Farmington Police Department

Effective Date		
04/17/2018	2-04	

Subject		
USE OF VIDEO RECORDING TECHNOLOGY		
Reference		*Special Instructions*
13.01		
Distribution	*Reevaluation Date*	*No. Pages*
All Sworn Personnel	**05/31/2019**	**11**

I. Purpose

The primary purpose of using Video Recording Technology (VRT) is to capture evidence arising from police-citizen encounters. This policy sets forth guidelines governing the use of VRT 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.

II. Policy

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

III. Scope

This policy governs the use of VRT in the course of official duties. It applies to In-Car Video (ICV) systems, Body Worm Camera (BWC) systems, and Weapon Mounted Camera (WMC) systems. The chief or chief's designee may supersede this policy by providing specific instructions for VRT 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 VRT 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.

IV. 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 VRT 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 wrecker, 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 VRT, 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.

V. Use and Documentation

A. Officers may use only department-issued VRT 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 VRT shall operate and use them consistent with this policy. Officers shall conduct a function test of their issued VRT 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 Administrative Sergeant via email. The Administrative Sergeant shall take prompt action to address malfunctions and document the steps taken in writing.

C. Officers should utilize their VRT in the manner specified in training.

D. Officers must document VRT use and non-use as follows:

1. Whenever an officer makes a required recording, the existence of the recording shall be documented in the incident report or citation. Due to the automatic activation feature of the WMC, the fact that WMC data exists is required to be documented in the incident report relating to use of force involving the handgun.

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 email to their Patrol Sergeant and the Administrative Sergeant. Supervisors shall review these reports and initiate any corrective action deemed necessary.

E. The department will maintain the following records and documents relating to VRT use, which are classified as public data:

1. The total number of ICVs, BWCs, and WMCs owned or maintained by the agency;

2. A daily record of the total number of ICVs, BWCs, and WMCs actually deployed and used by officers;

3. The total amount of recorded VRT data collected and maintained; and

4. This policy, together with the Records Retention Schedule.

VI. General Guidelines for Recording

A. Officers shall activate their BWCs when anticipating that they will be involved in, become involved in, or witness other officers of this agency involved in a pursuit, *Terry* stop of a motorist or pedestrian, search, seizure, arrest, use of force, adversarial contact, and during other

activities likely to yield information having evidentiary value. However, officers need not activate their cameras when it would be unsafe, impossible, or impractical to do so, but such instances of not recording when otherwise required must be documented as specified in the Use and Documentation guidelines, part (D)(2) (above).

ICV systems will be automatically set to begin recording whenever the emergency lights are activated or when the crash sensor is activated. Officers may also manually activate the ICV during other activities likely to yield information having evidentiary value.

WMCs are automatically activated and begin recording when the officer removes their handgun from the WMC-equipped holster. The WMC automatically ceases recording when the handgun is holstered. Officers will not deliberately keep their handgun out of the holster for the sole purpose of continuing to record with the WMC.

B. Officers have discretion to record or not record general citizen contacts.

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

D. Once activated, the ICV and 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.

E. Officers shall not intentionally block the VRTs audio or visual recording functionality to defeat the purposes of this policy.

F. Notwithstanding any other provision in this policy, officers shall not use their VRT 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.

VII. Special Guidelines for Recording

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

A. To use their ICVs and 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 ICV rear facing camera 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.

VIII. 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, an investigator shall take custody of the officer's BWC and assume responsibility for transferring the data from it.

ICV files will automatically upload to the police department's secure server when the patrol vehicle arrives at the police department. Each officer is responsible for ensuring that this process is functioning as intended. If an ICV fails to automatically upload, the officer shall notify the Administrative Sergeant via email.

Each officer using a WMC is responsible for notifying a Patrol Sergeant anytime their WMC captures a use of force incident. If the incident did not result in an actual shooting, the Patrol Sergeant shall manually upload the video to Evidence.com by using Evidence Upload XT or whatever the

current Axon method is, and label it appropriately. If the incident did result in an officer involved shooting, an investigator shall take custody of the officer's weapon and WMC and assume responsibility for transferring the data from it.

All WMCs will be scheduled for manual download, by a Patrol Sergeant, on a bi-monthly basis to save all other non-evidentiary data. All non-evidentiary WMC data will be uploaded to Evidence.com and labeled as 'Not Evidence'. The Administrative Sergeant will monitor the volume of WMC data generated to determine if a more or less frequent download schedule is necessary.

B. Officers and/or Patrol Sergeants shall label the VRT 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.

IX. 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. 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 his or her 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 himself/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 VRT data except for legitimate law enforcement or data administration purposes:

1. Officers may access and view stored VRT video only when there is a business need for doing so, including the need to defend against an allegation of misconduct or substandard performance. 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 by entering that reason in the notes section of the data on Evidence.com at the time of each access. This note shall become part of the official record and will also be logged in the audit trail. Agency personnel are prohibited from accessing BWC data for non-business reasons and from sharing the data for non-law enforcement related purposes, including but not limited to uploading BWC data recorded or maintained by this agency to public and social media websites.

3. Employees seeking access to VRT 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 VRT 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. VRT 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. VRT data shall be made available to prosecutors, courts, and other criminal justice entities as provided by law.

X. Data Security Safeguards

A. The Farmington Police Department utilizes two disparate data retention systems for the three types of VRT data.

1. BWC data is stored on Evidence.com, a secure platform provided by Axon. Access to this system uses multi-factor authentication and an audit trail exists within Evidence.com. By their role, officers can only view their own data. However, supervisors, investigations and records staff have access to view all videos in performance of their duties.

2. WMC data is stored on the camera, which is password protected. Employees holding the rank of Sergeant or higher have passwords. When the data is downloaded, it will be temporarily stored on the department's secure server and then uploaded to Evidence.com. Once uploaded, the data will be deleted from the department's secure server. The department's secure server is backed up daily, so in the event that the data is not immediately transferred to Evidence.com, the data will be retained.

3. ICV data is stored on the department's secure server through the Arbitrator platform. The data is wirelessly uploaded from the squad to the server via a secured access point. The system confirms that the data has been successfully transferred before removing it from the in-car recorder. Access to Arbitrator is password protected. By their role, officers can only view their own data. ICV data is backed up daily.

B. Access to VRT data from city or personally owned and approved devices shall be managed in accordance with established city policy.

C. Officers shall not intentionally edit, alter, or erase any VRT 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.

XI. Agency Use of Data

A. At least once a month, supervisors will randomly review VRT usage by each officer to ensure compliance with this policy and to identify any performance areas in which additional training or guidance is required.

B. In addition, supervisors and other assigned personnel may access VRT 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 VRT data as evidence of misconduct or as a basis for discipline.

D. Officers should contact their supervisors to discuss retaining and using VRT data for training purposes. Officer objections to preserving or using certain data 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.

XII. Data Retention

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

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

C. Certain kinds of VRT 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 VRT 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 VRT 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 VRT recordings having evidentiary value.

H. The department will post this policy, together with its Records Retention Schedule, on its website.

XIII. 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.