INDEPENDENT AUDITOR'S REPORT

South Lake Minnetonka Police Department Body-Worn Camera Program

MARCH 11, 2022

RAMPART DEFENSE LLC
P.O. Box 23 Clearbrook, MN 56634

Audit Overview and Recommendations

Dear Excelsior, Greenwood, Shorewood and Tonka Bay City Councils and Chief Tholen:

We have audited the body-worn camera (BWC) program of the South Lake Minnetonka Police Department (SLMPD) for the two-year period ended 12/31/2021. Minnesota Statute §13.825 mandates that any law enforcement agency operating a portable recording system (PRS)[1] program obtain an independent, biennial audit of its program. This program and its associated data are the responsibility of the South Lake Minnetonka Police Department. Our responsibility is to express an opinion on the operations of this program based on our audit.

On February 1, 2022, Rampart Defense LLC (Rampart) met with Lt. Justin Ballsrud, who provided information about SLMPD's BWC program policies, procedures and operations. As part of the audit, Rampart reviewed those policies, procedures and operations for compliance with Minnesota Statute §626.8473, which sets forth the requirements for creating and implementing a BWC program, and Minnesota Statute §13.825, which governs the operation of BWC programs. In addition, Rampart also conducted a sampling of BWC data to verify SLMPD's recordkeeping.

The purpose of this report is to provide an overview of this audit, and to provide recommendations to improve the SLMPD BWC program and enhance compliance with statutory requirements.

SLMPD BWC Program Implementation and Authorization

Effective August 1, 2016, Minnesota Statute §626.8473 Subd. 2 requires that:

> A local law enforcement agency must provide an opportunity for public comment before it purchases or implements a portable recording system. At a minimum, the agency must accept public comments submitted electronically or by mail, and the governing body with jurisdiction over the budget of the law enforcement agency must provide an opportunity for public comment at a regularly-scheduled meeting.

Lt. Ballsrud provided a copy of a notice soliciting comments and questions from the public regarding SLMPD's proposed BWC program in advance of a regularly scheduled meeting on October 10, 2018. A copy of this document has been retained in Rampart's audit files. In our opinion, South Lake Minnetonka Police Department met the public notice and comment requirements prior to the implementation of their BWC program.

[1] It should be noted that Minnesota statute uses the broader term "portable recording system" (PRS), which includes body-worn cameras. Because body-worn cameras are the only type of portable recording system employed by SLMPD, these terms may be used interchangeably in this report.

In addition, §626.8473 Subd. 3(a) requires that the law enforcement agency establish and enforce a written policy governing the use of its portable recording system, and states "[t]he written policy must be posted on the agency's Web site, if the agency has a Web site."

Lt. Ballsrud furnished to Rampart a copy of SLMPD's written BWC policy. At the time of our audit, there was no link to the BWC policy on SLMPD's website. Lt. Ballsrud advised us that he would have a link added immediately. Rampart received an email with the link the following morning. We have verified that this link works and is accessible from the SLMPD website. As of our report date, this issue has been resolved.

SLMPD BWC WRITTEN POLICY

As part of this audit, we reviewed SLMPD's BWC policy, a copy of which is attached to this report as Appendix A.

Minnesota Statute §626.8473 Subd. 3(b) requires a written BWC policy to incorporate the following, at a minimum:

1. The requirements of section 13.825 and other data classifications, access procedures, retention policies, and data safeguards that, at a minimum, meet the requirements of chapter 13 and other applicable law;
2. Procedures for testing the portable recording system to ensure adequate functioning;
3. Procedures to address a system malfunction or failure, including requirements for documentation by the officer using the system at the time of a malfunction or failure;
4. Circumstances where recording is mandatory, prohibited, or at the discretion of the officer using the system;
5. Circumstances under which a data subject must be given notice of a recording;
6. Circumstances under which a recording may be ended while an investigation, response, or incident is ongoing;
7. Procedures for the secure storage of portable recording system data and the creation of backup copies of the data; and
8. Procedures to ensure compliance and address violations of the policy, which must include, at a minimum, supervisory or internal audits and reviews, and the employee discipline standards for unauthorized access to data contained in section 13.09.

