
- 2. 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 document the circumstances and reasons for not recording in an incident report. Supervisors shall review these reports and initiate any corrective action deemed necessary.
- **E.** The department will maintain the following records and documents relating to BWC use, which are classified as public data:
- 1. The total number of BWCs owned or maintained by the agency;
- 2. A daily record of the total number of BWCs actually deployed and used by officers;
- 3. The total amount of recorded BWC data collected and maintained; and
- 4. This policy, together with the Records Retention Schedule.

# 43.4.7 General Guidelines for Recording

- **A.** This policy is not intended to describe every possible situation in which the recorder should be used, although there are many situations where its use is appropriate. Members shall activate their recorders in any of the following situations:
- 1. All enforcement and investigative contacts including stops and field interview situations.
- 2. Traffic stops including, but not limited to, traffic violations, stranded motorist assistance and all crime interdiction stops.
- 3. Self-initiated activity in which a member would normally notify Carver County Dispatch.
- 4. Any other contact that becomes adversarial after the initial contact in a situation that would not otherwise require recording.
- **B**. Officers need not activate their cameras when it would be unsafe, impossible, or impractical to do so, but such instances of not recording when otherwise required must be documented as specified in the Use and Documentation guidelines, part (D)(2) (above).
- **C.** Officers have discretion to record or not record general citizen contacts.
- **D.** Officers have no affirmative duty to inform people that a BWC is being operated or that the individuals are being recorded.

- E. Once activated, the BWC should continue recording until the conclusion of the incident or encounter, or until it becomes apparent that additional recording is unlikely to capture information having evidentiary value. The officer having charge of a scene shall likewise direct the discontinuance of recording when further recording is unlikely to capture additional information having evidentiary value. If the recording is discontinued while an investigation, response, or incident is ongoing, officers shall state the reasons for ceasing the recording on camera before deactivating their BWC. If circumstances change, officers shall reactivate their cameras as required by this policy to capture information having evidentiary value. Recording may be stopped during significant periods of inactivity such as report writing or other breaks from direct participation in the incident.
- **F**. Officers shall not intentionally block the BWC's audio or visual recording functionality to defeat the purposes of this policy, which is to capture evidence arising from police-citizen encounters. Recording may be temporarily ceased or the audio muted to exchange information with other officers, legal counsel, or the lens obstructed in order to avoid capturing images of undercover officers, informants, or citizens where based on training and experience, in the judgement of the officer a recording would not be appropriate or consistent with this policy. The reason to cease and resume recording (or to mute audio or obstruct the lens) will be noted by the officer either verbally on the BWC or in a written report.
- **G**. 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.
- **H.** The Department will configure BWCs to record 30 seconds of video, but not audio, prior to automatic or manual activation of the BWC.

# 43.4.8 Special Guidelines for Recording

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, and persons suspected of committing crimes, considering the needs of the investigation and the circumstances pertaining to the victim, witness, or suspect.

In addition,

- C. Officers need not record persons being provided medical care unless there is reason to believe the recording would document information having evidentiary value. When responding to an apparent mental health crisis or event, BWCs shall be activated as necessary to document any use of force and the basis for it, and any other information having evidentiary value, but need not be activated when doing so would serve only to record symptoms or behaviors believed to be attributable to the mental health issue.
- **D.** Officers shall use their BWCs and squad-based audio/video systems to record their transportation and the physical transfer of persons in their custody to hospitals, detox and mental health care facilities, juvenile detention centers, and jails, but otherwise should not record in these facilities unless the officer anticipates witnessing a criminal event or being involved in or witnessing an adversarial encounter or use-of-force incident.

