Policy Manual

# Surveillance Use Policy - Body Worn Cameras

#### 1300.1 **PURPOSE**

This Surveillance Use Policy is issued in compliance with BMC 2.99, and incorporates language from the Berkeley Police Department Body Worn Camera Policy #425 and adds elements as required by BMC 2.99.

The Berkeley Police Department recognizes that video recording of contacts between department personnel and the public provides an objective record of these events, and that the use of a recording system complements field personnel in the performance of their duties by providing a video record of enforcement and investigative field contacts, which can enhance criminal prosecutions, limit civil liability, increase transparency, and enhance professionalism in the delivery of police services to the community. A video recording of an event or contact also enables the delivery of timely, relevant, and appropriate training to maximize safety for both community members and BPD personnel. (Ref. policy 425.2).

#### 1300.2 **AUTHORIZED USE**

This policy is not intended to describe every possible situation in which the BWC should be used. Members shall activate the BWC as required by this policy in (a)-(f) below, and may activate the BWC at any time the member believes it would be appropriate or valuable to record an incident within the limits of privacy described herein.

The 8WC shall be activated in any of the following situations:

- All in-person enforcement and investigative contacts including pedestrian stops and field interview (FI) situations.
- Traffic stops including, but not limited to, traffic violations, stranded motorist assistance and all crime interdiction stops.
- Self-initiated field contacts in which a member would normally notify the Communications Center.
- Any search activity, including the service of search or arrest warrants; probation, parole, or consent searches where the member is seeking evidence of an offense, or conducting a safety sweep or community caretaking sweep of the premises. Once a location has been secured and the member is not interacting with detainees or arrestees, the member may mute their BWC when conducting a search for evidence.
- Any other contact that the member determines has become adversarial after the initial contact in a situation where the member would not otherwise activate BWC recording.
- **(f)** Transporting any detained or arrested person and where a member facilitates entry into or out of a vehicle, or any time the member expects to have physical contact with that person.

At no time is a member expected to jeopardize his or her safety in order to activate a BWC. The BWC should be activated by members in anticipation of situations described above, and in any unanticipated, rapidly unfolding situation where activation becomes required, as soon as the member can do so safely.

Members should activate their BWC when conducting custodial interviews unless there are other recording devices being used. Members shall document and explain in their report the reason for not recording custodial interviews, should a BWC be de-activated while conducting a custodial interview or interrogation. (Ref. policy 425.7)

## 1300.2.1 PROHIBITED USE

Members are prohibited from using a department-issued BWC for personal use and are prohibited from making personal copies of recordings created while on duty or while acting in their official capacity.

Members are prohibited from retaining BWC recordings. Members shall not duplicate or distribute such recordings, except for department business purposes. All such recordings shall be retained at the Department.

Recordings shall not be used by any member for the purpose of embarrassment, intimidation or ridicule. (Ref. policy 425.13)

#### 1300.3 DATA COLLECTION

BWC use is limited to enforcement and investigative activities involving members of the public. The BWC recordings will capture video and audio evidence for use in criminal investigations, administrative reviews, training, civil litigation, and other proceedings protected by confidentiality laws and department policy. Improper use or release of BWC recordings may compromise ongoing criminal and administrative investigations or violate the privacy rights of those recorded and is prohibited. (Ref. policy 425.3)

#### 1300.4 DATA ACCESS

Members are authorized to review their own BWC video files at any time in furtherance of official business. Such official business includes, but is not limited to, preparing written reports, prior to or while providing testimony in a case or being deposed. Members may review recordings as an evidentiary resource, except as stated in subsection 1300.4.1 below. Members shall not retain personal copies of recordings. Members shall not use the fact that a recording was made as a reason to write a less detailed report. (Ref. policy 425.17)

# 1300.4.1 OFFICER INVOLVED INCIDENTS RESULTING IN GRAVE BODILY INJURY OR DEATH

(a) In the event of a critical incident that results in grave bodily injury or death, including an officer-involved shooting or an in-custody death, the BWC of the involved member(s) shall be taken from him or her and secured by a supervisor, commander, or appropriate investigator, as necessary. The involved member(s) shall not access or obtain their footage

(

of the incident until such time as the criminal investigator(s) have reviewed the video files. It will be the responsibility of the investigation team's supervisor to coordinate with the involved member's supervisor to obtain footage of the incident on behalf of the member.

- (b) Personnel uploading secured BWC video files shall not view the files unless authorized.
- (c) No member involved in a critical incident may view any video recordings prior to an interview by the appropriate criminal investigative unit, and receiving command approval.
- (d) Prior to the conclusion of the criminal interview process, the involved member and/ or the member's representative will have an opportunity to review the member's recording(s). The involved member may choose to provide additional information to supplement his or her statement by providing a supplemental statement or separate supplemental document. In no case shall a member alter a report made prior to reviewing the recording.
- (e) The Department acknowledges that recordings taken during critical incidents obtained from BWCs do not necessarily reflect the full extent of the nature of the event or the experience, analysis, training, threat assessment or state of mind of the individual officers(s) in a given incident. Moreover, the recordings, especially video, have limitations and may depict events differently than the events recalled by the involved officer. Specifically, it is understood that the recording device will capture information that may not have been heard and/or observed by the involved officer and that officers may see and hear events that are not captured by the camera.

Officers who are involved in any critical incident where video recordings exist depicting the involved officer, either as a subject officer or witness, shall be provided the following admonishment to the initial interview or submission of the initial written report:

"In this case, there is video evidence that you will have an opportunity to view. Video evidence has limitations and may depict the events differently than you recall, and may not depict—all of the events as seen or heard by you. Video has a limited field of view and may not capture events normally seen by the human eye. The "frame rate" of video may limit the camera's ability to capture movements normally seen by the human eye. Lighting as seen on the video may be different than what is seen by the human eye. Videos are a two-dimensional medium and may not capture depth, distance or positional orientation as well as the human eye. Remember, the video evidence is intended to assist your memory and ensure that your statement explains your state of mind at the time of the incident." (Ref. policy 425.17.1)

## 1300.4.2 SUPERVISORY REVIEW

With the exception of section 1300.4.1 above, supervisors are authorized to review relevant recordings any time they are reviewing and approving case reports from their subordinates, (Ref. policy 425.17.2)

## 1300.4.3 INVESTIGATORY REVIEW

Supervisors are authorized to review relevant recordings any time they are investigating alleged misconduct or reports of meritorious conduct, or whenever such recordings support review of the member's performance. (Ref. policy 425.17.3)

- (a) Recorded files may also be reviewed:
  - Upon approval by a supervisor, by any member of the Department who is participating
    in conduct of an official investigation, such as a personnel complaint, an administrative
    investigation or a criminal investigation.
  - Pursuant to lawful process or by court or District Attorney personnel who are otherwise authorized to review evidence in a related case.
  - By personnel assigned to investigatory units who are authorized to view any 8WC video file associated to their active investigations, unless otherwise prohibited by policy.
  - Upon approval by the Chief of Police, Internal Affairs investigators may review BWC video with a complainant.
- (b) Investigators conducting criminal or internal investigations shall:
  - Advise the coordinator to restrict access to the BWC file in criminal or internal investigations, as necessary.
  - Review the file to determine whether the BWC file is of evidentiary value and process it in accordance with established protocols.
  - Notify the coordinator to remove the access restriction when the criminal/internal investigation is closed.

#### 1300.4.4 TEACHING OR LEARNING TOOL

BWC files may also be reviewed by training staff regarding specific incidents where such files may serve as an internal fearning or teaching tool. In the event that videos are intended to be used for training purposes, the involved officer(s) will first be consulted. If he/she objects to the use of the video, such objection shall be submitted to the person in charge of training who shall weigh the value of the video for training against the officer(s) objections and basis for the objection. Should the person in charge of training refuse to grant the request of the involved officer(s), the matter shall be heard by the Chief of Police, or his/her designee, prior to utilizing the video. (Ref. policy 425.17.4)

#### 1300.4.5 COB CIVIL CLAIMS AND LAWSUITS

BWC recordings may be reviewed and used by City of Berkeley defense counsel for the purposes of defending the city in civil claims and tawsuits, with the authorization of the Chief of Police, or his/her designee. (Ref. policy 425.17.5)

## 1300.5 DATA PROTECTION

To assist with identifying and preserving data and recordings, members shall tag and download recordings in accordance with procedure, and document the existence of the recording in the related case report. Transfers must occur at the end of the member's shift, and any time the member is aware that the storage capacity of the BWC is nearing its limit. In circumstances when the officer cannot complete this task, the officer's supervisor shall immediately take custody of the BWC and be responsible for uploading the data. Officers shall tag each file with the appropriate case/incident number, provide a descriptive title, and select an appropriate category for each

recording, using the Axon View app or via the Evidence.com site.

Members are prohibited from intentionally erasing, altering, reusing, modifying or tampering with original audio video recordings. (Ref. policy 425.14)

#### 1300.6 CIVIL LIBERTIES AND RIGHTS PROTECTION:

The Berkeley Police Department is dedicated to the most efficient utilization of its resources and services in its public safety endeavors. The Berkeley Police Department recognizes the need to protect its ownership and control over shared information and to protect the privacy and civil liberties of the public, in accordance with federal and state law. The procedures described within this policy (Data Access, Data Protection, Data Retention, Public Access and Third Party Data Sharing) protect against the unauthorized use of BWC data. These policies will ensure the data is not used in a way that would violate or infringe upon anyone's civil rights and/or liberties, including but not limited to potentially disparate or adverse impacts on any communities or groups.

#### 1300.7 DATA RETENTION

The Department shall retain all recordings for a minimum of 60 days. Incidents involving consensual contacts, and aid to citizens will be retained for six months; and cold reports will be retained for one year. Recordings of incidents involving use of force by a police officer, detentions, arrests, or recordings relevant to a formal or informal complaint shall be retained for a minimum of two years and one month. Recordings relating to court cases and personnel complaints that are being adjudicated will be manually deleted at the same time other evidence associated with the case is purged in line with the Department's evidence retention policy. Any recordings related to administrative or civil proceedings shall be maintained until such matter is fully adjudicated, at which time it shall be deleted in line with the Department's evidence retention policy, and any applicable orders from the court.

Recordings created by equipment testing or accidental activation may be deleted after 60 days. (Ref. policy 425.15)

## 1300.8 PUBLIC ACCESS

Access to recorded files will be granted for the purposes of review in response to a public records request, as permitted under Government Code § 6254(f) and BPD General Order R-23 (Release of Public Records and Information). General Order R-23 does not authorize release of investigative files or documents that would constitute an unwarranted invasion of privacy. Circumstances where this might arise in video include footage taken inside a home, a medical facility, the scene of a medical emergency, or where an individual recorded has a "reasonable expectation of privacy."

Access to recorded files will be granted for the purposes of review to media personnel or the general public with permission of the Chief of Police, or his/her designee, subject to General Order R-23 and privacy protections indicated in this policy. (Ref. policy 425,18)

#### 1300.9 THIRD-PARTY DATA-SHARING

#### 1300.9.1 CITY ATTORNEY

All recordings should be reviewed by the Custodian of Records and the City Attorney's Office prior to public release, see General Order R-23 (Release of Public Records and Information).

In the event that the Police Department or City Department intends to release or publish for any purpose video recordings where officers are captured on video or the video depicts actions taken by them in the course of the performance of their official duties, those officers shall be given written notice of the intention to release or publish said video at least 48 hours prior to such release.

BPD may, without prior notice to involved officers, share video footage with law enforcement, national security, military, or other government agencies outside of Berkeley, when there is reasonable suspicion that criminal activity has occurred or is about to occur. (Ref. policy 425.18)

## 1300.9.2 POLICE REVIEW COMMISSION (PRC)

Access to recorded files will be granted for the purposes of review to the Police Review Commission Officer and/or Investigator investigating a specific complaint where BWC evidence files are available, and are not part of any ongoing criminal investigation. (Ref. policy 425.18.1)

- (a) The PRC Officer and PRC investigator will be provided user account access to evidence files through the evidence management system for their use during a complaint investigation and to facilitate viewing by 8oard of Inquiry members during a Board of Inquiry.
- (b) The PRC Officer and PRC investigator shall not make or create a copy of any evidence file, nor make or allow to be made any audio or video recording of any evidence file while it is being streamed and viewed from the evidence management system.
- (c) The PRC Officer and PRC Investigator shall not allow any unauthorized individuals to view or access evidence files.
- (d) The evidence management system associates an audit trail record with each evidence file, thereby logging the date, time, user, activity, and client IP address occurring during each evidence file access.
- (e) The evidence management system shall only be accessed on City premises.
- (f) The Department retains custody and control of the recordings, and content of the video will be subject to applicable legal standards including, but not limited to the confidentiality requirements of the Public Safety Officers' Procedural Bill of Rights, (Government Code § 3300, et seq., Penal Code § 832.7, and the California Public Records Act; Government Code § 6250, et seq.)