Due to their complexity and interrelatedness, clauses 1 and 7 are discussed separately below. Clause 8 is also discussed separately.

In our opinion, the SLMPD BWC policy is compliant with respect to clauses 2 – 6.

SLMPD BWC Data Retention

South Lake Minnetonka Police Department follows the General Records Retention Schedule for Minnesota Cities (GRRSMC) with respect to BWC data classified as evidentiary in nature. SLMPD's BWC policy defines this to include "information [that] 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." A review of the relevant sections of the current GRRSMC schedule indicates that the stated retention guidelines appear to meet or exceed the requirements specified for each category of BWC data enumerated in §13.825 Subd. 3(b). SLMPD's policy specifies a 90-day retention period for all other BWC data, as required in §13.825 Subd. 3(a).

SLMPD employs Watchguard body-worn cameras, with all BWC data stored on Watchguard's secure, cloud-based servers. SLMPD manages BWC data retention automatically through its Watchguard software, based on the data classification assigned to each video at the time of upload.

SLMPD's BWC policy requires that each officer transfer data from his or her body-worn camera via the Watchguard Transfer Station by the end of each shift, and also requires that the officer assign the appropriate label or labels to each file to identify the nature of the data.

SLMPD's BWC policy states that "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." Data sharing is accomplished via a weblink through Watchguard's cloud service. Lt. Ballsrud also submitted a sample of the written disclaimer that is included with every such weblink regarding the receiving agency's obligations under §13.825 Subd. 7 and Subd. 8, which include a requirement to maintain BWC data security. Lt. Ballsrud is responsible for reviewing and approving all external requests for BWC data.

In our opinion, SLMPD's written BWC policy is compliant with respect to applicable data retention requirements.

SLMPD BWC Data Destruction

As discussed in the preceding section, Lt. Ballsrud advised us that SLMPD BWC data are stored on Watchguard's cloud-based servers, with data retention and deletion schedules managed automatically through the Watchguard software based on the assigned data classification of each video.

In our opinion, SLMPD's written BWC policy is compliant with respect to the applicable data destruction requirements.

SLMPD BWC Data Access

SLMPD's BWC policy states that the Records Division is responsible for processing requests from members of the public or the media for access to BWC data. All such requests are processed "in accordance with the MGDPA [Minnesota Government Data Practices Act] and other governing laws."

According to SLMPD policy, 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." In addition, "BWC data shall be made available to prosecutors, courts, and other criminal justice entities as provided by law."

In our opinion, SLMPD's written BWC policy is compliant with respect to the applicable data access requirements.

SLMPD BWC Data Classification

SLMPD BWC Policy states that "BWC data is presumptively private," and further states that "BWC recordings are classified as private data about the data subjects unless there is a specific law that provides differently." Active criminal investigation data are classified as confidential. SLMPD BWC Policy also identifies certain categories of BWC data that are public.

This section of the SLMPD BWC policy mirrors the categories and language of §13.825 Subd. 2. In our opinion, this policy is compliant with respect to the applicable data classification requirements.

SLMPD BWC Internal Compliance Verification

The SLMPD BWC Agency/Supervisor Use of Data section states that:

> Supervisors shall review BWC usage by each officer to ensure compliance with this policy, including in areas of required recording and data labeling.
>
> In addition, supervisors may access BWC data for the purpose of reviewing or investigating a specific incident that has given rise to a complaint or concern about officer misconduct or performance.

SLMPD's written BWC policy addresses consequences associated with violations of the policy, to include both disciplinary action and potential criminal penalties.

In our opinion, this policy is compliant with respect to the compliance and disciplinary requirements contained in §626.8473 Subd. 3(b)(8).

SLMPD BWC Program and Inventory

SLMPD currently possesses sixteen (16) Watchguard body-worn cameras.

The SLMPD BWC policy identifies those circumstances in which deputies are expected to activate their body-worn cameras, as well as circumstances in which they are prohibited from activating their body-worn cameras. The policy also provides guidance for those circumstances in which BWC activation is deemed discretionary.