# 43.4.9 **Downloading and Labeling Data**

- **A.** Each officer using a BWC is responsible for transferring or assuring the proper transfer of the data from his or her camera to evidence.com by the end of that officer's shift. However, if the officer is involved in a shooting, in-custody death, or other law enforcement activity resulting in death or great bodily harm, a supervisor or investigator shall take custody of the officer's BWC and assume responsibility for transferring the data from it.
- **B.** Officers shall label the BWC data files at the time of video capture or transfer to storage, and should consult with a supervisor if in doubt as to the appropriate labeling. Officers should assign as many of the following labels as are applicable to each file:
- 1. **Evidence—criminal:** The information has evidentiary value with respect to an actual or suspected criminal incident or charging decision.
- 2. **Evidence—force:** Whether or not enforcement action was taken or an arrest resulted, the event involved the application of force by a law enforcement officer of this or another agency.
- 3. **Evidence—property:** Whether or not enforcement action was taken or an arrest resulted, an officer seized property from an individual or directed an individual to dispossess property.
- 4. **Evidence—administrative:** The incident involved an adversarial encounter or resulted in a complaint against the officer.
- 5. **Evidence—other:** The recording has potential evidentiary value for reasons identified by the officer at the time of labeling.
- 6. **Training:** The event was such that it may have value for training.
- 7. **Not evidence:** The recording does not contain any of the foregoing categories of information and has no apparent evidentiary value. Recordings of general citizen contacts and unintentionally recorded footage are not evidence.

- C. Prior to the release of data, the person releasing the data shall determine if the BWC data contains information about data subjects who may have rights under the MGDPA limiting disclosure of information about them. These individuals include:
- 1. Victims and alleged victims of criminal sexual conduct and sex trafficking.
- 2. Victims of child abuse or neglect.
- 3. Vulnerable adults who are victims of maltreatment.
- 4. Undercover officers.
- 5. Informants.
- 6. When the video is clearly offensive to common sensitivities.
- 7. Victims of and witnesses to crimes, if the victim or witness has requested not to be identified publicly.
- 8. Individuals who called 911, and services subscribers whose lines were used to place a call to the 911 system.
- 9. Mandated reporters.
- 10. Juvenile witnesses, if the nature of the event or activity justifies protecting the identity of the witness.
- 11. Juveniles who are or may be delinquent or engaged in criminal acts.
- 12. Individuals who make complaints about violations with respect to the use of real property.
- 13. Officers and employees who are the subject of a complaint related to the events captured on video.
- 14. Other individuals whose identities the officer believes may be legally protected from public disclosure.
- **D.** Labeling and flagging designations may be corrected or amended based on additional information.

# 43.4.10 Administering Access to BWC Data:

- A. **Data subjects.** Under Minnesota law, the following are considered data subjects for purposes of administering access to BWC data:
- 1. Any person or entity whose image or voice is documented in the data.
- 2. The officer who collected the data.
- 3. Any other officer whose voice or image is documented in the data, regardless of whether that officer is or can be identified by the recording.
- B. **BWC data is presumptively private.** BWC recordings are classified as private data about the data subjects unless there is a specific law that provides differently. As a result:
- 1. BWC data pertaining to people is presumed private, as is BWC data pertaining to businesses or other entities.
- 2. Some BWC data is classified as confidential (see C. below).
- 3. Some BWC data is classified as public (see D. below).
- C. **Confidential data.** BWC data that is collected or created as part of an active criminal investigation is confidential. This classification takes precedence over the "private" classification listed above and the "public" classifications listed below.

- D. Public data. The following BWC data is public:
- 1. Data documenting the discharge of a firearm by a peace officer in the course of duty, other than for training or the killing of an animal that is sick, injured, or dangerous.
- 2. Data that documents the use of force by a peace officer that results in substantial bodily harm.
- 3. Data that a data subject requests to be made accessible to the public, subject to redaction. Data on any data subject (other than a peace officer) who has not consented to the public release must be redacted if practicable. In addition, any data on undercover officers must be redacted.
- 4. Data that documents the final disposition of a disciplinary action against a public employee.

However, if another provision of the 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 Minn. Stat. § 13.82, subd. 17 (e.g., certain victims, witnesses, and others) should not be released even if it would otherwise fit into one of the public categories listed above.

- E. Access to BWC data by non-employees. Officers shall refer members of the media or public seeking access to BWC data to the Chief of Police or their designee, who shall process the request in accordance with the MGDPA and other governing laws. In particular:
- 1. An individual shall be allowed to review recorded BWC data about him- or herself and other data subjects in the recording, but access shall not be granted:
- a. If the data was collected or created as part of an active investigation. b. To portions of the data that the agency would otherwise be prohibited by law from disclosing to the person seeking access, such as portions that would reveal identities protected by Minn. Stat. § 13.82, subd. 17.
- 2. Unless the data is part of an active investigation, an individual data subject shall be provided with a copy of the recording upon request, but subject to the following guidelines on redaction:
- a. Data on other individuals in the recording who do not consent to the release must be redacted.
- b. Data that would identify undercover officers must be redacted.
- c. 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.