#### 1300.10 TRAINING

Training for the operation of BWC's shall be provided by BPD personnel. All BPD personnel who use BWC's shall be provided a copy of this Surveillance Use Policy.

#### 1300.11 AUDITING AND OVERSIGHT

Division Captains for divisions utilizing BWC's shall ensure compliance with this Surveillance Use Policy.

#### 1300.12 MAINTENANCE

The BWC system will be maintained by the Applications Programmer Analyst and assigned Department of Information and Technology (IT) staff.

The Chief of Police, or his/her designee shall appoint a member of the Department to coordinate the use and maintenance of BWCs and the storage of recordings, including (Penal Code § 832.18) (Ref policy 425.4):

- (a) Establishing a system for uploading, storing and security of recordings.
- (b) Designating persons responsible for uploading recorded data.
- (c) Establishing a maintenance system to ensure availability of BWCs.
- (d) Establishing a system for tagging and categorizing data according to the type of incident captured.
- (e) Establishing a system to prevent tampering, deleting and copying recordings and ensure chain of custody integrity.
- (f) Working with the City Attorney's office to ensure an appropriate retention schedule is being applied to recordings and associated documentation.
- (g) Maintaining an audit trail record for all access to evidence files, wherein access information for each evidence file is togged through use of a secure log-in system. The Department's storage system associates an audit trail record with each evidence file, thereby logging the date, time, user name, activity and client IP address occurring during each evidence file access.
- (h) All recordings made by members acting in their official capacity shall remain the property of the Department. Subject to the provisions of this Policy, members shall have no expectation of privacy or ownership interest in the content of these recordings.



## BODY WORN CAMERAS (BWCs)

#### A. DESCRIPTION

The 8WC system consists of four main components: The camera, the docking station, and the Digital Information Management System (DIMS) and smartphone applications.

The first component, the Axon camera, is a system which incorporates an audio and video recording device. It is designed to record events in real time for secure storage, retrieval, and analysis. The camera is to be attached to an officer's uniform and is powered by an internal rechargeable battery. The camera features low-light performance, full-shift battery life, a capture rate of 30 frames per second with no dropped frames, HD video, pre-event buffering, multi-camera playback, and the ability to automatically categorize video using the police department's computer aided dispatch system. An officer can start and stop recording by pressing a button on the front of the camera. The camera does not contain a screen for footage review.



The second component of the system is the docking station. Once the Axon camera is placed in the docking station it recharges the camera's battery. The dock also triggers the uploading of data from the camera to a cloud based Digital Information Management System (DIMS) called Evidence.com. The dock does not directly provide functionality to view, modify or delete video data stored on Axon cameras.



The third component is the Digital Information Management System called Evidence.com. Evidence.com streamlines data management and sharing on one secure platform. The evidence management system is comprehensive, secure, and intuitive to use. The DIMS is located in a cloud-based data center for security, scalability, and ease of administration. Users can add

metadata to existing videos such as associated case numbers, incident type, incident dispositions, etc. to make the videos easier to find. However, the videos themselves cannot be altered by the user.

The fourth component of the system to be utilized are two Axon mobile applications, which allow officers to collect and review evidence in the field and more effectively use their BWCs. The applications use secure Bluetooth and Wi-Fi technology to access the BWC systems and footage. These applications are compliant with US Department of Justice evidentiary standards, meaning that they are both secure and are set up in a way that prohibits the altering or destruction of evidence. The applications are called Axon View and Axon Capture. Axon View allows users to change their camera settings, view live video, and review and tag recorded videos while they are stored on the BWC. Recorded videos remain in the BWC's memory, and cannon be manipulated or deleted. Axon Capture allows officers to use their city-issued smartphone's camera and microphone to take photographs, and record audio and video, and to upload this data directly to Evidence.com. These applications do not allow users to alter, manipulate, or edit any of the footage recorded by the BWC. These applications use secure technology to add value and efficiency to the BWC program.

#### B. PURPOSE

The primary objective of the BWC system is to document officer contacts, arrests, and critical incidents. Video footage collected by the BWCs will be used as evidence in both criminal and administrative investigations. Video footage not relevant to any investigation will be discarded after a defined retention period.

In instances where the officer might be expected to take law enforcement action of any kind, the officer is expected to record the encounter for the benefit of both the officer and the member of the public.

- The 8WC shall be activated in any of the following situations:
  - All in-person enforcement and investigative contacts including pedestrian stops and field interview (FI) situations.
  - ii. Traffic stops including, but not limited to, traffic violations, stranded motorist assistance and all crime interdiction stops.
  - iii. Self-initiated field contacts in which a member would normally notify the Communications Center.
  - iv. Any search activity, including the service of search or arrest warrants; probation, parole, or consent searches where the member is seeking evidence of an offense, or conducting a safety sweep or community caretaking sweep of the premises. Once a location has been secured and the member is not interacting with detainees or arrestees, the member may mute their BWC when conducting a search for evidence.

- v. Any other contact that the member determines has become adversarial after the initial contact in a situation where the member would not otherwise activate 8WC recording.
- vi. Transporting any detained or arrested person and where a member facilitates entry into or out of a vehicle, or any time the member expects to have physical contact with that person.

At no time is an officer expected to jeopardize his or her safety in order to activate a BWC. The BWC should be activated in anticipation of situations described above, and in any unanticipated, rapidly unfolding situation where activation becomes required, as soon as the user can do so safely.

Officers should activate their BWC when conducting custodial interviews unless there are other recording devices being used. Officers shall document and explain in their report the reason for not recording custodial interviews, should a BWC be de-activated while conducting a custodial interview or interrogation.

## 2. Prohibited uses of the BWC system include:

- Officers shall not surreptitiously record another department member without a court order unless lawfully authorized by the Chief of Police, or his/her designee.
- ii. Officers are prohibited from using a department-issued 8WC for personal use and are prohibited from making personal copies of recordings created while on duty or while acting in their official capacity.
- iii. Officers are prohibited from retaining BWC recordings.
- Officers shall not duplicate or distribute such recordings, except for department business purposes.

#### C. LOCATION

Officers may use BWCs anywhere where officers have jurisdiction to operate as sworn officers, in accordance with BPD policy #425.

## D. IMPACT

With the introduction of BWCs, officers record all enforcement contacts with the public. To that end, an officer could find themselves engaged in their lawful duties in both public and private areas. Additionally, due to the nature of law enforcement work, an officer may be required to engage in sensitive conversations with individuals of all ages, including children.

The right to maintain someone's anonymity versus the need to gain information to maintain public safety is of paramount concern. The Department recognizes that all people have a right to privacy and is committed to protecting and safeguarding civil rights by adhering to the

strictest requirements of both state and federal law concerning release of audio/video recordings.

#### E. MITIGATION

In order to minimize violations of privacy, BWC policy provides that:

- Officers should record any incident they feel would be appropriate or valuable to document. The BWC policy shall require officers to activate the BWC under the criteria listed above.
- 4. Officers should not activate the BWC and/or use caution when entering a public locker room, changing room, restroom, doctor's or attorney's office, or other place where individuals unrelated to the investigation are present and would have a heightened expectation of privacy unless the officer is investigating criminal activity or responding to a call for service.
- 5. 8WC use is limited to enforcement and investigative activates involving members of the public. The BWC recordings will capture video and audio evidence for use in criminal investigations, administrative reviews, training, civil litigation, and other proceedings protected by confidentiality laws and department policy.
- BWC footage will be retained or released in accordance with applicable state and federal law. Criminal defendants will have access to relevant BWC footage via the court discovery process.
- Officers are prohibited from retaining BWC recordings, Officers shall not duplicate or distribute such recordings, except for department business purposes. All such recordings shall be retained at the Department.
- 8. Officers are prohibited from intentionally erasing, altering, reusing, modifying or tampering with original audio video recordings. Officers may request restriction and subsequent deletion of an accidental recording according to the BWC policy.
- 9. Access to recorded files will be granted for the purposes of review in response to a public records request, as permitted by law and department policy. Department policy does not authorize release of investigative files or documents that would constitute an unwarranted invasions of privacy. Circumstances where this might arise in video include footage taken inside a home, a medical facility, the scene of a medical emergency, or where an individual recorded has a "reasonable expectation of privacy

#### F. DATA TYPES AND SOURCES

BWC use is limited to enforcement and investigative activities involving members of the public. The BWC recordings will capture video and audio evidence for use in criminal investigations, administrative reviews, training, civil litigations, and other proceedings protected by confidentiality laws and department policy.

The BWC collects video and audio recordings of events occurring in the user's presence. As each video is created, the system automatically stamps the video with the current date/time and the camera user's identity. The user has the option to add metadata manually to existing recordings after they are created. Such metadata may include but is not limited to:

- 1. Category of contact (from Department's defined list)
- 2. Disposition of contact (arrest, citation, etc.)
- 3. Associated case number

#### G. DATA SECURITY

To assist with identifying and preserving data and recordings, members shall tag and download recordings in accordance with procedure, and document the existence of the recording in the related case report. Transfers must occur at the end of the member's shift, and any time the member is aware that the storage capacity of the BWC is nearing its limit. In circumstances when the officer cannot complete this task, the officer's supervisor shall immediately take custody of the BWC and be responsible for uploading the data. Officers shall tag each file with the appropriate case/incident number, provide a descriptive title, and select an appropriate category for each recording, using the Axon View app or via the Evidence.com site.

Members are prohibited from intentionally erasing, altering, reusing, modifying or tampering with original audio video recordings.

Improper use or release of BWC recordings may compromise ongoing criminal and administrative investigations or violate the privacy rights of those recorded and is prohibited. The Chief of Police, or his/her designee shall appoint a member of the Department to coordinate the use and maintenance of BWCs and the storage of recordings, including (Penal Code Section 832.18) (Ref. policy 425.14):

- Establishing a system for uploading, storing and security of recordings.
- 2. Designating persons responsible for uploading recorded data.
- 3. Establishing a maintenance system to ensure availability of BWCs.
- 4. Establishing a system for tagging and categorizing data according to the type of incident captured.
- Establishing a system to prevent tampering, deleting and copying recordings and ensure chain of custody integrity.
- Working with the City Attorney's office to ensure an appropriate retention schedule is being applied to recordings and associated documentation.
- 7. Maintaining an audit trail record for all access to evidence files, wherein access information for each evidence file is logged through use of a secure log-in system. The Department's storage system associates an audit trail record with each evidence file,

thereby logging the date, time, user name, activity and client IP address occurring during each evidence file access.

(

(

#### H. FISCAL COST

In 2017, the Berkeley City Council approved a resolution authorizing a contract between 8PD and Axon. Axon was chosen after a competitive Request for Proposal (RFP) process. The contract will not exceed \$1,218,103 and includes the cost of 200 body worn cameras, charging stations, accessories, software licenses, training and unlimited storage for five years. The purchase also includes replacement cameras and charging stations during the third and fifth year of the contract.

There will be an annual cost of approximately \$250,000 to the police department's budget for a staff person to administer the body worn camera program beginning in FY 2019.

#### I. THIRD PARTY DEPENDENCE AND ACCESS

All BWC data will be uploaded and stored on Axon Cloud Services, Evidence.com. Axon complies with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States (collectively, "Privacy Shield"). Axon has certified to the U.S. Department of Commerce that it adheres to the Privacy Shield Principles.

#### J. ALTERNATIVES

Officers rely primarily on traditional policing techniques to gather evidence related to criminal investigations such as speaking to witnesses and suspects, gathering information from observations, and using standard data aggregation systems. These methods will continue to be employed as primary investigative tools that will be supplemented by use of BWCs to document police activity.

BWC technology provides video and audio documentation of policing activity in addition to the oral and written statements of officers, victims, and witnesses. Alternatives to the use of BWCs would be vehicle-based cameras and/or not utilizing BWCs. However, BPD sees the use of BWCs as an integral strategy to strengthen police transparency, prevent and resolve complaints against the police by civilians, document police-public interaction, and promote the perceived legitimacy and sense of procedural justice that communities have about their departments. There is a broad consensus – among community leaders, the ACLU, the Department of Justice, the Berkeley Police Department, and elected officials – that body-worn cameras can be an important tool for improving the high-quality public service expected of police officers.