Lt. Ballsrud advised us that he is able to determine the number of BWCs deployed by reviewing the schedule and/or payroll data.

As of the audit date, February 1, 2022, SLMPD maintained 18,351 BWC file events.

SLMPD BWC Physical, Technological and Procedural Safeguards

SLMPD BWC data are initially recorded to a hard drive in each officer's BWC. Prior to the end of each shift, the officer places his or her BWC in a docking station at SLMPD. Any BWC data are then uploaded automatically to Watchguard's cloud-based servers. During the period covered by our audit, Lt. Ballsrud identified instances in which two cameras failed to apply the proper labels to some BWC data. This appears to be a synching issue between the cameras and the squad video systems. Because unlabeled data is retained indefinitely, this issue did not result in the loss of data. SLMPD is currently working with Watchguard to resolve the issue. As the administrator, Lt. Ballsrud is able to add or correct labels as needed.

Officers have view-only access to their own data for report writing, trial preparation, data administration, investigatory purposes and other legitimate law enforcement purposes. Officers are required to document the reasons for accessing BWC data each time they do so. All BWC data access is logged in the Watchguard software and is available for audit purposes.

As noted above, requests by other law enforcement agencies for SLMPD BWC data must be approved by Lt. Ballsrud. This data is furnished to the requesting agency via a weblink. SLMPD follows this same process when providing BWC data to prosecutors and the courts.

Enhanced Surveillance Technology

SLMPD currently employs BWCs with only standard audio/video recording capabilities. They have no plans at this time to add enhanced BWC surveillance capabilities, such as thermal or night vision, or to otherwise expand the type or scope of their BWC technology.

If SLMPD should obtain such enhanced technology in the future, Minnesota Statute §13.825 Subd. 10 requires notice to the Minnesota Bureau of Criminal Apprehension within 10 days. This notice must include a description of the technology and its surveillance capability and intended uses.

Data Sampling

Rampart selected a random sample of 133 ICRs from which to review any available BWC recordings. It should be noted that not every call will result in an officer activating his or her BWC. For example, an officer who responds to a driving complaint but is unable to locate the suspect vehicle would be unlikely to activate his or her BWC. It should also be noted that because the audit covers a period of two years, while most BWC data is only required to be retained for 90 days, there is a significant likelihood that the sample population will include ICRs for which BWC data was created, but which has since been deleted due to the expiration of the retention period. The auditor reviewed the retained BWC videos to verify that this data was accurately documented in SLMPD records.

During this review, we identified three instances in which the synching issue described earlier resulted in BWC data lacking classification labels. In all instances, however, the videos were properly identified by ICR number. Two of the three videos were manually labeled after the fact; the third had not been manually labeled and was therefore retained beyond its allowable destruction date.

SLMPD's Watchguard system is programmed to activate both the squad camera and the officer's BWC when an officer activates his squad's emergency lights. We identified one instance in which the synching issue resulted in a body-worn camera failing to record when an officer activated his emergency lights to conduct a traffic stop. The Rampart auditor was able to review the squad video from the stop. As noted above, Lt. Ballsrud is working with Watchguard to resolve the synching issue.

Audit Conclusions

In our opinion, the South Lake Minnetonka Police Department's Body-Worn Camera Program is substantially compliant with Minnesota Statutes §13.825 and §626.8473.

