Biennial Audit of the Oak Park Heights Police Department Portable Recording System (Body-Worn Cameras) Conducted by LEADS Consulting
Audit Summary Report
Submitted July 23, 2018

Pursuant to Minnesota Statute 13.825, LEADS Consulting conducted an audit of the Portable Recording System (Body Worn Cameras) at the Oak Park Heights Police Department to ensure compliance with state law. The site visit was conducted on March 20, 2018. Police Chief Brian DeRosier who manages the system was the point of contact for auditors. Chief DeRosier serves as the department "Responsible Authority" for data practice issues and also supervises the maintenance of data for the Portable Recording System. The Oak Park Heights Police Department policies regarding "Body Worn Cameras" were collected and reviewed in detail in the weeks following the site visit. A copy of the policy is attached to this audit as appendix A.

Verbal information regarding operations and practices was received from Chief DeRosier. The audit examined the policies and practices of the department in regards to the use and operation of their Portable Recording Systems including the following functions:

1. Portable Recording System Technology
2. Records Maintenance and Data Protection
3. Data Classification
4. Retention and Destruction of Data
5. Data Use and Access to Data by Agency
6. Sharing Data with other Agencies
7. Access to Data by Subjects

Oak Park Heights Police Department Policy

The Oak Park Heights Police Department Policy #4900 regarding their Portable Recording System is specific regarding use and practices. A copy is attached to this report as appendix A.

The Oak Park Heights Portable Recording System Technology

The Oak Park Heights Police Department has been utilizing the "WatchGuard Evidence Library 4 web" Body-Worn Camera System since March of 2016. At the time of the site visit they had four body worn cameras. The system data base had recorded 2057 video events from March 23, 2016 to March 20, 2018. The system recorded 1279 events during the previous year and 290 events during the 90 days prior to the site visit. Each event is coded with an event category upon its creation or in the near future by the officer who initiated the recorded event.

Maintenance of Records and Data Protection

The WatchGuard Evidence Library 4 system used by the Oak Park Heights Police Department maintains detailed records showing the date and time that portable recording system data was collected. The Oak Park Heights Police Department has a dedicated computer server at their police department to house the data and the system is password and user role protected from unauthorized intrusion.

Data Classification

The Oak Park Heights Police Department utilizes the applicable classification of data under Minnesota Statute 13.825. Their department policy makes reference to the Minnesota Data Practices law. Chief DeRosier is knowledgable of the "Portable Recording System" data classifications required under MN statues and he also serves as the "Responsible Authority" under the Data Practices provisions.

The Oak Park Heights Police Department had not had a recording of an incident documenting the discharge of a firearm by a police officer in the course of duty or an incident documenting the use of force by a police officer that resulted in substantial bodily harm. Active criminal investigative data are considered confidential or protected nonpublic.

The department had not had a request from a subject of a video recording to make the data public or to extend the retention period.

The Oak Park Heights Police Department policies and practices regarding data classification are consistent with state statutes.

Retention and Destruction of Data

Minnesota Statute 13.825 Subd. 3 sets out specific minimum data retention requirements for different types of incidents captured by Portable Recording System devices. PRS data that are not active or inactive criminal investigation must be maintained for 90 days. After 90 days the data may be destroyed according to the agency's records retention schedule.

The Oak Park Heights Police Department had not deleted or destroyed any line of duty data at the time of the site visit. The data that is not required to be kept under Minnesota Statutes will be destroyed consistent with the city's retention schedule.

The WatchGuard system allows the officers to create event descriptions that provide guidance as to whether the data has a further investigative purpose or requires longer retention. The department policy states that "all files will be tagged with an ICR number, Officer #, date and time associated with the event". The "Tag List" includes categories such as "1. Officer Information, 2. Warning, 3. Cit/Arrest, 4. Traffic Accident, 5. Public Assist, 6. DOC, 7. Assault, 8. Domestic, 9. Drugs, 10. DUI, 11. EDP, 12. Theft, 13. Alarm, 14. Test. The policy also states that "Officers shall note in their report, all incidents in which the BWC was activated during an arrest, use of force incidents or other evidentiary incidents".