## K. EXPERIENCE OF OTHER ENTITIES

Numerous police agencies have adopted BWCs as a tool to help combat crime, to reduce citizen complaints and to reduce use of force situations. Many departments have developed their own usage policies which may include standards for required officer use, supervisory review, storage and data retention standards, and internal and public access.

A report for the U.S. Bureau of Justice Administration, <a href="https://www.b/a.gov/owc/pgfs/14-205-Report-8007\_WQRN\_CAMERAS.pdf-pages 6-8">https://www.b/a.gov/owc/pgfs/14-205-Report-8007\_WQRN\_CAMERAS.pdf-pages 6-8</a>, cites a 2013 Rialto, CA study that showed that the use of BWCs led to a 59 percent decrease in UOF and an 87.5 percent decrease in citizen complaints. Likewise, the Mesa, AZ report noted in "Impact" Section above also points to large decreases in UOF and citizen complaints.

The 2017 Police Body Worn Cameras: A Policy Scorecard, <a href="https://www.bwcscorecard.org/">https://www.bwcscorecard.org/</a>, provides an analysis of how scores of different police agencies have employed BWCs through a defined list of metrics.

		<i>C</i> :
		I

Law Enforcement Services Manual

# **Body Worn Cameras**

## 425.1 PURPOSE AND SCOPE

This policy provides guidelines for the use of portable Body Worn Cameras (BWCs) by members of this department while in the performance of their duties.

This policy does not apply to non-BWC evidence, including other methods of audio or video recordings, interviews or interrogations conducted at any Berkeley Police Department facility, authorized undercover operations, wiretaps or eavesdropping (concealed listening devices).

#### 425.2 POLICY

The Berkeley Police Department recognizes that video recording of contacts between department personnel and the public provides an objective record of these events, and that the use of a recording system complements field personnel in the performance of their duties by providing a video record of enforcement and investigative field contacts, which can enhance criminal prosecutions, limit civil liability, increase transparency, and enhance professionalism in the delivery of police services to the community. A video recording of an event or contact also enables the delivery of timely, relevant, and appropriate training to maximize safety for both community members and BPD personnel.

While recordings obtained from BWCs provide an objective record of events, it is understood that video recordings do not necessarily capture all events, activities and information, or reflect the full experience of the individual member(s) in a given incident. Moreover, the recordings, especially video, have limitations and may depict events differently than the events as perceived and recalled by the involved member. Specifically, it is understood that the BWC will capture information that may not have been seen and/or heard by the involved member and that the involved member may see and hear information that may not have been captured by the BWC.

## 425.3 CONFIDENTIALITY AND PROPER USE OF RECORDINGS

BWC use is limited to enforcement and investigative activities involving members of the public. The BWC recordings will capture video and audio evidence for use in criminal investigations, administrative reviews, training, civil litigation, and other proceedings protected by confidentiality laws and department policy. Improper use or release of BWC recordings may compromise ongoing criminal and administrative investigations or violate the privacy rights of those recorded and is prohibited.

#### 425.4 COORDINATOR

The Chief of Police, or his/her designee shall appoint a member of the Department to coordinate the use and maintenance of 8WCs and the storage of recordings, including (Penal Code § 832.18):

- (a) Establishing a system for uploading, storing and security of recordings.
- (b) Designating persons responsible for uploading recorded data.

Law Enforcement Services Manual

## Body Worn Cameras

- (c) Establishing a maintenance system to ensure availability of BWCs.
- (d) Establishing a system for tagging and categorizing data according to the type of incident captured.
- (e) Establishing a system to prevent tampering, deleting and copying recordings and ensure chain of custody integrity.
- (f) Working with the City Attorney's office to ensure an appropriate retention schedule is being applied to recordings and associated documentation.
- (g) Maintaining an audit trail record for all access to evidence files, wherein access information for each evidence file is logged through use of a secure log-in system. The Department's storage system associates an audit trail record with each evidence file, thereby logging the date, time, user name, activity and client IP address occurring during each evidence file access.

All recordings made by members acting in their official capacity shall remain the property of the Department. Subject to the provisions of this Policy, members shall have no expectation of privacy or ownership interest in the content of these recordings.

#### 425.5 MEMBER RESPONSIBILITIES

Prior to going into service, each uniformed member who is assigned to wear a BWC will be responsible for making sure that he or she is equipped with a BWC issued by the Department, and that the BWC is in good working order. If the BWC is not in working order or the member becomes aware of a malfunction at any time, the member shall promptly report the failure to his/her supervisor to permit the supervisor or other department employee to provide the member with a functioning BWC as soon as practicable. Uniformed members should wear the recorder in a conspicuous manner as prescribed by the Department, to provide a generally unobstructed camera view of contacts between members of the public and department members.

Members lawfully engaged in their duties as a police officer are not required to obtain consent from, or give notice to, members of the public, prior to recording with their BWC.

Upon the approval of the Chief of Police, or his/her designee, non-uniformed members fawfully engaged in their duties as a police officer may use an approved BWC.

Members are required to document the existence of a recording in any report or other official record of the contact, such as a CAD entry, including any instance where the member is aware that the BWC malfunctioned or the member deactivated the recording. In the event activity outlined in section 425.7 is not captured in whole or in part the member shall document this and explain in their report their understanding, if any, of why the footage was not captured in the recording.

## 425.6 SUPERVISOR RESPONSIBILITIES

At such time as the scene is considered secure and safe, the on-scene supervisor shall take immediate physical custody of involved officer's/officers' BWC when the device may have captured an incident involving an officer-involved shooting or use of force resulting in death or great bodily injury, and shall ensure the data is uploaded in a timely manner as prescribed by BPD policy

Law Enforcement Services Manual

## Body Worn Cameras

(Penal Code § 832.18). Supervisors may review relevant 8WC video and audio files in the field in furtherance of their duties and responsibilities.

Supervisors shall also review relevant BWC recordings prior to submitting any administrative reports.

### 425.7 ACTIVATION OF THE BODY WORN CAMERA

This policy is not intended to describe every possible situation in which the BWC should be used. Members shall activate the BWC as required by this policy in (a)-(f) below, and may activate the BWC at any time the member believes it would be appropriate or valuable to record an incident within the limits of privacy described herein.

The BWC shall be activated in any of the following situations:

- (a) All in-person enforcement and investigative contacts including pedestrian stops and field interview (FI) situations.
- (b) Traffic stops including, but not limited to, traffic violations, stranded motorist assistance and all crime interdiction stops.
- Self-initiated field contacts in which a member would normally notify the Communications Center.
- (d) Any search activity, including the service of search or arrest warrants; probation, parole, or consent searches where the member is seeking evidence of an offense, or conducting a safety sweep or community caretaking sweep of the premises. Once a location has been secured and the member is not interacting with detainees or arrestees, the member may mute their 8WC when conducting a search for evidence.
- (e) Any other contact that the member determines has become adversarial after the initial contact in a situation where the member would not otherwise activate BWC recording.
- (f) Transporting any detained or arrested person and where a member facilitates entry into or out of a vehicle, or any time the member expects to have physical contact with that person.

At no time is a member expected to jeopardize his or her safety in order to activate a BWC. The BWC should be activated by members in anticipation of situations described above, and in any unanticipated, rapidly unfolding situation where activation becomes required, as soon as the member can do so safely.

Members should activate their BWC when conducting custodial interviews unless there are other recording devices being used. Members shall document and explain in their report the reason for not recording custodial interviews, should a BWC be de-activated while conducting a custodial interview or interrogation.

## 425.8 VICTIMS AND WITNESSES OF CRIMES; INFORMANTS

In the event that an officer has the opportunity to record interviews of victims and witnesses of crimes, they shall consider the following:

- (a) Witnesses: In the event a crime witness or a member of the community wishes to report or discuss criminal activity anonymously, officers have the discretion to not record. Members may offer to avert their camera to capture only audio during the interview, when doing so would facilitate obtaining the witness's recorded statement. In cases where a witness requests they not be recorded, and the member agrees not to record, members should record their request prior to turning the camera off. When a member is already recording, the member shall record their explanation for turning the camera off prior to doing so.
- (b) Victims: Upon request by the victim, officers have the discretion to not record the interview. Members may offer to avert their camera to capture only audio during the interview, when doing so would facilitate obtaining the victim's recorded statement. In cases where a victim requests they not be recorded, and the member agrees not to record, members should record their request prior to turning the camera off. When a member is already recording, the member shall record their explanation for turning the camera off prior to doing so.
  - Domestic Violence Victims: Members should attempt to record interviews of domestic violence victims to facilitate future prosecution efforts and discourage later recanting of statements. Members should also record interviews with children who witness domestic violence, when the child is willing.
  - Child Abuse and Sexual Assault Victims: Members shall have the discretion to record, absent any request to not record the interview by victims, witnesses, or non-suspect parents of victims, during child abuse and/or sexual assault investigations.
- (c) **Informants:** Members shall not activate their recorders when conducting an interview or engaging in a conversation with a confidential informant, unless needed as evidence.

Members have no obligation to advise a victim or witness that he or she is being recorded, but may do so at their discretion. When a victim or witness requests they not be recorded, members may consider their request (See Penal Code 632).

Members shall remain sensitive to the dignity of all individuals being recorded and exercise discretion to respect privacy by discontinuing recording whenever it reasonably appears to the member that such privacy concerns may outweigh any tegitimate law enforcement interest in recording. Recording should resume when privacy concerns are no longer at issue unless the member determines that the circumstances no longer fit the criteria for recording.

Informal community interactions differ from "consensual encounters" in which members make an effort to develop reasonable suspicion to detain or probable cause to arrest. To strengthen relationships between police and citizens, members may use discretion regarding the recording of informal, non-enforcement related interactions with members of the community.

#### 425.9 ACTIVATION IN CROWD CONTROL SITUATIONS

During crowd control, protest or mass arrest incidents, members shall use their BWCs consistent with this policy, or when directed by the Incident Commander. The Incident Commander shall document his or her orders to activate in an appropriate report (e.g. Operations Plan or After Action Report).

The limitations outlined in the Intelligence Procedures for First Amendment Activities Policy governing intelligence-gathering procedures for First Amendment activities, apply to the use of BWCs and other recording devices.

Video recording of individuals who are picketing or engaged in peaceful protest will be avoided unless the officer believes a violation of criminal law is occurring, may occur, or if the officer interacts with a participant or third party to the event, or a participant or third party initiates contact with the member.

## 425.10 SURREPTITIOUS USE OF THE BWC

Members of the Department may surreptitiously record any conversation during the course of a criminal investigation in which the member reasonably believes that such a recording will be lawful. and beneficial to the investigation.

Members shall not surreptitiously record another department member without a court order unless. lawfully authorized by the Chief of Police, or his/her designee.

Members are prohibited from using department-issued BWCs for non-work related personal activity. BWCs will not be activated in places where members have a reasonable expectation of privacy, such as workplace locker rooms, dressing rooms, members' private vehicles or restrooms.

## 425.11 CESSATION OF RECORDING

Once activated, the member may mute or deactivate their BWC at any time based on their discretion, in the following circumstances:

- Discussion of tactical or confidential information with other law enforcement personnel.
- (b) Where members are on a perimeter or assigned to a static post where the member's direct participation in the incident is complete and they are not actively part of an investigation.
- If it is necessary to discuss issues or concerns with an employee, supervisor, doctor, nurse, or paramedic in private.
- In the member's judgment, a recording would interfere with his or her ability to conduct (d) an investigation.

Decisions regarding the reason for muting or BWC deactivation shall be noted on the recording. or otherwise documented.

Law Enforcement Services Manual

## Body Worn Cameras

Members shall cease audio/video recording whenever necessary to ensure conversations are not recorded between a person in custody and the person's attorney, religious advisor or physician, unless there is explicit consent from all parties to the conversation. This does not apply to conversations with paramedics or EMTs during their response at a scene, and during transport.

#### 425.12 EXPLOSIVE DEVICE

Many portable recorders, including BWCs and audio/video transmitters, emit radio waves that could trigger an explosive device. Therefore, these devices should not be used where an explosive device may be present.

Members believing that the use of a BWC may detonate an explosive device may deactivate their 8WC in such cases.