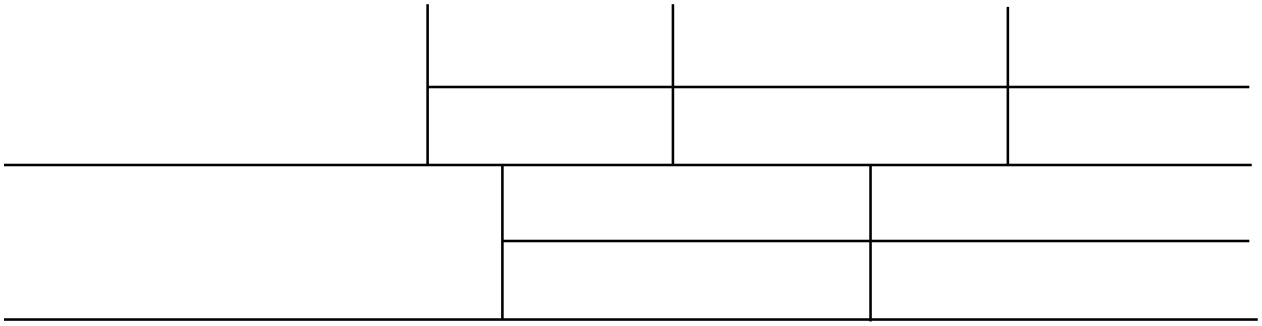
_____

Daniel E. Gazelka

Rampart Defense LLC

3/11/2022

Appendix A Below



APPENDIX A:

DEPARTMENT MANUAL

SOUTH LAKE MINNETONKA POLICE DEPARTMENT	ISSUE DATE	EFFECTIVE DATE	NUMBER
GENERAL ORDER	06/22/2017	06/22/2017	2004

BODY WORN CAMERAS	DISTRIBUTION	RESCINDS
	ALL PERSONNEL	N/A

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 is generated. 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.

OBJECTIVES

The South Lake Minnetonka Police Department has adopted the use of BWCs to

accomplish the following objectives:

A. To enhance the public trust by preserving factual representations of officer-citizen interactions in the form of audio-video recordings.
B. To document statements and events during an incident.
C. To enhance the officer's ability to document and review statements and actions for both internal reporting requirements and for courtroom preparation/presentation.
D. To preserve audio and visual information for use in current and future investigations.
E. To provide a tool for self-critique and field evaluation during officer training.
F. To enhance officer safety.
G. To assist with the defense of civil actions against law enforcement officers and the South Lake Minnetonka Police Department.
H. To assist with the training and evaluation of officers.

POLICY

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

SCOPE

Every sworn, full-time officer of the South Lake Minnetonka Police Department will be issued a body-worn-camera for use during their official duties.

This policy governs the use of BWCs during official duties. It does not apply to the use of squad-based camera recording systems or mobile surveillance cameras. This policy does not apply to audio/video recordings, interviews or interrogations conducted at any South Lake Minnetonka Police Department facility, undercover operations, wiretaps, or eavesdropping (concealed listening devices) unless captured by a BWC.

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 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.

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 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 which 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.

I. **Body-Worn-Camera (BWC)** – A device worn on the person of a police department employee that is capable of recording video and audio footage.

J. **Data Subject** – Under Minnesota Law, the following are considered data subjects for purposes of administering 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

K. **Confidential Data** – BWC data that is collected or created as part of an active criminal investigation is confidential. This classification takes precedence over private and/or public classifications.

L. **Private Data** – BWC recordings are presumptively classified as private data about the data subjects under MN statutes, with applicable Data Practices Act provisions applying.

M. **Public Data** – In certain instances, BWC data is classified public data under MN statutes, with applicable provisions of the Data Practices Act applying:

    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, injured, or dangerous.
    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 (Minn. Stat. §13.825, subd. 2(a)(2)). In addition, any data on undercover officers must be redacted.
    d. Data that documents the final disposition of a disciplinary action against a public employee.
    e. If another provision of the Data Practices Act classifies data as private or otherwise not public, the data retains that other more restricted classification. For instance, data that reveals protected identities under MN Statute 13.82, subd. 17 would not be released, even if it would otherwise fit into the public category.

USE AND DOCUMENTATION

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. BWC use for off duty law enforcement related employment purposes must be approved by the Chief of Police.

B. All police officers working uniform patrol, uniform special details, and traffic duties shall use a BWC unless permission has been granted by a supervisor to deviate from this clause. Plain clothes investigators/officers and administrators are not obligated to use a BWC but may elect to use a BWC on a case by case basis, pursuant to the needs of the specific investigation or job duty.

C. Officers who have deployed a BWC shall operate and use it 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. As soon as is practical, the malfunctioning BWC shall be put down for service and the officer should deploy a working BWC. If a BWC malfunctions while recording, is lost or damaged, the circumstances shall be documented in a police report and a supervisor shall be notified.