Active criminal investigative data is maintained and destroyed pursuant to MN Statute 13.87 Subd 7 and the department's retention schedule. The department policy also states that destruction "will be done in accordance with current MN data retention duties"

The examination indicates that the Oak Park Heights Police Department is in compliance with the "retention and destruction" of data provisions regarding Portable Recording Systems.

Data Use and Access to Data

The Oak Park Heights Police Department policy states “Officers will be allowed to review recordings prior to making a statement, completing reports and in a serious use of force event. This allows the officer to refresh their memory and provide a more detailed and accurate statement of report.” Officers only have access to their own recordings. The policy also states that “The department reserves the right to limit or restrict viewing of recordings as allowed for investigation and in conformance with data practice law.”

Chief DeRosier has also authorized Sergeants Chris Vierling and Jon Givand to review the videos as necessary for investigation, supervision or training.

The department policy states that “The Chief of Police or their designee will be responsible for data release”.

Auditors examined 5% of the 2057 video data events including each video audit trail to review appropriate use, classification and access. 103 randomly selected video events were reviewed and the audit trail examined for any anomaly. All recordings were made in the line of duty. 25 of the 103 videos had been viewed by the recording officer shortly after their creation consistent with report writing practices. Sergeant Vierling had observed one of the 103 videos and Chief DeRosier had reviewed one. No videos had been watched repeatedly. Four of the video events had been downloaded for court purposes. If this review had revealed any abnormalities the pool of examined video incidents would have been expanded.

The examination revealed that the Oak Park Heights Police Department data use and access to data are in compliance with state law.

Sharing Data with other Law Enforcement Agencies

All requests for sharing of data from other agencies are directed to Chief DeRosier. He states that they have only had three requests from other agencies in the past two years. Two from the Bayport Police and one from Washington County. These requests were incidents in which both agencies were on scene at the same time. The requests included the case number and the reason for the request.

The Oak Park Heights Police Department is in compliance with the “Sharing Among Agencies” provision of state law.

Access to Data by Subjects

The Oak Park Heights Police Department follows MN Data Practice law and provides for release of subject data when requested. Chief DeRosier is the "responsible authority" for those requests but states that at the time of the audit they had not received any requests for Portable Recording System video data.

The Oak Park Heights Police Department is in compliance with the "Access to Data by Subjects" provision of state law.

Audit Conclusion

The Oak Park Heights Police Department has a Portable Recording System policy that reflects MN statute 13.825 and contains significant specific regulations to ensure compliance with the statute. The department's policies and practices are consistent with state law. The data system is properly maintained and professionally monitored by Chief Brian DeRosier.

LEADS Consulting finds the Oak Park Heights Police Department "Portable Recording System" policies and practices to be in compliance with the provisions referenced in Minnesota Statute 13.825 Subd. 9, Biennial Audit.

Bob Fletcher
Director
LEADS Consulting
Law Enforcement Audit and Data Services
www.leads50.com

Oak Park Heights Police Department Policy Manual

Re: Body worn Cameras

Effective Date: 10-01-2015

Revision Dates: 07-20-2016

Policy #4900

The Oak Park Heights Police Department strives to provide professional law enforcement services to the citizens of Oak Park Heights. The use of technology in today's society has become the norm and is often times an expectation. Body Worn Cameras are a readily available technology and provide a platform for recording and documentation of evidence and details of an incident that officers respond to. This information can allow officers to complete more accurate reports, document evidence, better court testimony, protection of officers against conduct complaints, provide documentation for investigation of citizen complaints. The BWC is an extension of technology already in place and used by the department with In Car Video systems.

This policy is intended to provide officers with the instructions on when and how to use body-worn cameras (BWC) so that officers may reliably record their contacts with the public.

