INDEPENDENT AUDITOR'S REPORT

ROYALTON POLICE DEPARTMENT BODY-WORN CAMERA PROGRAM

JUNE 2, 2021

RAMPART DEFENSE, LLC
P.O. BOX 23 CLEARBROOK, MN 56634

What Follows is the Royalton Police Department as presented to Rampart Defense LLC for compliance auditing check. After that Policy you will find our audit overview and recommendations.

ROYALTON POLICE DEPARTMENT

GENERAL ORDER: 600.200

EFFECTIVE DATE: OCTOBER 2020

SUBJECT: BODY WORN CAMERA

I. Purpose

The use of body-worn cameras (BWCs) in law enforcement is relatively new. The primary purpose of using BWCs is to capture evidence arising from police-citizen encounters. While this technology allows for the collection of valuable information, it opens up many questions about how to balance public demands for accountability and transparency with the privacy concerns of those being recorded. In deciding what to record, this policy also reflects a balance between the desire to establish exacting and detailed requirements and the reality that officers must attend to their primary duties and the safety of all concerned, often 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 BWCs as set forth below.

III. Scope

This policy governs the use of BWCs in the course of official duties. It does not apply to the use of surreptitious recording devices in undercover operations or the use of squad-based (dash-cam) video recorders. The chief or chief's designee may supersede this policy by providing specific instructions for the use of BWCs to individual officers, or

providing specific instructions for the use of BWCs pertaining to certain events or classes of events, including but not limited to political rallies and demonstrations. The chief or chief 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.

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 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 encounter 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. Unintentional Recording 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 or administrative 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. Traffic/Pedestrian Stop, for purposes of this policy, means that the officer is on duty and performing authorized law enforcement services on behalf of this agency, and has undertaken a stop of this nature.

V. 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.

B. Officers who have been issued BWCs shall operate and use them consistent with this policy. Officers shall check their issued BWCs at the beginning of each shift to make sure the devices are functioning properly and shall promptly report any malfunctions to the officer's supervisor.

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

D. Officers must document BWC use and nonuse as follows:

1. 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 or CAD. Supervisors shall review these reports and initiate any corrective action deemed necessary.

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 toyield 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).

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 they are being recorded.

D. 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. 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 BWC's audio or visual recording functionality to defeat the purposes of this policy. Officers may when deemed necessary, mute the audio for the purposes of sensitive conversations with other officers.

F. 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.

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

VII. Special Guidelines for Recording

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

A. To use their BWC 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 BWC to take recorded statements from persons believed to be victims and witnesses of 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. Officers may activate their BWCs when dealing with individuals believed to be experiencing a mental health crisis or event. BWCs shall be activated as necessary to document any use of force and the basis therefor 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 should use their BWCs and or 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.

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 by docking the unit at 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.

1. Evidentiary: The information has evidentiary value with respect to an actual or suspected criminal incident or charging decision above the level of Petty Misdemeanor. The recording has potential evidentiary value for reasons identified by the officer at the time of labeling. 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.

2. Use of Force/Pursuit: 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. Adversarial: The incident involved an adversarial encounter.

4. Training Value: The event was such that it may have value for training.

5. Unintentional Recording: Footage captured through unintentional activation will be deleted at the end of the officer shift.

6. General: The recording does not contain any of the foregoing categories of information and has no apparent evidentiary value. Recordings of general citizen contacts are not evidence.

7. Traffic/Petty Citation: The recording documents the issuance of a Petty Misdemeanor violation.

8. Traffic/Pedestrian Stop: The recording documents the undertaking of a pedestrian or traffic stop no resulting in charges.

C. Labeling and flagging designations may be corrected or amended based on additional information.

IIX. Access to BWC DataA. All safeguards in place by WATCHGUARD VIDEO SYSTEMS will meet or exceed required security parameters. In addition:

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

C. 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.

D. 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 limit these displays to protect against the incidental disclosure of individuals whose identities are not public.