## 425.13 PROHIBITED USE OF BODY WORN CAMERAS

Members are prohibited from using a department-issued BWC for personal use and are prohibited from making personal copies of recordings created while on duty or while acting in their official capacity.

Members are prohibited from retaining BWC recordings. Members shall not duplicate or distribute such recordings, except for department business purposes. All such recordings shall be retained at the Department.

Members may not use personally owned recorders (e.g. personal cell phone) to document contacts unless exigent circumstances exist to warrant the use of personally owned recording devices. Regardless, if a member is using a department-issued 8WC, and/or another recording device, members shall comply with the provisions of this policy, including retention and release requirements. In every event where members use any recording device aside from or in addition to their department-issued BWC, the member shall document and explain the use and the exigent circumstance in their police report (e.g. the BWC failed and evidence needed to be captured at that moment in time).

Recordings shall not be used by any member for the purpose of embarrassment, intimidation or ridicule.

## 425.14 PROCESSING AND HANDLING OF RECORDINGS

To assist with identifying and preserving data and recordings, members shall tag and download recordings in accordance with procedure, and document the existence of the recording in the related case report. Transfers must occur at the end of the member's shift, and any time the member is aware that the storage capacity of the BWC is nearing its limit. In circumstances when the officer cannot complete this task, the officer's supervisor shall immediately take custody of the BWC and be responsible for uploading the data. Officers shall tag each file with the appropriate case/incident number, provide a descriptive title, and select an appropriate category for each recording, using the Axon View app or via the Evidence.com site.

(

Members are prohibited from intentionally erasing, altering, reusing, modifying or tampering with original audio video recordings. Members may request restriction and subsequent detetion of an accidental recording as described under section 425.16 below.

#### 425.15 RETENTION REQUIREMENTS

The Department shall retain all recordings for a minimum of 60 days. Incidents involving consensual contacts, and aid to citizens will be retained for six months, and cold reports will be retained for one year. Recordings of incidents involving use of force by a police officer, detentions, arrests, or recordings relevant to a formal or informal complaint shall be retained for a minimum of two years and one month. Recordings relating to court cases and personnel complaints that are being adjudicated will be manually deleted at the same time other evidence associated with the case is purged in line with the Department's evidence retention policy. Any recordings related to administrative or civil proceedings shall be maintained until such matter is fully adjudicated, at which time it shall be deleted in line with the Department's evidence retention policy, and any applicable orders from the court.

Recordings created by equipment testing or accidental activation may be deleted after 60 days.

#### 425.16 ACCIDENTAL RECORDING - REQUEST FOR RESTRICTION

In the event of an accidental or sensitive personal recording of non-departmental business activity, where the resulting recording is of no investigative or evidentiary value, the recording employee may request that the file be restricted pending 60-day deletion by submitting an email request via their chain of command to the Professional Standards Division Captain. The Professional Standards Division Captain will approve or deny the restriction request. In cases where the request is denied, an appeal may be submitted to the Chief of Police, or his/her designee, for restriction authorization. In all cases of restriction requests, a determination should be made within seven calendar days.

## 425.17 REVIEW OF RECORDINGS BY A MEMBER

Members are authorized to review their own BWC video files at any time in furtherance of official business. Such official business includes, but is not limited to, preparing written reports, prior to or while providing testimony in a case or being deposed. Members may review recordings as an evidentiary resource, except as stated in subsection 425.17.1 below. Members shall not retain personal copies of recordings. Members shall not use the fact that a recording was made as a reason to write a less detailed report.

# 425.17.1 OFFICER INVOLVED INCIDENTS RESULTING IN GRAVE BODILY INJURY OR DEATH

(a) In the event of a critical incident that results in grave bodlly Injury or death, including an officer-involved shooting or an in-custody death, the 8WC of the involved member(s) shall be taken from him or her and secured by a supervisor, commander, or appropriate investigator, as necessary. The involved member(s) shall not access or obtain their footage of the incident until such time as the criminal investigator(s) have reviewed

Law Enforcement Services Manual

## Body Worn Cameras

the video files. It will be the responsibility of the investigation team's supervisor to coordinate with the involved member's supervisor to obtain footage of the incident on behalf of the member.

- (b) Personnel uploading secured BWC video files shall not view the files unless authorized.
- (c) No member involved in a critical incident may view any video recordings prior to an interview by the appropriate criminal investigative unit, and receiving command approval.
- (d) Prior to the conclusion of the criminal interview process, the involved member and/ or the member's representative will have an opportunity to review the member's recording(s). The involved member may choose to provide additional information to supplement his or her statement by providing a supplemental statement or separate supplemental document. In no case shall a member after a report made prior to reviewing the recording.
- (e) The Department acknowledges that recordings taken during critical incidents obtained from BWCs do not necessarily reflect the full extent of the nature of the event or the experience, analysis, training, threat assessment or state of mind of the individual officers(s) in a given incident. Moreover, the recordings, especially video, have limitations and may depict events differently than the events recalled by the involved officer. Specifically, it is understood that the recording device will capture information that may not have been heard and/or observed by the involved officer and that officers may see and hear events that are not captured by the camera.

Officers who are involved in any critical incident where video recordings exist depicting the involved officer, either as a subject officer or witness, shall be provided the following admonishment to the initial interview or submission of the initial written report:

"In this case, there is video evidence that you will have an opportunity to view. Video evidence has limitations and may depict the events differently than you recall, and may not depict all of the events as seen or heard by you. Video has a limited field of view and may not capture events normally seen by the human eye. The "frame rate" of video may limit the camera's ability to capture movements normally seen by the human eye. Lighting as seen on the video may be different than what is seen by the human eye. Videos are a two-dimensional medium and may not capture depth, distance or positional orientation as well as the human eye. Remember, the video evidence is intended to assist your memory and ensure that your statement explains your state of mind at the time of the incident."

#### 425.17.2 SUPERVISORY REVIEW

With the exception of section 425.17.1 above, supervisors are authorized to review relevant recordings any time they are reviewing and approving case reports from their subordinates.

#### 425.17.3 INVESTIGATORY REVIEW

Supervisors are authorized to review relevant recordings any time they are investigating alleged misconduct or reports of meritorious conduct, or whenever such recordings support review of the member's performance.

Recorded files may also be reviewed:

- Upon approval by a supervisor, by any member of the Department who is participating in conduct of an official investigation, such as a personnel complaint, an administrative investigation or a criminal investigation.
- (b) Pursuant to lawful process or by court or District Attorney personnel who are otherwise authorized to review evidence in a related case.
- (¢) By personnel assigned to investigatory units who are authorized to view any BWC video file associated to their active investigations, unless otherwise prohibited by policy.
- Upon approval by the Chief of Police, Internal Affairs investigators may review BWC video with a complainant.

Investigators conducting criminal or internal investigations shall:

- 1. Advise the coordinator to restrict access to the BWC file in criminal or internal investigations, as necessary.
- 2. Review the file to determine whether the BWC file is of evidentiary value and process it in accordance with established protocols.
- 3. Notify the coordinator to remove the access restriction when the criminal/internal investigation is closed.

#### 425.17.4 TEACHING OR LEARNING TOOL

BWC files may also be reviewed by training staff regarding specific incidents where such files may serve as an internal learning or teaching tool. In the event that videos are intended to be used for training purposes, the involved officer(s) will first be consulted. If he/she objects to the use of the video, such objection shall be submitted to the person in charge of training who shall weigh the value of the video for training against the officer(s) objections and basis for the objection. Should the person in charge of training refuse to grant the request of the involved officer(s), the matter shall be heard by the Chief of Police, or his/her designee, prior to utilizing the video.

#### 425.17.5 COB CIVIL CLAIMS AND LAWSUITS.

BWC recordings may be reviewed and used by City of Berkeley defense counsel for the purposes of defending the city in civil claims and lawsuits, with the authorization of the Chief of Police, or his/her designee.

#### 425.18 RELEASE OF RECORDINGS

All recordings should be reviewed by the Custodian of Records and the City Attorney's Office prior to public release, see General Order R-23 (Release of Public Records and Information).

Law Enforcement Services Manual

## Body Worn Cameras

In the event that the Police Department or City Department intends to release or publish for any purpose video recordings where officers are captured on video or the video depicts actions taken by them in the course of the performance of their official duties, those officers shall be given written notice of the intention to release or publish said video at least 48 hours prior to such release.

BPD may, without prior notice to involved officers, share video footage with law enforcement, national security, military, or other government agencies outside of Berkeley, when there is reasonable suspicion that criminal activity has occurred or is about to occur.

## 425.18.1 POLICE REVIEW COMMISSION (PRC)

Access to recorded files will be granted for the purposes of review to the Police Review Commission Officer and/or Investigator investigating a specific complaint where BWC evidence files are available, and are not part of any ongoing criminal investigation.

- (a) The PRC Officer and PRC Investigator will be provided user account access to evidence files through the evidence management system for their use during a complaint investigation and to facilitate viewing by Board of Inquiry members during a Board of Inquiry.
- (b) The PRC Officer and PRC investigator shall not make or create a copy of any evidence file, nor make or allow to be made any audio or video recording of any evidence file white it is being streamed and viewed from the evidence management system.
- (c) The PRC Officer and PRC Investigator shall not allow any unauthorized individuals to view or access evidence files.
- (d) The evidence management system associates an audit trail record with each evidence file, thereby togging the date, time, user, activity, and client IP address occurring during each evidence file access.
- (e) The evidence management system shall only be accessed on City premises.
- (f) The Department retains custody and control of the recordings, and content of the video will be subject to applicable legal standards including, but not limited to the confidentiality requirements of the Public Safety Officers' Procedural Bill of Rights, (Government Code § 3300, et seq., Penal Code § 832.7, and the California Public Records Act; Government Code § 6250, et seq.)

## 425.18.2 PUBLIC RECORDS ACT (PRA) REQUEST

Access to recorded files will be granted for the purposes of review in response to a public records request, as permitted under Government Code § 6254(f) and BPD General Order R-23 (Release of Public Records and Information). General Order R-23 does not authorize release of investigative files or documents that would constitute an unwarranted invasion of privacy. Circumstances where this might arise in video include footage taken inside a home, a medical facility, the scene of a medical emergency, or where an individual recorded has a "reasonable expectation of privacy."

Law Enforcement Services Manual

## **Body Worn Cameras**

#### 425.18.3 MEDIA

Access to recorded files will be granted for the purposes of review to media personnel or the general public with permission of the Chief of Police, or his/her designee, subject to General Order R-23 and privacy protections indicated in this policy.

# 425.19 COMPLIANCE WITH BMC 2.99 ACQUISITION AND USE OF SURVEILLANCE TECHNOLOGY

This policy shall comply at all times with the requirement of BMC 2.99 Acquisition and Use of Surveillance Technology.

#### 425.20 TRAINING REQUIRED

Officers who are assigned BWCs must complete department-approved training in the proper use and maintenance of the devices before deploying to the field.

As part of a continual improvement process, regular review should be conducted by BPD staff of the training on this policy and the related use of BWCs under this policy. Information resulting from the outcomes of this review shall be incorporated into the City Manager's annual "Surveillance Technology Report" as required under BMC 2.99 Acquisition and Use of Surveillance Technology.

The Department, Police Review Commission and other City Departments shall maintain the confidentiality of Department sworn employee personnel records as required by state and local law. Failure to maintain the confidentiality of Department sworn employee personnel records, whether or not intentional, may subject individuals to civil penalties and discipline, up to and including termination of employment.

		<i>C</i> :
		(

Policy Manual

# Surveillance Use Policy - GPS Tracking Devices

#### 1301.1 PURPOSE

Global Positioning System (GPS) tracking devices designed to track the movements of vehicles, bicycles, cargo, machinery, and other items. GPS trackers are utilized during active criminal investigations and shall be used pursuant to a lawfully issued search warrant, court order or with consent.

#### 1301.2 AUTHORIZED USE

GPS trackers shall only be used pursuant to a valid search warrant; pursuant to court-ordered parole or probation conditions, if applicable; or with consent of the owner of the object to which the GPS tracker is attached.

GPS trackers shall only be utilized for law enforcement purposes.

#### 1301.3 DATA COLLECTION

Location data may be obtained through the use of a GPS Tracker.

#### 1301.4 DATA ACCESS

Access to GPS tracking data shall be limited to Berkeley Police Department (BPD) personnel utilizing the GPS Tracker(s) for active criminal investigations. Information may be shared in accordance with 1301,9 below.