This policy is written with the understanding BWC's are another tool for officers and the department to capture the conduct of persons and other evidentiary elements during an incident. This policy reflects a balance between the desire to establish the exacting and detailed requirements of police work and the reality that officers face attending to their duties with the safety of all concerned, often in circumstances that are tense, uncertain, and rapidly evolving. The devices are not without limitations and some of these limitations deserve special notation as part of this policy. These limitations have been documented in the industry from past recorded incidents and testing. When video captured is analyzed after the fact and without the immediacy, stress of the event, and many other factors that may impact an officer's perception of the situation it may not evoke similar responses in the viewer.

1. A camera mounted to a person does not follow the eyes of the officer, or see as the officer sees. Cameras may see in better or worse detail than the officer, the camera may be limited in peripheral view, and other anomalies associated with video and photography.
2. Some tactile clues cannot be recorded visually. Officers may feel a suspect tense up and or start to pull away while being arrested. A suspect bringing his hands up may appear to be surrendering on camera but that may not be perceived by an officer on scene who is taking into consideration all elements at hand and may actually feel and appear as if the subject is preparing to fight the officer.
3. Camera speed is different than real life observation. Cameras may miss some details or other details may be seen by the camera that could not or were not seen by the officer. Lighting, camera recording speed, and other circumstances may affect what is recorded or not recorded.

4. Cameras record in 2D. Depth perception is perceived by human eye. Multiple cameras at different angles may capture an incident in what appears to be vastly different details or circumstances. A single camera may present images that appear to be farther away or closer than they really are.
5. Time stamping may or may not be accurate or coincide with other data.
6. Camera footage can encourage second guessing of officer perceptions and impressions of an event by uninformed persons while in calm and comfortable conditions and not being subjected to the event at real life speeds that the officer involved in the incident was subjected to.
7. Not all audio may be captured. The microphone may be covered, the sound may be too loud, soft, or of a pitch that is not captured.

POLICY

It is the policy of this department that officers should attempt to activate the BWC when such use is appropriate to the performance of his or her official duties and where recordings are consistent with policy and law.

This policy does not govern the use of surreptitious recording used in authorized undercover operations.

The Chief of Police or their designee may supersede this policy by providing specific instructions for the use of BWC's to individual officers, or providing instruction pertaining to certain events or classes of events.

Nothing in this policy prohibits the use of a recording or lack of recording by an officer, from discipline in conformance with department established disciplinary guidelines. Recordings may be accessed by supervisory or other specifically assigned persons for the purpose of review or investigation of a complaint or concern of officer misconduct or performance.

OBJECTIVES

1. BWC's record details of an event and serve to aid the officer in recalling details of an event and provide evidence in court.
2. The recordings enhance the agency's ability to review incidents, officer and subject interactions, and document evidence for court or resolution of complaints.
3. BWC's may also be useful in documenting crime and accident scenes or other events such as confiscation of property, documentation of evidence or contraband at a scene.

HOW and WHEN CAMERAS SHOULD BE USED

1. Officers should activate BWC's to record all contacts with adversarial citizens in the performance of their duties or contacts and events that the officer would reasonably expect an arrest, citation, need for documentation of physical evidence, documentation of suspect actions and statements, use of force, witness statements or victim statements especially those that show emotion or state of mind at time of incident. "**Adversarial Defined** – a person or encounter that becomes confrontational, during which at least one person expresses anger, resentment, or hostility toward another, 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 their own are deemed adversarial."