E. 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 onto public and social media websites.

F. Officers shall refer members of the media or public seeking access to BWC data to the the Chief of Police, who will process the request in accordance with the MGDPA and other governing laws. 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. BWC data shall be made available to prosecutors, courts, and other criminal justice entities as provided by law.

H. Prior to release of data, the Records Division shall determine if a file is appropriate for release if it contains subjects who may have rights under the MGDPA limiting public disclosure of information about them. These individuals include:

1. Victims and alleged victims of criminal sexual conduct.

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.

IX. Agency Use of Data

A. 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.

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

C. Officers should contact their supervisor 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 trainee's performance.

X. Data Retention

A. Evidentiary data shall be retained for the period specified in the General Records Retention Schedule for Minnesota Cities. When a particular recording is subject to multiple retention periods, it shall be maintained for the longest applicable retention period

B. Unintentionally recorded footage shall not be retained

C. BWC footage that is classified as non-evidentiary, or becomes classified as non-evidentiary, shall be retained for a minimum of 90 days following the date of

capture If information comes to light indicating that non-evidentiary data has evidentiary value or value for training, it may be reclassified and retained for a longer period

D. The department shall maintain an inventory of BWC recordings

Audit Overview and Recommendations

Dear Royalton City Council and Chief Bruyere:

We have audited the body-worn camera (BWC) program of the Royalton Police Department (RPD) for the period of 3/30/2019 – 3/31/2021. 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 Royalton Police Department. Our responsibility is to express an opinion on the operation of this program based on our audit.

On April 13, 2021, Rampart Defense LLC (Rampart) met with Chief Lindsey Bruyere, who provided information about RPD's BWC program policies, procedures and operations. As part of the audit, Rampart also conducted a sampling of BWC data to verify RPD's recordkeeping.

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

RPD 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.

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."

Chief Bruyere advised us that the RPD BWC program was already in operation when he was appointed chief in July of 2019. He also advised us that he had voluntarily suspended BWC use effective January 1, 2021, until Rampart could complete our audit and verify that the program was substantially compliant with Minnesota Statutes §13.825 and §626.8473, and any necessary policy updates could be made. At the time of our initial engagement, Chief Bruyere was unable to determine whether the public notification requirement under §626.8473 Subd. 2 had been met, or whether the RPD BWC policy had been properly adopted by the Royalton City Council. Such a suspension was our recommended

[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 RPD, these terms may be used interchangeably in this report.

approach. Chief Bruyere subsequently submitted documentation showing that these requirements were, in fact, met in July of 2017.

At the time of our audit, there was no link to the RPD BWC policy on the RPD page of the City of Royalton website. As noted above, such a link is required by §626.8473 Subd. 3(a). Prior to the issuance of this report, however, we verified and documented that a link to the BWC policy had been added to the City of Royalton website.

RPD BWC WRITTEN POLICY

As part of this audit, we reviewed RPD'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.

While the RPD policy is comprehensive and thorough with respect to clauses 2 - 6, we noted that it does not address potential disciplinary actions for violations, such as misusing cameras and/or data, which is a requirement of clause 8. Chief Bruyere advised us that the City of Royalton's personnel policy addresses data usage and misconduct. We strongly recommend incorporating that policy by reference in RPD's BWC policy.

In addition, Chief Bruyere advised us that he conducts internal audits of BWC data. We recommend noting this in RPD's BWC policy as well.

RPD BWC Data Retention

RPD currently follows League of Minnesota Cities guidelines for data retention, which specify a minimum 90-day retention period. This is consistent with Minnesota Statute §13.825, which also includes certain exceptions requiring longer retention periods. Chief Bruyere advised that he is assessing the feasibility of adopting a minimum two-year retention schedule for BWC data.

We noted that that Item B of the Data Retention Section states: "Unintentionally recorded footage shall not be retained." As discussed above, §13.825 specifies a minimum retention period of 90 days for all BWC data. Because there is no exception listed in the statute for unintentional or test recordings, we strongly recommend that RPD retain these recordings for a minimum of 90 days prior to deletion.