D. Officers should wear their issued BWCs at the location on their body and in the manner specified in training.

E. 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, citation, or in a CAD event (if no report is completed).

2. Whenever an officer fails to record an activity that is recommended 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 or Records Management System (RMS) event (if no report is completed). Supervisors shall ensure BWC use is in compliance with this policy when reviewing reports and CAD data.

F. The department will maintain the following records 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.

G. Pursuant to Minn. Stat. § 13.825, subd. 6, officers may only use a portable recording system issued and maintained by the South Lake Minnetonka Police Department in documenting the officer's activity.

GENERAL GUIDELINES FOR RECORDING

A. This policy is not intended to describe every possible situation in which the BWC should be activated, although there are many situations where use of the BWC is appropriate. Officers should activate the BWC any time the user believes it would be appropriate or valuable to record an incident.

B. Officers are encouraged to activate their BWCs when responding to all calls for service and field generated activities, including but not limited to pursuits, *Terry* stops of motorists or pedestrians, arrests, searches, suspect interviews and interrogations, implied consent protocols conducted outside of a recorded booking facility, search warrant advisories (blood & urine), and during any police/citizen contact that becomes, or is anticipated to be adversarial. 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 recommended must be documented as specified in the Use and Documentation guidelines, part (E-2 above).

C. Recording After-the-Fact. Officers shall follow the record-after-the-fact protocol when they are unable to activate their BWC during an on-duty event and the event falls into any of the following categories:

1. The event is a critical incident as defined by South Lake Minnetonka PD Policy 2030.

2. Whenever force is used by a SLMPD officer.

3. Whenever a firearm is discharged by an officer other than for training or the killing of an animal that is sick, injured, or dangerous.

4. It is reasonably foreseeable that data from the BWC will be valuable for potential civil litigation.

5. It is reasonably foreseeable that data from the BWC will be valuable for the resolution of a complaint against an officer(s).

6. Any other instances of non-recording where the officer believes it may be beneficial to save BWC data.

D. Record After-the Fact Protocol

1. **Activating the body-worn-camera (BWC) in mid event:**
   a) As soon as the officer realizes they are not recording, activate the BWC. This will start the recorder including the 30 second pre-record. Because the BWC mics are not enabled, audio will begin after the 30 second pre-record.
   b) When the event is finished, stop and tag the video as usual.
   c) Return to the office and place the BWC in the transfer station and upload the video.
   d) Power down the BWC and place it in an evidence locker in accordance with South Lake Minnetonka Policy 2039.
   e) Notify a supervisor of the date and time of the incident, that the BWC is locked in evidence, and the BWC requires recording-after-the-fact.

2. **Activating the BWC after an event has finished:**
   a) Power down the BWC and place it in an evidence locker in accordance with South Lake Minnetonka Policy 2039.
   b) Notify a supervisor of the date and time of the incident, that the BWC is locked in evidence, and the BWC requires recording-after-the-fact.

E. Officers have discretion to record or not record general citizen contacts of a non-adversarial nature.

F. Officers shall not record encounters with undercover officers or informants.

G. Officers have no affirmative duty to, without prompting or question, inform people that a BWC is being operated or that the individuals are being recorded during an incident. Officers may elect to inform individuals that they are being recorded if the officer deems it necessary and appropriate, in furtherance of conflict resolution and/or de-escalation of tense situations. If an individual asks the officer if they are recording, the officer shall answer truthfully. Individuals requesting government data will be referred to the records division.

H. 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 supervisor having charge of a scene may 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. Any decision to discontinue recording shall be made with respect to the eight policy objectives.

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

J. 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.

K. In instances of non-recording, where recording was preferred or required, the officers shall consult with the supervisor and/or Lieutenant to see if the video data may be recovered from the BWC utilizing the record-after-the-fact function. This consultation should occur as soon as practical after it is realized that a recording was not captured.

L. Formal statements from suspects, victims, or witnesses that are captured on the BWC shall be recorded as separate recordings on a non BWC audio recording device to be entered as evidence and transcribed.

M. Officers are not required to use the BWC while inside the SLMPD booking facility or other recorded booking facility.

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. 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, collecting evidentiary recordings, or being involved in or witnessing an adversarial encounter or use-of-force incident.