2. If reasonable and not a safety or tactical consideration the officer will inform subjects that directly and clearly request to know if they are being recorded, and if the officer is in a location the subject would otherwise have an expectation of privacy if the officer where not there. This would include inside a private residence.
3. Officers should record the entire event until the officer has cleared the scene, subject has been turned over to jail staff, or the officer is otherwise not engaging persons. Lapses in recordings will be documented in the officer's report. Suspects secured in a squad with the in car video system running are considered to be recorded for the purpose of this policy. Dual recording with BWC and In Car Video is not required -i.e. during transport, while waiting and performing vehicle tow operations, etc.
4. Supervisory personnel within the OPH PD may, after taking charge of incident, direct personnel to discontinue ongoing recordings when further recording is unlikely to capture further evidentiary information.
5. Audio should only be turned off temporarily if the officer is in need of confidentially conferring with another officer, anon complainant, or other documented situation. Officers will document in their report as to why there were any lapses in recording. Officers should momentarily block the functions of the camera to capture audio or video in these situations if possible rather then turning the BWC off to avoid creating multiple files for an event.
6. Officers will follow other operating procedures separately outlined in procedure manual about marking video clips, storage, equipment handling, and other operational issues respective of the equipment.
7. Officers are not required to activate their camera when it would be unsafe, impossible, or impractical; however are required to notify a supervisor as soon as reasonable after the event of an incident that was not recorded that would normally have been required to be recorded.

USE and OPERATION

1. BWC's are issued primarily to uniformed officers, however plain clothes officers or investigators may also use BWC's.
2. Only BWC's issued and approved by this department will be worn by Officers. Officers assigned to a SWAT team will be considered to have been issued an approved device if issued or assigned by SWAT command during SWAT operations.
3. BWC's are property of the department and all data captured by the device is property of the department.
4. Personnel will complete training prior to the use of BWC's. Personnel will be retrained or provided documentation if operation of the BWC's is changed by update or change of equipment.
5. BWC's will be the responsibility of the officer wearing a BWC to care for and ensure proper operation of the unit. Equipment malfunctions shall be brought to the attention of

administrative personnel or other assigned person. Officers will use equipment malfunction reports describing the malfunction and circumstances surrounding the cause if known.

6. Officers will test BWC's at the start of and at the conclusion of each shift.
7. Officers will not edit, alter, erase, duplicate, share, or otherwise distribute in any manner BWC recordings without prior approval of the Chief of Police or Chief's designee.
8. Officers should inform supervisors of recordings that may be of training value, community outreach, or other value to the department other than those specifically saved for evidentiary value.
9. Officers will be allowed to review recordings prior to providing a statement, completing reports, and in a serious use of force event. This allows the officer to refresh their memory and provide a more detailed and accurate statement or report.
10. The department does reserve the right to limit or restrict viewing of recordings as allowed for investigation and in conformance with data practice law.
11. Requests for deletion of recordings (e.g., in the event of mistakenly recording a personal event) shall be submitted to the Chief of Police or their designee. The CLEO or their designee will review the request and determine if the event will be deleted or retained. All requests approved or denied will be kept on file.
12. Officers shall note in their report, all incidents in which a BWC was activated during arrest, use of force incidents, or other evidentiary incidents.
13. As allowable by type of equipment being used, all files will be "tagged" with the ICR number, Officer #, Date, and Time associated with the event. Any event not having an ICR number associated will be identified by Officer #, Date, Time.

RESTRICTIONS and PROHIBITED USE

1. BWC's should only be used to document law enforcement related events as previously described, or events in the public view that may be of public outreach value or other noncriminal purposes. **Our intent is not documenting daily activity of citizens or employees not related to law enforcement purposes or activity which is not of other value as a specific police related incident.**
2. BWC shall not generally be used to record other police personnel involved in routine non-enforcement daily activity without approval of the CLEO.
3. BWC will not be used in the police department outside of the interview rooms, unless there is a specific incident inside the department requiring police response, or for training purposes.
4. BWC shall not generally be used to record interaction with undercover officers or confidential informants.
5. BWC's should not be used during breaks or other personal activity of the officer.
6. BWC's should not be used in an area or location open to the public, or a private location, having other persons not involved or unaware of the call for service, who would normally have a higher reasonable expectation of privacy "i.e locker room of fitness club", unless the officer is

specifically there for a reported law enforcement activity and the officer feels the need to record the situation outweighs the consideration for privacy.