#### 1301.5 DATA PROTECTION

The data from the GPS tracker is encrypted by the vendor. The data is only accessible through a secure website to BPD personnel who have been granted security access.

## 1301.6 CIVIL LIBERTIES AND RIGHTS PROTECTION:

The Berkeley Police Department is dedicated to the most efficient utilization of its resources and services in its public safety endeavors. The Berkeley Police Department recognizes the need to protect its ownership and control over shared information and to protect the privacy and civil liberties of the public, in accordance with federal and state law. The procedures described within this policy (Data Access, Data Protection, Data Retention, Public Access and Third Party Data Sharing) protect against the unauthorized use of GPS tracker data. These procedures ensure the data is not used in a way that would violate or infringe upon anyone's civil rights and/or liberties, including but not limited to potentially disparate or adverse impacts on any communities or groups.

#### 1301.7 DATA RETENTION

Data is stored electronically by the host company for 90 days, and then it is purged.

Printed data shall be kept in accordance with applicable laws, BPD policies that do not conflict with applicable law or court order, and/or as specified in a search warrant.

## 1301.8 PUBLIC ACCESS

Data collected and used in a police report shall be made available to the public in accordance with department policy and applicable state or federal law.

#### 1301.9 THIRD-PARTY DATA-SHARING

Data collected from the GPS trackers may be shared with the following:

- (a) The District Attorney's Office for use as evidence to aid in prosecution, in accordance with laws governing evidence;
- (b) Other law enforcement personnel as part of an active criminal investigation;
- (c) Other third parties, pursuant to a Court Order.

## 1301.10 TRAINING

Training for the operation of the GPS trackers shall be provided by BPD personnel. All BPD personnel shall be provided with this Surveillance Use Policy.

## 1301.11 AUDITING AND OVERSIGHT

Division Captains or their designee shall ensure compliance with this Surveillance Use Policy.

#### 1301.12 MAINTENANCE

GPS trackers shall only be obtained with the permission of the Investigations Division Captain or his/her designee. The Investigations Division Captain or his/her designee will ensure the trackers are returned when the mission/investigation is completed.

#### **GPS TRACKING DEVICES**

#### A. DESCRIPTION

Global Positioning System (GPS) trackers are devices designed to track the movements of vehicles, bicycles, cargo, machinery, and/or individuals.

The Berkeley Police Department currently uses two types of GPS Tracking Devices. The manufacturer, 3SI Security System, describes them as follows:

- 1. The "Slap-n-Track" (SNT) tracker tracks vehicles, cargo, and other large assets for long deployments. Offers extended battery life, rugged and weatherproof housing, and optional magnets per the manufacturer.
- 2. The "Electronic Stake Out" (ESO) tracker offers Law Enforcement miniaturized and covertly packaged GPS Tracking Solutions to target property crimes, especially pattern crimes, in their local jurisdictions.

#### B. PURPOSE

The purpose of GPS trackers is to enhance the quality of active investigations. The trackers are utilized during active investigations and shall be used pursuant to a lawfully issued search warrant, court order, or with consent as described below.

#### C. LOCATION

GPS tracking devices shall be deployed in locations consistent with the authority granted by consent or a lawfully issued search warrant or court order.

## D. IMPACT

The Berkeley Police Department is dedicated to the most efficient utilization of its resources and services in its public safety endeavors. The Berkeley Police Department recognizes the need to protect its ownership and control over shared information and to protect the privacy and civil liberties of the public, in accordance with federal and state law. The procedures utilized with GPS trackers help to ensure unauthorized use of its data. The policies ensure the data is not used in a way that would violate or infringe upon anyone's civil rights and/or liberties, including but not limited to potentially disparate or adverse impacts on any communities or groups.

#### E. MITIGATION

Data from a GPS tracker is encrypted from the vendor. Data shall be maintained in a secure, non-public location, such as locations requiring security access or badge access, thereby safeguarding the public from any impacts identified in subsection (D).

#### F. DATA TYPES AND SOURCES

Location data is obtained through the use of a GPS Tracker.

Latitude and longitude data is captured and stored indefinitely by 3SI when both types of trackers are used. This data is only shared with the District Attorney's Office for prosecution purposes.

#### G. DATA SECURITY

Data from a GPS tracker is encrypted from the vendor. Data shall be maintained in a secure, non-public location, such as locations requiring security access or badge access. In addition, Captains for Divisions utilizing GPS trackers are responsible for ensuring compliance with the procedures for utilizing GPS Trackers.

#### H. FISCAL COST

The initial cost of the GPS trackers totaled \$4,335.

- Between 2015-present BPD purchased 5 GPS "ESO" trackers for \$2,250 (\$450 each).
- In 2017 BPD purchased 3 GPS "SNT" trackers for \$2,085 (\$695 each).

The annual cost for the GPS data service totals \$1,920.

- The annual data service for the five ESO trackers is \$1,020 (\$204 each).
- The annual data service for the three SNT trackers is \$900 (\$300 each).

Personnel costs are minimal in that the GPS trackers are used as a resource during normal working hours.

GPS trackers are funded through the Investigations Division's general budget.

#### I. THIRD PARTY DEPENDENCE AND ACCESS

Data collected from the GPS trackers may be shared with the following:

- a. The District Attorney's Office for use as evidence to aid in prosecution, in accordance with laws governing evidence;
- b. Other law enforcement offices as part of a criminal investigation;
- Other third parties, pursuant to a Court Order.

#### J. ALTERNATIVES

None.

#### K. EXPERIENCE OF OTHER ENTITIES

The use of GPS technology is common amongst law enforcement agencies throughout the country.

Policy Manual

# Surveillance Use Policy - ALPR

## 1302.1 PURPOSE

This Surveillance Use Policy is issued in compliance with 8MC 2.99, and incorporates language from the Berkeley Police Department ALPR Policy #422 and adds elements as required by BMC 2.99.

The policy of the Serkeley Police Department is to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public.

All data and images gathered by the ALPR are for the official use of this department. Because such data may contain confidential information, it is not open to public review. (Ref. policy 422.2)

## 1302.2 AUTHORIZED AND PROHIBITED USES USE

Use of an ALPR is restricted to the purposes outlined below. Department members shall not use, or allow others to use the equipment or database records for any unauthorized purpose (Civil Code § 1798.90.51; Civil Code § 1798.90.53). (Ref. policy 422.4)

- (a) An ALPR shall only be used for official law enforcement business.
- (b) An ALPR may be used in conjunction with any routine patrol operation or criminal investigation. Reasonable suspicion or probable cause is not required before using an ALPR.
- (c) While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped cars to canvass areas around homicides, shootings and other major incidents. Partial license plates reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.

#### 1302.3 DATA COLLECTION

All data and images gathered by an ALPR are for the official use of the Berkeley Police Department. Such data may contain confidential CLETS information and is not open to public review. ALPR information gathered and retained by this department may be used and shared with prosecutors or other law enforcement agencies only as permitted by law and Berkeley Police Department policy. (Ref. policy 422.5)

#### 1302.4 DATA ACCESS

- (a) No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.
- (b) No ALPR operator may access California Law Enforcement Telecommunications System (CLETS) data unless otherwise authorized to do so.
- (c) If practicable, the officer should verify an ALPR response through the California Law Enforcement Telecommunications System (CLETS) before taking enforcement action that

is based solely on an ALPR alert.

#### 1302.5 DATA PROTECTION

All saved data will be safeguarded and protected by both procedural and technological means. The Berkeley Police Department will observe the following safeguards regarding access to and use of stored data (Civil Code § 1798.90.51; Civil Code § 1798.90.53) (Ref. policy 422.6):

- (a) All ALPR data downloaded to any workstation or server shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time (Civil Code § 1798.90.52).
- (b) Berkeley Police Department members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action and parking enforcement.
- (c) Aggregated ALPR data not related to specific criminal investigations shall not be released to any local, state or federal agency or entity without the express written consent of the City Manager.
- (d) Measures will be taken to ensure the accuracy of ALPR information. Errors discovered in ALPR data collected by ALPR units shall be marked, corrected or deleted in accordance with the type and severity of the error in question

## 1302.6 CIVIL LIBERTIES AND RIGHTS PROTECTION:

The Berkeley Police Department is dedicated to the most efficient utilization of its resources and services in its public safety endeavors. The Serkeley Police Department recognizes the need to protect its ownership and control over shared information and to protect the privacy and civil liberties of the public, in accordance with federal and state law. The procedures described within this policy (Data Access, Data Protection, Data Retention, Public Access and Third Party Data Sharing) protect against the unauthorized use of ALPR data. These policies ensure the data is not used in a way that would violate or infringe upon anyone's civil rights and/or liberties, including but not limited to potentially disparate or adverse impacts on any communities or groups.

#### 1302.7 DATA RETENTION

The Investigations Division Captain, or his/her designee, is responsible for ensuring proper collection and retention of ALPR data. Technical support and assistance shall be provided by the City of Berkeley's Department of Information Technology (IT) and associated ALPR system providers/vendors as identified in Appendix A. IT staff will not have the ability to access or view individual records or reports, as they may contain CLETS information they are not authorized to receive. IT's role will be limited to providing initial infrastructure set-up, unless particular IT staff members have been cleared by OOJ background checks and authorized by the Chief of Police to receive ALPR records.

All ALPR data downloaded to the server should be stored for a minimum of one year (Government Code § 34090.6) and in accordance with the established records retention schedule. Thereafter, ALPR data should be purged unless it has become, or it is reasonable to believe it will become,

evidence in a criminal or civil action or is subject to a lawful action to produce records. In those circumstances the applicable data should be downloaded from the server onto portable media and booked into evidence. (Ref. policy 422.5)

(a) Collected images and metadata of hits will not be stored for more than 365 days. Metadata of reads will not be stored for more than 30 days. Images of reads will not be transferred to the server.

#### 1302.8 PUBLIC ACCESS

- (a) Non-law enforcement requests for access to stored ALPR data shall be processed according to the Records Maintenance and Release Policy in accordance with applicable law. (Ref. policy 422.6 (a))
- (b) Non-law enforcement requests for information regarding a specific vehicle's license plate may be honored when the requester is the registered owner of the vehicle in question, and when providing such information will not invade the privacy of a third party. The requestor in such cases must provide acceptable proof of his or her identity and of ownership of the vehicle in question. (Ref. policy 422.6 (b))

## 1302.9 THIRD-PARTY DATA-SHARING

The ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law.

Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Records Maintenance and Release Policy (Civil Code § 1798.90.55).

Aggregated ALPR data not related to specific criminal investigations shall not be released to any local, state or federal agency or entity without the express written consent of the City Manager. (Ref. policy 422.6 (e))

## 1302.10 TRAINING

Training for the operation of ALPR Technology shall be provided by BPD personnel. All BPD employees who utilize ALPR Technology shall be provided a copy of this Surveillance Use Policy.

## 1302.11 AUDITING AND OVERSIGHT

ALPR system audits will be conducted by the Professional Standards Bureau's Audit and Inspections Sergeant on a regular basis, at least biannually, (Ref. policy 422.6 (g))

#### 1302.12 MAINTENANCE

Any installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Investigations Division Captain. The Investigations Division Captain will assign members under his/her command to administer the day-to-day operation of the ALPR equipment and data. (Ref. policy 422.3)

#### 1302.12.1 ALPR ADMINISTRATOR

The Investigations Division Captain, or his/her designee, shall be responsible for developing guidelines and procedures to comply with the requirements of Civil Code § 1798.90.5 et seq. This includes, but is not limited to (Civil Code § 1798.90.51; Civil Code § 1798.90.53) (Ref. policy 422.3.1):

- (a) A description of the job title or other designation of the members and independent contractors who are authorized to use or access the ALPR system or to collect ALPR information.
- (b) Training requirements for authorized users.
- (c) A description of how the ALPR system will be monitored to ensure the security of the information and compliance with applicable privacy laws.
- (d) Procedures for system operators to maintain records of access in compliance with Civil Code § 1798.90.52.
- (e) The title and name of the current designee in overseeing the ALPR operation.
- (f) Ensuring this policy and related procedures are conspicuously posted on the City's website.

# AUTOMATED LICENSE PLATE READER (ALPR) DEVICES

#### A. DESCRIPTION

Automated License Plate Readers (ALPRs) are high-speed, computer controlled camera systems that are typically mounted on Berkeley Police Department Parking Enforcement Vehicles.