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 the BWC server/cloud 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 end of each video capture and should consult with a supervisor if in doubt as to the appropriate labeling. Officers shall properly categorize all BWC recordings using one of the labels pre-programmed into the BWC. The category label selected shall most closely represent the type of content captured on the BWC. The selected category shall determine the retention period of the file.

C. If a BWC data file is mislabeled by an officer, or additional information is discovered that suggests a data file label should be changed, a request to change the label and reasoning for said change shall be forwarded to the support services technician.

BWC DATA ACCESS BY LAW ENFORCEMENT EMPLOYEES

A. **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. 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. Officers shall not use the fact that a recording was made as a reason to write a less detailed report.

2. Supervisors may view recordings any time they are making inquiry into an alleged complaint, performance issue, or to ensure policy compliance.

3. 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. All instances of access to BWC data are digitally logged. Allegations of inappropriate access to BWC data will be investigated and discipline may be issued pursuant to the labor contract.

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.

B. **Other authorized disclosures of data by officers.** 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. BWC footage should not be used for purposes of suspect identification in a "show-up" and use of BWC data must comply with SLMPD Policy 4020. Officers should generally limit these displays 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.

AGENCY/SUPERVISOR USE OF DATA

A. Supervisors shall review BWC usage by each officer to ensure compliance with this policy, including in areas of required recording and data labeling.

B. In addition, supervisors 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.

DATA CALSSIFICATION AND ACCES BY NON-EMPLOYEES

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 (Minn. Stat. §13.825, subd. 2(a)(2)) 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 Records Division 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:

    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.

    d. Data subject shall complete an official request form and pay any associated fees from the adopted fee schedule.

DATA SECURITY SAFEGUARDS

A. BWC devices issued by the South Lake Minnetonka Police Department are designed and manufactured to prevent users from being able to alter, edit and/or delete recorded footage. Any recorded footage will automatically upload to a central storage location via a secured wireless and/or wired connection to the department's video server.

B. The South Lake Minnetonka Police Department's BWC server/cloud is capable of, and will automatically note the user, date, and time of access to BWC footage in the chain of custody report.

C. 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.

D. Officers shall not intentionally edit, alter, or erase any BWC recording unless otherwise expressly authorized by the chief or the chief's designee.

E. 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.

DATA RETENTION

It is the BWC user's responsibility to properly categorize all recorded BWC footage for purposes of retention timelines, using categories set up in South Lake Minnetonka Police Department's BWC server/cloud and on individual BWCs. The following guidelines will be adhered to regarding data retention:

A. All BWC 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 of one year.

C. The following types of BWC footage shall be retained for at least six years:
   - Data that documents the use of deadly force by a peace officer, or force of a sufficient degree to require a use of force report or supervisory review
   - Data documenting circumstances that have given rise to a formal complaint against the officer

D. Other data having evidentiary value shall be retained for the period specified in the Records Retention Schedule. When a recording is subject to multiple retention periods, it shall be maintained for the longest applicable period.

E. All other BWC footage that is classified as non-evidentiary, or that no longer contains evidentiary value, or is not maintained for training, shall be destroyed after 90 days.

F. Upon written request of a BWC data subject, the agency shall retain a recording pertaining to that subject for an additional time period requested 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 request is received.

The South Lake Minnetonka Police Department's BWC server/cloud shall maintain an inventory of all BWC recordings listed as having evidentiary value.

ALLEGATIONS OF MISCONDUCT

Any complaints of misconduct surrounding South Lake Minnetonka Police Department BWC use under this policy or others will be investigated on a case-by-case basis, pursuant to the collective bargaining agreement, MN police officer discipline procedures act (M.S. 626.89) and department policy (Allegations of Misconduct).

Any employee misusing recorded media or devices in violation of this or other policies or statutes will be subject to disciplinary action. Discipline may include verbal reprimand, written reprimand, suspension, demotion, or termination. If criminal behavior is alleged, appropriate agencies will be notified for further investigation.

The specific situation in each case of a policy violation will be evaluated with consideration to all circumstances when determining disciplinary actions.