- F. Access by peace officers and law enforcement employees. No employee may have access to the department's BWC data except for legitimate law enforcement or data administration purposes:
- 1. Officers may access and view stored BWC video only when there is a business need for doing so, including the need to defend against an allegation of misconduct or substandard performance or while preparing a police report. As provided in the critical incident response policy, officers may review video footage of an incident in which they were involved prior to preparing a report, giving a statement, or providing testimony about the incident.
- 2. Agency personnel shall document their reasons for accessing stored BWC data at the time of each access. Agency personnel are prohibited from accessing BWC data for non-business reasons and from sharing the data for non-law enforcement related purposes, including but not limited to uploading BWC data recorded or maintained by this agency to public and social media websites.
- 3. Members shall not retain personal copies of recordings.
- 4. Employees seeking access to BWC data for non-business reasons may make a request for it in the same manner as any member of the public.
- G. Other authorized disclosures of data. Officers may display portions of BWC footage to witnesses as necessary for purposes of investigation as allowed by Minn. Stat. § 13.82, subd. 15, as may be amended from time to time. Officers should generally limit these displays in order to protect against the incidental disclosure of individuals whose identities are not public. Protecting against incidental disclosure could involve, for instance, showing only a portion of the video, showing only screen shots, muting the audio, or playing the audio but not displaying video. In addition,
- 1. BWC data may be shared with other law enforcement agencies only for legitimate law enforcement purposes that are documented in writing at the time of the disclosure.
- 2. BWC data shall be made available to prosecutors, courts, and other criminal justice entities as provided by law.

# 43.4.11 Data Security Safeguards

- **A**. At the end of their shift, officers shall place the BWC into the docking station. This will allow the data to be transferred from the audio/video recorder through the docking station to Evidence.com. The data is considered impounded at this point and the BWC is cleared of existing data. The BWC should not be removed from the docking station until the data has been uploaded and the battery has been fully recharged.
- **B.** Personally owned devices, including but not limited to computers and mobile devices, shall not be programmed or used to access or view agency BWC data.
- C. Officers shall not intentionally edit, alter, or erase any BWC recording unless otherwise expressly authorized by the chief or the chief's designee.

**D.** 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.

## 43.4.12 Agency Use of Data

- **A**. At least once a month, supervisors will review BWC usage by each officer to ensure compliance with this policy
- **B**. In addition, supervisors and other assigned personnel may access BWC data for the purposes of reviewing or investigating a specific incident that has given rise to a complaint or concern about officer misconduct or performance.
- C. Nothing in this policy limits or prohibits the use of BWC data as evidence of misconduct or as a basis for discipline.
- **D**. Officers should contact their supervisors to discuss retaining and using BWC footage for training purposes. Officer objections to preserving or using certain footage for training will be considered on a case-by-case basis. Field training officers may utilize BWC data with trainees for the purpose of providing coaching and feedback on the trainees' performance.
- **E.** Recordings shall not be used by any member for the purpose of embarrassment, harassment, ridicule, or personal entertainment.
- **F.** Members should not use the fact that a recording was used as a reason to write a less detailed report.

# 43.4.13 Data Retention

- **A.** All BWC data shall be retained for a minimum period of 90 days.
- **B.** Data documenting the discharge of a firearm by a peace officer in the course of duty, other than for training or the killing of an animal that is sick, injured, or dangerous, must be maintained for a minimum period of one year.
- C. Certain kinds of BWC data must be retained for six years:
- 1. Data that documents the use of deadly force by a peace officer, or force of a sufficient type or degree to require a use of force report or supervisory review.
- 2. Data documenting circumstances that have given rise to a formal complaint against an officer.
- **D**. 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.

- **E.** Subject to Part F (below), all other BWC footage that is classified as non-evidentiary, becomes classified as non-evidentiary, or is not maintained for training shall be destroyed after 90 days.
- **F.** Upon written request by a BWC data subject, the agency shall retain a recording pertaining to that subject for an additional time period requested by the subject of up to 180 days. The agency will notify the requestor at the time of the request that the data will then be destroyed unless a new written request is received.
- G. The department shall maintain an inventory of BWC recordings having evidentiary value.
- **H.** The department will post this policy, together with its Records Retention Schedule, on its website.

# 43.4.14 Compliance

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