ALPRs capture license plate numbers which come into view, along with the location, date and time. The data, which includes a photo of the front or the back of the car displaying the ficense plate, is then uploaded to a central server.

# B. PURPOSE

The Berkeley Police Department's Parking Enforcement Unit utilizes vehicles equipped with ALPRs to conduct enforcement of posted time limits in commercial areas and Residential Preferential Parking (RPP) permit areas. These ALPR's also access information in the California Law Enforcement Telecommunications System's (CLETS) Stolen Vehicle System (SVS) database, which provides information on matches for stolen and wanted vehicles.

The Berkeley Police Department's Scofflaw Enforcement program (often referred to as the "booting" program) utilizes an ALPR to scan license plates, and check the scanned "reads" against a list of vehicles which have five or more outstanding parking citations exceeding 30 days old. Typically, upon a confirmed "hit," the vehicle is immobilized with a "boot", or towed, and the owner has to pay the outstanding citations and fees in order to release the boot and/or recover their car from storage. This allows the City to recover outstanding parking citation fees.

#### C. LOCATION

Parking Enforcement vehicles travel throughout the city; using the ALPRs as described above.

# D. IMPACT

The Berkeley Police Department is dedicated to the most efficient utilization of its resources and services in its public safety endeavors. The Berkeley Police Department recognizes the need to protect its ownership and control over shared information and to protect the privacy and civil liberties of the public, in accordance with federal and state law. The procedures utilized with ALPR Units will help to ensure unauthorized use of its data. The procedures will ensure the data is not used in a way that would violate or infringe upon anyone's civil rights and/or liberties, including but not limited to potentially disparate or adverse impacts on any communities or groups.

#### E. MITIGATION

All saved data will be safeguarded and protected by both procedural and technological means which are implemented to safeguard the public from any impacts identified in subsection (D). See subsection (G) for further.

1

(

#### F. DATA TYPES AND SOURCES

Photographs of license plates and location data may be obtained through the use of ALPR Units.

#### G. DATA SECURITY

The Berkeley Police Department will observe the following safeguards regarding access to and use of stored data (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

- All ALPR data downloaded to any workstation or server shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time (Civil Code § 1798.90.52).
- Berkeley Police Department members approved to access ALPR data under these
  guidelines are permitted to access the data for legitimate law enforcement purposes
  only, such as when the data relate to a specific criminal investigation or departmentrelated civil or administrative action and parking enforcement.
- Aggregated ALPR data not related to specific criminal investigations shall not be released to any local, state or federal agency or entity without the express written consent of the City Manager.
- 4. Measures will be taken to ensure the accuracy of ALPR information. Errors discovered in ALPR data collected by ALPR units shall be marked, corrected or deleted in accordance with the type and severity of the error in question.

## H. FISCAL COST

In 2015, Public Works brought an ALPR Contract to City Council. Council approved a contract for Public Works to buy five Genetec ALPR Units with PCS Mobile communication, for a pilot program for \$450,000.

In 2017, after success with the program, City Council approved an amendment to the contract, allowing Public Works to purchase 15 more ALPR Units for Parking Enforcement vehicles, and to continue its use of PCS Mobile, for 1,200,000. The money was allocated from the goBerkeley/Federal Highway Administration Parking Meter Fund.

Yearly service for the ALPR Units includes warranties, hosting services, cellular connection, mobile computing, and training which varies. The costs through fiscal year 2022 are currently estimated at \$1,175,000.

Personnel costs are minimal in that the ALPR Units are used as a resource during normal working hours.

# THIRD PARTY DEPENDENCE AND ACCESS

- Vendor Access-Scofflaw Enforcement: The contracted vendor for the City's Scofflaw Enforcement program is currently Paylock. Paylock stores data on a secure server, and provides access to authorized personnel via Paylock's "Bootview" secure website, as described below:
  - a. All data captured by the ALPR is stored on the laptop for 30 days, and is only accessible during that period via the ALPR proprietary software. This includes reads, hits, and photographs associated with each.
  - b. When a car is booted and/or towed, the read, hit and photographic data relating to the booting and/or towing of scofflaw vehicles is uploaded to Paylock's secure server. No other data is uploaded to Paylock's secure server.
- Vendor Access-General Parking Enforcement and goBerkeley Program: The
  contracted vendor for the City's Parking Enforcement ALPR is currently Genetec. The
  city uses Genetec ALPRs to support efficient enforcement of posted time limit parking
  and Residential Preferential Parking permits.
  - a. In addition, Genetec periodically provides reports to the City of Berkeley Transportation Division's "goBerkeley" parking management program so that the City's program can analyze data about parking demand. These reports do not contain any information about a vehicle's license plate number, the name of the registered owner, address of registered owner, or any other information gleaned from the license plate number associated with a particular vehicle. Rather, the reports consist of completely anonymized information, using identification numbers that are not associated with a particular license plate or registered owner.
  - b. The reports will provide only the date, time, location, approximate address, "goBerkeley" blockface ID, and Residential Permit Pass (RPP) area in which a vehicle was observed. If a citation was not issued for an RPP or other time limit violation, the report may also provide the reason a parking enforcement officer concluded there was no parking violation, e.g., RPP visitor pass, disabled placard or license plate, etc.
- Department of Information Technology Access: Technical support and assistance for ALPR's is provided by the City of Berkeley's Department of Information Technology (IT) and associated ALPR system providers/vendors as identified herein. IT staff who

do not have the proper clearance and training do not have the ability to access or view individual records or reports, as they may contain CLETS information they are not authorized to receive. IT provides initial infrastructure set-up, and continued systems support as needed to ensure efficient and accurate performance of the ALPR hardware and software. Only IT staff members who have successfully undergone DOJ background checks and training are authorized by the Chief of Police to view specific ALPR records.

- 4. Other Law Enforcement Agency Access: ALPR data may only be shared with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law. Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Records Maintenance and Release Policy (Civil Code § 1798.90.55). Aggregated ALPR data not related to specific criminal investigations shall not be released to any local, state or federal agency or entity without the express written consent of the City Manager.
- 5. Member Access: No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training. No ALPR operator may access CLETS data unless otherwise authorized to do so. If practicable, the officer should verify an ALPR response through CLETS before taking enforcement action that is based solely on an ALPR alert.

1

6. Public Access: Non-law enforcement requests for access to stored ALPR data shall be processed according to the Records Maintenance and Release Policy in accordance with applicable law. Non-law enforcement requests for information regarding a specific vehicle's license plate may be honored when the requester is the registered owner of the vehicle in question, and when providing such information will not invade the privacy of a third party. The requestor in such cases must provide acceptable proof of his or her identity and of ownership of the vehicle in question.

# J. ALTERNATIVES

None.

## K. EXPERIENCE OF OTHER ENTITIES

The use of ALPR technology is common amongst law enforcement agencies throughout the country, in support of parking enforcement, and law enforcement criminal investigations.

**DATE ISSUED: 02/18/16** 

# SUBJECT: AUTOMATED LICENSE PLATE READER (ALPR)

# <u>PURPOSE</u>

1 - This order establishes guidelines for the use of the Berkeley Police Department's Automated License Plate Reader (ALPR) technology and data. ALPR technology functions by automatically capturing an image of a vehicle's license plate, transforming that image into alphanumeric characters using optical character recognition software, and storing that information, along with relevant metadata (e.g. geo-location and temporal information, as well as data about the ALPR). ALPRs may be used by the Berkeley Police Department Parking Enforcement and Traffic Units for official law enforcement purposes.

# <u>POLICY</u>

# Administration of ALPR Data

2- Any installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Investigations Division Captain through the Traffic Bureau. The Investigations Division Captain will assign personnel under his/her command to administer the day-to-day operation of the ALPR equipment and data.

# ALPR Operation

- 3- Department personnel shall not use, or allow others to use, the ALPR equipment or database records for any unauthorized purpose.
  - a. An ALPR shall only be used for official and legitimate law enforcement business.
  - Reasonable suspicion or probable cause is not required before using an ALPR.
  - No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.
  - d. No ALPR operator may access California Law Enforcement Telecommunications System (CLETS) data unless otherwise authorized to do so.

# DEPARTMENT ORDER

# ADMINISTRATIVE ORDER #001-2016

**DATE ISSUED: 02/18/16** 

# ALPR Data Collection and Retention

- 4- All data and images gathered by an ALPR are for the official use of the Berkeley Police Department. Such data may contain confidential CLETS information and is not open to public review. ALPR information gathered and retained by this department may be used and shared with prosecutors or other law enforcement agencies only as permitted by law.
- 5- The Parking Enforcement Manager is responsible for ensuring proper collection and retention of ALPR data. Technical support and assistance shall be provided by City Department of Information Technology personnel and associated ALPR system providers/vendors as identified below. IT staff will not have the ability to access or view individual records or reports, as they may contain CLETS information they are not authorized to receive. IT's role will be limited to providing initial infrastructure set-up, unless particular IT staff members have been cleared by DOJ background checks and authorized by the Chief of Police to receive ALPR records.
- 6- All ALPR data shall be stored as described in this order and thereafter shall be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a lawful action to produce records. In those circumstances the applicable data shall be downloaded from the server onto portable media and booked into evidence. The records will then be subject to standard evidence retention polices and statutes.
  - a. Collected images and metadata of hits will not be stored for more than 365 days. Metadata of reads will not be stored for more than 30 days. Images of reads will not be transferred to the server.

# Accountability and Safeguards

- 7- All saved data will be safeguarded and protected by both procedural and technological means. The Berkeley Police Department will observe the following safeguards regarding access to and use of stored data:
  - Non-law enforcement requests for access to stored ALPR data shall be processed according to General Order R-23 in accordance with applicable law.
  - Non-law enforcement requests for information regarding a specific vehicle's license plate may be honored when the requestor is the registered owner of the vehicle in question, and when providing such

information will not invade the privacy of a third party. The requestor in such cases must provide acceptable proof of his or her identity and of ownership of the vehicle in question.

- ALPR data downloaded to any workstation or server shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time.
- d. Berkeley Police personnel approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relates to a specific criminal investigation or department-related civil or administrative action and parking enforcement.
- ALPR data may be released to other authorized and verified law enforcement officials and agencies for legitimate law enforcement purposes only in connection with specific criminal investigations.
- f. Aggregated ALPR data not related to specific criminal investigations shall not be released to any local, state, or federal agency or entity without the express written consent of the City Manager.
- g. Measures will be taken to ensure the accuracy of ALPR information. Errors discovered in ALPR data collected by ALPR units are marked, corrected, or deleted in accordance with the type and severity of the error in question.
- ALPR system audits will be conducted by personnel assigned to the Professional Standards Bureau on a regular basis, at least biennially.

# Current ALPR Deployments

- 9- The Berkeley Police Department uses ALPR technology in the Parking Enforcement Unit for parking and scofflaw enforcement.
- 10- Effective 2/18/16, the Parking Enforcement Unit will utilize five (5) Parking Enforcement Go-4 vehicles equipped with ALPR units to conduct enforcement of posted time limits in commercial areas and Residential Preferential Parking (RPP) permit areas. These ALPR's will also access information in the DMV/SVS database (stolen and wanted vehicles). The

## DEPARTMENTALORDER

# ADMINISTRATIVE ORDER #001-2016

**DATE ISSUED: 02/18/16** 

current contracted vendor for this system is PCS Mobile using Genetec ALPR technology.

- 11- The Scofflaw Enforcement program (often referred to as the "booting" program) utilizes an ALPR to scan license plates, and checks scanned "reads" against a file of vehicles which have five or more outstanding parking citations exceeding 30-days old. Typically, upon a confirmed "hit," the vehicle is immobilized with a "boot", or towed, and the owner has to pay the outstanding citations and fees in order to release the boot and/or recover their car from storage. This allows the city to recover outstanding citation fees and penalties. ALPR equipment is installed in the Parking Enforcement Unit's Scofflaw Enforcement vehicle.
- 12- The contracted vendor for the City's Scofflaw Enforcement program is currently Paylock. Paylock stores data on a secure server, and provides access to authorized personnel via Paylock's "Bootview" secure website, as described below:
  - a. All data captured by the ALPR is stored on the laptop for 30 days, and is only accessible during that period via the ALPR proprietary software. This includes reads, hits, and photographs associated with each.
- 13- When a car is booted and/or towed, the read, hit, and photographic data relating to the booting and/or towing of scofflaw vehicles is uploaded to Paylock's secure server. No other data is uploaded to Paylock's secure server.
- 14- The City's Parking Enforcement ALPR vendor (currently Genetec) will periodically provide reports to the City of Berkeley Transportation Division's goBerkeley parking management program so that it can analyze data about parking demand. These reports will not contain any information about a vehicle's license plate number, the name of the registered owner, address of registered owner, or any other information gleaned from the license plate number associated with a particular vehicle. Rather, the reports will consist of 100 percent anonymized information using identification numbers that are not associated with a particular license plate or registered owner. The reports will provide only the date, time, location, approximate address, goBerkeley blockface ID, and RPP area in which a vehicle was observed. If a citation was not issued for an RPP or other time limit violation, the report may also provide the reason a parking enforcement

# **DEPARTMENTALORDER**

# ADMINISTRATIVE ORDER #001-2016

DATE ISSUED: 02/18/16

officer concluded there was no parking violation, e.g., RPP visitor pass, disabled placard or license plate, etc.