7. A recording capturing data including but not limited to; victims of child abuse, nudity, informants, mandated reporters, or video that is clearly offensive to the common sensibilities, the officer shall notify the Chief of Police of the recording so it may be flagged and only specific articulated viewing for evidence allowed or it may be destroyed if not needed for evidence.
8. Body worn cameras will not be used in hospital or medical settings, unless specifically responding to a request for police and the officer feels recording the situation provides evidentiary value. This will be documented by the officer in their report
9. Medical response / assistance calls will not normally be recorded unless it is believed the recording would provide evidentiary value.
10. BWC should not be used for routine contact with citizens such as lockouts, public assistance, questions or other generalized incidents or contacts.
11. Officers responding to persons with possible mental health crisis that may require the officer to use force or provide other evidentiary value should record the event, but not merely to record symptoms or behavior.
12. Officers will not record interactions with Magistrates or other Court proceeding, unless responding to an incident in the courts.
13. Officers will not intentionally block the audio or visual functions of the BWC to defeat the purpose of this policy. Officers may however momentarily block the functions when needed to confer with other officers or other administrative actions away from contact with citizens in lieu of stopping and starting the recording creating multiple files documenting such actions in their report.

STORAGE

All video will be stored on secure computer server located within the physically secured area of the police department in conformance with all established FBI security rules for other data. Access to the server is limited ONLY to those personnel specifically authorized by the department and trained on use and access of BWC and data. Each user will have specifically assigned user access using user name and password. Officers unless otherwise assigned by the Chief of Police will only have access to video created by themselves.

1. All files shall be securely downloaded periodically during the officer's shift if needed to create additional space and no later than the end of the officer's daily shift.
2. Officers will be able to review video captured by them at any reasonable time. A log will be maintained and officers reviewing a recording after the initial review to complete their report will log this viewing. Personnel are prohibited from accessing BWC data for nonbusiness reasons or from sharing or disseminating the data for non-law enforcement purposes unless specifically authorized by the Chief of Police.

3. All images and data are exclusive property of this department. Accessing, copying, or releasing of files shall be by designated personnel only. Release will be approved by the Chief of Police or their designee only.
4. Files will be securely stored in accordance with state records retention rule for purposes of evidentiary value, investigation, training, department use, or community outreach use.
5. Files kept as evidence will be kept secure until criminal prosecution and appeal processes have been completed, or as required for evidentiary retention.
6. Investigative files will be kept as needed until the investigation is complete without prosecution or there is no longer reasonable expectation of solving the case and the statute of limitations has expired, then the file may be flagged for 90 day destruction.
7. BWC capturing events involving death or great bodily harm will be kept perpetually.
8. Files not being retained for evidence, investigation, or departmental use should be destroyed after 90 days. This destruction will normally be completed once every 90 days. This provides time for complaints or other concerns to be brought forward before the data is destroyed that may provide details of the event in question. Prior to destruction, the Chief of Police will be provided a listing of the number of recordings being destroyed, date of destruction, and the date range of the recordings (i.e. 25 recordings between the dates of Jan 1, 2015 to March 31, 2015 erased on 04-01-2015. This record will be maintained.
9. If not previously addressed or as required, recordings will be processed under current MGDPA rules or temporary ruling by the MN Commissioner of Administration or another charged with those duties.
10. Destruction unless previously addressed will be done in accordance with current MN data retention rules.
11. Nothing in this policy limits or prohibits the use of BWC data as evidence of misconduct or as a basis for discipline by the department.

Release of Video / Data

12. All recordings will be released as required by MN Data practice or other law.
13. Files part of an incident resulting in criminal prosecution will be considered to be under investigation until the disposition of the case and the period of appeal having lapsed.
14. Other than as required by law for subjects of the data or in conformance with criminal prosecution disclosure rules; all requests for video / data that may be released under MGDPA will be charged actual costs of employee time for retrieval, redaction review and redaction, processing, and data storage media.
15. The Chief of Police or their designee will be responsible for data release.
16. Requestors will provide ALL the expected cost for the data processing and copying requested at the time the request is made. Payment will be made prior to the processing or receiving the data. Any overage will be returned by city finance department in accordance with their processing rules.