RPD creates an optical disc (CD/DVD) of evidentiary data for case files. These discs are retained until the statute of limitations expires or all judicial proceedings are complete.

RPD BWC Data Destruction

Chief Bruyere advised us that RPD BWC data stored on hard drives is destroyed through manual deletion and overwriting. In addition, any hard drive retired from service will be physically destroyed through mechanical means. Any optical discs created for case files are physically destroyed by breaking the discs after the statute of limitations expires or all judicial proceedings are complete.

We recommend noting these procedures in the written policy.

RPD BWC Data Access

RPD contracts with the Morrison County Sheriff's Office to process data requests. Any requests for access to BWC data by data subjects would be facilitated by Chief Bruyere in accordance with the provisions of §13.825 Subd. 4(b).

RPD BWC data is shared with other law enforcement agencies for evidentiary purposes only. All such requests must be made to Chief Bruyere by the requesting agency's chief law enforcement officer (CLEO). Existing verbal agreements between RPD and other area law enforcement agencies address data classification, destruction and security requirements, as specified in §13.825 Subd. 8(b).

We recommend such requests be made in writing and include a brief explanation of the law enforcement purpose for the request. This could be accomplished through email. A file of these requests should be maintained for audit purposes.

RPD BWC Data Classification

RPD has adopted recommendations of the League of Minnesota Cities regarding data classification. These classifications are similar but not identical to the classification requirements for BWC data set forth in Minnesota Statute §13.825, which specifies that such data are private data on individuals or nonpublic data, subject to certain exceptions. While we did not identify any data that were misclassified

as a result, we strongly recommend adopting the statutory BWC data classifications and incorporating this information by reference in RPD's BWC policy.

Royalton Police Department BWC Program and Inventory

RPD currently possesses three (3) Watchguard body-worn cameras, one for each officer. Officers wear the BWC while on-duty and, by policy, are required to activate the BWC "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."

While RPD does not maintain a separate log of BWC deployment or use, Chief Bruyere advised us that because each officer wears a BWC while on duty, the number of BWC units deployed each shift can be determined based on a review of RPD payroll records. BWC use would be determined based on the creation of BWC data.

As of 4/13/2021, RPD maintained 516 GB of BWC data.

RPD BWC Physical, Technological and Procedural Safeguards

Chief Bruyere uploads RPD BWC data from each device at the end of each pay period. At that time, the data are manually copied to an offline, password-protected computer that is secured behind multiple sets of locked doors. Data that are evidentiary in nature are also archived to optical discs (CD/DVD). Officers have access to their data for report writing prior to the biweekly upload. Access thereafter requires both authorization and the provision of physical access by Chief Bruyere.

We recommend employing an external hard drive or other means to create an archive copy of all BWC data as a safeguard against the possibility of data loss due to a failure of the primary storage device.

Enhanced Surveillance Technology

RPD 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 RPD 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.

BWC Policy Violations

Chief Bruyere advised us that there were no violations of the RPD BWC policy resulting in employee disciplinary action during the audit period.

Audit Data Sampling

Rampart selected a random sample of 80 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 initial sample did not locate any retained BWC data. The auditor reviewed these results and determined that the lack of data was attributable to the current 90-day retention schedule, as well as the suspension of the BWC program as of January 1, 2021. The auditor then reviewed a selection of retained BWC videos to verify that this data was accurately documented in RPD records.

Audit Conclusions

In our opinion, the Royalton Police Department's operation of its body-worn camera program during the period of 3/30/2019 – 3/31/2021 is substantially compliant with Minnesota Statutes §13.825 and §626.8473, with the following exceptions:

- All BWC data, including unintentional or test recordings, must be retained for a minimum of 90 days suggesting a change in wording to the policy "To be deleted after 90 days (See policy section VIII-B-5)."
- BWC policy must address disciplinary actions for violations of BWC policy.

We recommend RPD resume use of its BWC program once the recommended policy modifications noted in this report are made.

Daniel Gazelka

Daniel E. Gazelka

Rampart Defense LLC

6/02/2021