Michael K. Meehan Chief of Police

References: NCRIC ALPR Policy

SB 34

General Order R-23

Cc: All BPD Personnel



Policy Manual

# **Automated License Plate Readers (ALPRs)**

#### 422.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance for the capture, storage and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology.

#### 422.2 POLICY

The policy of the Berkeley Police Department is to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public.

All data and images gathered by the ALPR are for the official use of this department. Because such data may contain confidential information, it is not open to public review.

# 422.3 ADMINISTRATION

Any installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Investigations Division Captain. The Investigations Division Captain will assign members under his/her command to administer the day-to-day operation of the ALPR equipment and data.

## 422.3.1 ALPR ADMINISTRATOR

The Investigations Division Captain, or his/her designee, shall be responsible for developing guidelines and procedures to comply with the requirements of Civil Code § 1798.90.5 et seq. This includes, but is not limited to (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

- (a) A description of the job title or other designation of the members and independent contractors who are authorized to use or access the ALPR system or to collect ALPR information.
- (b) Training requirements for authorized users.
- (c) A description of how the ALPR system will be monitored to ensure the security of the information and compliance with applicable privacy laws.
- (d) Procedures for system operators to maintain records of access in compliance with Civil Code § 1798.90.52.
- (e) The title and name of the current designee in overseeing the ALPR operation.
- (f) Ensuring this policy and related procedures are conspicuously posted on the City's website.

# 422.4 OPERATIONS

Use of an ALPR is restricted to the purposes outlined below. Department members shall not use, or allow others to use the equipment or database records for any unauthorized purpose (Civil Code § 1798.90.51; Civil Code § 1798.90.53).

- (a) An ALPR shall only be used for official law enforcement business.
- (b) An ALPR may be used in conjunction with any routine patrol operation or criminal investigation. Reasonable suspicion or probable cause is not required before using an ALPR.
- (c) While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped cars to canvass areas around homicides, shootings and other major incidents. Partial license plates reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.
- (d) No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.
- (e) No ALPR operator may access California Law Enforcement Telecommunications System (CLETS) data unless otherwise authorized to do so.
- (f) If practicable, the officer should verify an ALPR response through the California Law CLETS before taking enforcement action that is based solely on an ALPR alert.

#### 422.5 DATA COLLECTION AND RETENTION

All data and images gathered by an ALPR are for the official use of the Berkeley Police Department. Such data may contain confidential CLETS information and is not open to public review. ALPR information gathered and retained by this department may be used and shared with prosecutors or other law enforcement agencies only as permitted by law.

The Investigations Division Captain, or his/her designee, is responsible for ensuring proper collection and retention of ALPR data.

Technical support and assistance for ALPR's is provided by the City of Berkeley's Department of Information Technology (IT) and associated ALPR system providers/vendors as identified herein. IT staff who do not have the proper clearance and training do not have the ability to access or view individual records or reports, as they may contain CLETS information they are not authorized to receive. IT provides initial infrastructure set-up, and continued systems support as needed to ensure efficient and accurate performance of the ALPR hardware and software. Only IT staff members who have successfully undergone DOJ background checks and training are authorized by the Chief of Police to view specific ALPR records.

All ALPR data downloaded to the server should be stored for a minimum of one year (Government Code § 34090.6) and in accordance with the established records retention schedule. Thereafter, ALPR data should be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a lawful action to produce records. In those circumstances the applicable data should be downloaded from the server onto portable media and booked into evidence.

(a) Collected images and metadata of hits will not be stored for more than 365 days. Metadata of reads will not be stored for more than 30 days. Images of reads will not be transferred to the server. (

#### 422.6 ACCOUNTABILITY

All saved data will be safeguarded and protected by both procedural and technological means. The Berkeley Police Department will observe the following safeguards regarding access to and use of stored data (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

- (a) Non-law enforcement requests for access to stored ALPR data shall be processed according to the Records Maintenance and Release Policy in accordance with applicable law.
- (b) Non-law enforcement requests for information regarding a specific vehicle's license plate may be honored when the requester is the registered owner of the vehicle in question, and when providing such information will not invade the privacy of a third party. The requestor in such cases must provide acceptable proof of his or her identity and of ownership of the vehicle in question.
- (c) All ALPR data downloaded to any workstation or server shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time (Civil Code § 1798.90.52).
- (d) Berkeley Police Department members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action or parking enforcement.
- (e) Aggregated ALPR data not related to specific criminal investigations shall not be released to any local, state or federal agency or entity without the express written consent of the City Manager.
- (f) Measures will be taken to ensure the accuracy of ALPR information. Errors discovered in ALPR data collected by ALPR units shall be marked, corrected or deleted in accordance with the type and severity of the error in question
- (g) ALPR system audits will be conducted by the Professional Standards Bureau's Audit and Inspections Sergeant on a regular basis, at least biannually.

For security or data breaches, see the Records Release and Maintenance Policy.

#### 422.7 RELEASING ALPR DATA

The ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law, using the following procedures:

- (a) The agency makes a written request for the ALPR data that includes:
  - The name of the agency.
  - 2. The name of the person requesting.
  - 3. The intended purpose of obtaining the information.

- (b) The request is reviewed by the Investigations Division Captain, or his/her designee, and approved before the request is fulfilled.
- (c) The approved request is retained on file.

Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Records Maintenance and Release Policy (Civil Code § 1798.90.55).

# 422.8 GENERAL PARKING AND SCOFFLAW ENFORCEMENT

The Berkeley Police Department's Parking Enforcement Unit utilizes vehicles equipped with ALPRs to conduct enforcement of posted time limits in commercial areas and Residential Preferential Parking (RPP) permit areas. These ALPR's also access information in the CLETS Stolen Vehicle System (SVS) database, which provides information on matches for stolen and wanted vehicles.

The Berkeley Police Department's Scofflaw Enforcement program (often referred to as the "booting" program) utilizes an ALPR to scan license plates, and check the scanned "reads" against a list of vehicles which have five or more outstanding parking citations exceeding 30 days old. Typically, upon a confirmed "hit," the vehicle is immobilized with a "boot", or towed, and the owner has to pay the outstanding citations and fees in order to release the boot and/or recover their car from storage. This allows the City to recover outstanding parking citation fees.

The contracted vendor for the City's Scofflaw Enforcement program is currently Paylock. Paylock stores data on a secure server, and provides access to authorized personnel via Paylock's "Bootview" secure website, as described below:

All data captured by the ALPR is stored on the booting vehicle's laptop for 30 days, and is only accessible during that period via the ALPR proprietary software. This includes reads, hits, and photographs associated with each.

When a car is booted and/or towed, the read, hit and photographic data relating to the booting and/or towing of scofflaw vehicles is uploaded to Paylock's secure server. No other data is uploaded to Paylock's secure server.

The contracted vendor for the City's Parking Enforcement ALPR is currently Genetec. The city uses Genetec ALPRs to support efficient enforcement of posted time limit parking and Residential Preferential Parking permits.

In addition, Genetec periodically provides reports to the City of Berkeley Transportation Division's "goBerkeley" parking management program so that the City's program can analyze data about parking demand. These reports do not contain any information about a vehicle's license plate number, the name of the registered owner, address of registered owner, or any other information gleaned from the license plate number associated with a particular vehicle. Rather, the reports consist of completely anonymized information, using identification numbers that are not associated with a particular license plate or registered owner.

The reports will provide only the date, time, location, approximate address, "goBerkeley" blockface ID, and Residential Permit Pass (RPP) area in which a vehicle was observed. If a citation was not issued for an RPP or other time limit violation, the report may also provide the reason a parking enforcement officer concluded there was no parking violation, e.g., RPP visitor pass, disabled placard or license plate, etc.

			C
	٠		1
			1
			Ç



June 12,2019 PRC meeting ent Agenda Item 9.6. Replaces pp. 15-20 in packet.

# **Missing Persons**

#### 316.1 PURPOSE AND SCOPE

This policy provides guidance for handling missing person investigations.

#### 316.1.1 DEFINITIONS

At risk - Includes, but is not limited to (Penal Code § 14215):

- A victim of a crime or foul play.
- A person missing and in need of medical attention.
- A missing person is age 11 or younger.
- A missing person with no pattern of running away or disappearing.
- A missing person who may be the victim of parental abduction.
- A mentally impaired missing person, including cognitively impaired or developmentally disabled.

**Missing person** - Any person who is reported missing to law enforcement when the person's location is unknown. This includes a child who has been taken, detained, concealed, enticed away or kept by a parent in violation of the law (Penal Code § 277 et seq.). It also includes any child who is missing voluntarily, involuntarily or under circumstances that do not conform to his/her ordinary habits or behavior, and who may be in need of assistance (Penal Code § 14215).

**Missing person networks** - Databases or computer networks available to law enforcement and that are suitable for information related to missing persons investigations. These include the National Crime Information Center (NCIC), the California Law Enforcement Telecommunications System (CLETS), and the Missing and Unidentified Person System (MUPS).

# 316.2 POLICY

The Berkeley Police Department does not consider any report of a missing person to be routine and assumes that the missing person is in need of immediate assistance until an investigation reveals otherwise. The Berkeley Police Department gives missing person cases priority over property-related cases and will not require any time frame to pass before beginning a missing person investigation (Penal Code § 14211).

# 316.3 REQUIRED FORMS AND BIOLOGICAL SAMPLE COLLECTION KITS

The <u>Detective Bureau Lieutenant</u>, or their designee, <u>Investigation supervisor</u> should <u>develop and make available</u> ensure the forms and <u>forms and kits are developed and available</u> in accordance with this policy, state law, federal law and the California Peace Officer Standards and Training (POST) Missing Persons Investigations guidelines, including:

Department report form for use in missing person cases

- Missing person investigation checklist that provides investigation guidelines and resources that could be helpful in the early hours of a missing person investigation (Penal Code § 13519.07)
- Missing person school notification form
- Medical records release form from the California Department of Justice
- California DOJ missing person forms as appropriate
- · Biological sample collection kits

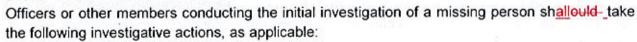
Dealth the Will M. S. Short ..

## 316.4 ACCEPTANCE OF REPORTS

Any member encountering a person who wishes to report a missing person or runaway shall render assistance without delay (Penal Code § 14211). This can be accomplished by accepting the report via telephone or in-person and initiating the investigation. Those members who do not take such reports or who are unable to render immediate assistance shall promptly dispatch or alert a member who can take the report.

A report shall be accepted in all cases and regardless of where the person was last seen, where the person resides or any other question of jurisdiction (Penal Code § 14211).

## 316.5 INITIAL INVESTIGATION



- (a) Respond to a dispatched call for service as soon as practicable.
- (b) Interview the reporting party and any witnesses to determine whether the person qualifies as a missing person and, if so, whether the person may be at risk.
- (c) Notify a supervisor immediately if there is evidence that a missing person is either at risk or may qualify for a public alert, or both (see the Public Alerts Policy).
- (e)(d) Broadcast a "Be on the Look-Out" (BOLO) bulletin if the person is under 21 years of age or there is evidence that the missing person is at risk. The BOLO should be broadcast as soon as practicable but in no event more than one hour after determining the missing person is under 21 years of age or may be at risk (Penal Code § 14211).
- (d)(e) Make Ensure that entries are made into the appropriate missing person networks as follows:
  - Immediately Within 2 hours of the initial report, when the missing person is under 21 years old or is considered at risk.
  - In all other cases, as soon as practicable, but not later than <u>fourtwo</u> hours from the time of <u>the officer's contact with the reporting party</u>. the initial report.
- (e)(f) Complete the appropriate report forms accurately and completely and initiate a search as applicable under the facts.
- (f)(g) Collect and/or review:
  - A photograph and a fingerprint card of the missing person, if available.



- 4.2. Any documents that may assist in the investigation, such as court orders regarding custody.
- 2.3. Any other evidence that may assist in the investigation, including personal electronic devices (e.g., cell phones, computers).
- (9)—When circumstances permit and if appropriate, attempt to determine the missing person's location through his/her telecommunications carrier.
- (h) Contact the appropriate agency if the report relates to a previously made missing person report and another agency is actively investigating that report. When this is not practical, the information should be documented in an appropriate report for transmission to the appropriate agency. If the information relates to an at-risk missing person, the member should notify a supervisor and proceed with reasonable steps to locate the missing person.

# 316.6 REPORT PROCEDURES AND ROUTING

Employees should complete all missing person reports and forms promptly and <u>submit them for supervisor approval.</u> advise the appropriate supervisor as soon as a missing person report is ready for review.

# 316.6.1 SUPERVISOR RESPONSIBILITIES

The responsibilities of the supervisor shall include, but are not limited to:

- (a) Reviewing and approving missing person reports upon receipt.
- (b) The reports should be promptly sent to the Records Management.
- (c)(b) Ensuring resources are deployed as appropriate.
- (d)(c) Initiating a command post as needed.
- (e)(d) Ensuring applicable notifications and public alerts\_-are made and documented-(Nixle, AMBER, etc., see Public Alerts Policy).
- (f)(e) Ensuring that records have been entered into the appropriate missing persons networks.
- (9)(f) Taking reasonable steps to identify and address any jurisdictional issues to ensure cooperation among agencies.

If the case falls within the jurisdiction of another agency, the supervisor should facilitate transfer of the case to the agency of jurisdiction.

#### 316.7 RECORDS MANAGEMENT RESPONSIBILITIES

The receiving member shall:

- (a) As soon as reasonable under the circumstances, notify and forward a copy of the report to the law enforcement agency having jurisdiction over the missing person's residence in cases where the missing person is a resident of another jurisdiction (Penal Code § 14211).
- (b) Notify and forward a copy of the report to the law enforcement agency in whose jurisdiction the missing person was last seen (Penal Code § 14211).

- (c) Notify and forward a copy of the report to the law enforcement agency having jurisdiction over the missing person's intended or possible destination, if known.\_
- (e)(d) Forward a copy of the report to the Detective Bureau.
- (d)(e)Coordinate with the NCIC Terminal Contractor for California to have the missing person record in the NCIC computer networks updated with additional information obtained from missing person investigations (42 USC § 5780).

# 316.8 FOLLOW UP TIMELINE

- (a) Adult Missing Person Cases: The initial assigned investigator handles the 24 hour and one week follow ups, then forwards the case to the Homicide Detail for follow up.
- (b) <u>Juvenile Missing Person/Runaway Cases: The initial assigned investigator handles the 24 hour follow up, then forwards the case to the Youth Services Detail for follow up.</u>

# 316.9 DETECTIVE FOLLOW UP

In addition to completing or continuing any actions listed above, the investigator assigned to a missing person investigation:

- (a) Shall ensure that the missing person's school is notified within 10 days if the missing person is a juvenile.
  - The notice shall be in writing and should also include a photograph (Education Code § 49068.6).
  - The investigator should meet with school officials regarding the notice as appropriate to stress the importance of including the notice in the juvenile's student file, along with contact information if the school receives a call requesting the transfer of the missing child's files to another school.
- (b) Should recontact the reporting person and/or other witnesses within 30 days of the initial report and within 30 days thereafter to determine if any additional information has become available via the reporting party.
- (c) Should consider contacting other agencies involved in the case to determine if any additional information is available.
- (d) Shall verify and update CLETS, NCIC and any other applicable missing person networks within 30 days of the original entry into the networks and every 30 days thereafter until the missing person is located (42 USC § 5780).
- (e) Should continue to make reasonable efforts to locate the missing person and document these efforts at least every 30 days.
- (f) Shall maintain a close liaison with state and local child welfare systems and the National Center for Missing and Exploited Children® (NCMEC) if the missing person is under the age of 21 and shall promptly notify NCMEC when the person is missing from a foster care family home or childcare institution (42 USC § 5780).
- (g) Should make appropriate inquiry with the <u>Coroner[Medical Examiner/JOP]</u>.

- (h) Should obtain and forward medical and dental records, photos, X-rays and biological samples pursuant to Penal Code § 14212 and Penal Code § 14250.
- (i) Shall attempt to obtain the most recent photograph for persons under 18 years of age if it has not previously been obtained and forward the photograph to California DOJ (Penal Code § 14210) and enter the photograph into applicable missing person networks (42 USC § 5780).
- Should consider making appropriate entries and searches in the National Missing and Unidentified Persons System (Namus MUPS).
- (k) In the case of an at-risk missing person or a person who has been missing for an extended time, should consult with a supervisor regarding seeking federal assistance from the FBI and the U.S. Marshals Service (28 USC § 586).

# 316.9316.10 WHEN A MISSING PERSON IS FOUND

When any person reported missing is found, the assigned investigator shall document the location of the missing person in the appropriate report, notify the relatives and/or reporting party, as appropriate, and other involved agencies and refer the case for additional investigation if warranted.

The <u>assigned investigator Public Safety Business Manager</u> shall ensure that, upon receipt of information that a missing person has been located, the following occurs (Penal Code § 14213):

- (a) Notification is made to California DOJThe person's name is removed from MUPS.
- (b) The missing person's school is notified, if applicable.
- (c) Entries are made in the applicable missing person networks.
- (d) Immediately notify the Attorney General's Office.
- (e)(c) Notification shall be made to any other law enforcement agency that took the initial report or participated in the investigation within 24 hours.

# 316.8.1 UNIDENTIFIED PERSONS

Department members investigating a case of an unidentified person who is deceased or a living person who cannot assist in identifying him/herself should:

- (a) Obtain a complete description of the person.
- (b) Enter the unidentified person's description into the NCIC Unidentified Person File.
- (c) Use available resources, such as those related to missing persons, to identify the person.

# 316.10316.11 CASE CLOSURE

The Detective Bureau <u>Lieutenant or his/her designee</u>, <u>supervisor</u> may authorize the closure of a missing person case after considering the following:

(a) Closure is appropriate when the missing person is confirmed returned or evidence has matched an unidentified person or body.

- (b) If the missing person is a resident of Berkeley or this department is the lead agency, the case should be kept under active investigation for as long as the person may still be alive. Exhaustion of leads in the investigation should not be a reason for closing a case.
- (c) If this department is not the lead agency, the case can be made inactivate if all investigative leads have been exhausted, the lead agency has been notified and entries are made in the applicable missing person networks as appropriate.
- (d) A missing person case should not be closed or reclassified because the person would have reached a certain age or adulthood or because the person is now the subject of a criminal or civil warrant.

# 316,11316,12 TRAINING

Subject to available resources, the Personnel and Training Sergeant should ensure that members of this department whose duties include missing person investigations and reports receive regular training that includes:

- (a) The initial investigation:
  - 1. Assessments and interviews
  - 2. Use of current resources, such as Mobile Audio Video (MAV)
  - 3. Confirming missing status and custody status of minors
  - Evaluating the need for a heightened response
  - 4. Identifying the zone of safety based on chronological age and developmental stage
- (c)(b) Briefing of department members at the scene.
- (d)(c) Identifying NCIC Missing Person File categories (e.g., disability, endangered, involuntary, juvenile and catastrophe).
- (e)(d) Verifying the accuracy of all descriptive information.
- (f)(e) Initiating a neighborhood investigation.
- (9)(f) Investigating any relevant recent family dynamics.
- (h)(g) Addressing conflicting information.
- (h) Key investigative and coordination steps.
- (i) Managing a missing person case.
- (k)(j) Additional resources and specialized services.
- (I) Update procedures for case information and descriptions.
- (m)(l) Preserving scenes.
- (n)(m)Internet and technology issues (e.g., Internet use, cell phone use).
- (o)(n) Media relations.



ACTION CALENDAR July 9, 2019

To:

Honorable Mayor and Members of the City Council

From:

Dee Williams-Ridley, City Manager

Submitted by: Kelly Wallace, Director, Health, Housing and Community Services

Department

Andrew Greenwood, Police Chief, Berkeley Police Department

Subject:

Companion Report: Law Enforcement Use of Restraint Devices in the City of

Berkeley

# RECOMMENDATION

Continue current policy to provide City of Berkeley Police and Fire personnel protection from individuals whose untawful and assaultive spitting or biting actions may spread infectious diseases during a lawful detention or arrest.

# FISCAL IMPACTS OF RECOMMENDATION

There is no fiscal impact to continue the existing policy.

A change in policy that prohibits the use of spit masks could result in increases in staff costs due to: (a) injuries and employee exposure to infectious disease and pathogens; (b) lost staff time; (c) overtime coverage costs; (d) Workers' Compensation claims; and (d) loss of police and city attorney staff time due to preparing and managing documentation supporting court orders to compel blood tests and report results to the affected officer.

# CURRENT SITUATION AND ITS EFFECTS

At its February 28, 2019 meeting, the Mental Health Commission unanimously passed a motion "to pass the spithood resolution and submit the resolution to the City Council for approval." At its April 25, 2019 meeting, the commission passed a motion to withdraw the previous resolution and replace it with one that prohibits law enforcement from using restraint devices such as spit hoods in the line of duty, and resolving that law enforcement shall only use their own N95 masks or an equivalent substitute in the line of duty.

The Commission did not request or receive any information or input from the Police or Fire Department during their consideration of this matter.

# BACKGROUND

Individuals who spit at or bite first responders pose a threat to public health. Risks from Aerosol Transmissible Diseases and from blood borne pathogens endanger all personnel involved in an incident in which responders are spat at or upon. Personnel use a soft mask "spit mask" to provide protection from infection. Spit masks are temporary protective devices designed to prevent the wearer from transferring or transmitting fluids (saliva and mucous) to others. The mask is made of a translucent fabric mesh which allows air and light to pass through, but blocks spittle.

Aerosol Transmissible Diseases (ATD) include but are not limited to Chickenpox, Shingles, Measles, Meningitis, Pneumonia and Tuberculosis. See Appendix A for the Stanford Environmental Health and Safety program's more comprehensive list of ATDs. Transmission of ATDs can occur when the pathogen leaves its reservoir (or host) through a portal of exit (mouth/nose), is conveyed by some mode of transmission (spit/droplet), and enters through an appropriate portal of entry to infect a susceptible host. This sequence is sometimes called the chain of infection (Center for Disease Control). If there is blood in the mouth, the saliva can also contain blood-borne pathogens. These include, but are not limited to, hepatitis B (HBV), hepatitis C (HCV) and human immunodeficiency virus (HIV). Appendix B provides further information from the Occupational Health and Safety Administration (OSHA).

It is an unfortunate fact that Police and Fire personnel at times encounter individuals who—for whatever reason—spit at, spit on, bite, or otherwise assault City personnel. These behaviors may occur for a variety of reasons: deliberate assaultive behavior, a loss of temper, drug and/or alcohol intoxication, an aftered mental status due to a medical emergency, or a result of mental illness. Regardless of the underlying reason for the behavior, the behavior creates a risk for responding personnel, and the need to mitigate this risk and keep staff safe through the spit mask.

Masks provide the most effective method of managing the risk of exposure and safeguarding employee health. Donning N95 masks and eye protection as proposed by the Mental Health Commission does not provide adequate protection to staff from individuals spitting at or upon them. N-95 masks and eye protection cover only a portion of the face. Droplets from an individual actively spitting can easily make their way to an entry point like the eyes through gaps that exist between goggles and the face. N-95 masks and goggles are impractical to carry and unwieldy to put on, and are easily dislodged or knocked off when a person is combative. If there are any cuts, abrasions or punctures to the exposed skin of a first responder, pathogens can make entry. Spit and mucous on the skin, clothing and uniforms or other surfaces can spread disease at a later time. Droplets that contain pathogens remain on surfaces after the individual has been removed from the scene; these can spread disease for up to four days. The use of masks allow first responders to humanely and safely break the chain of infection. The mask mitigates the spread of pathogens by containing them within the mask, and thereby disallowing them from infecting a susceptible host, e.g. first

responder. The mask also prevents the collateral impact of spit and mucous on surfaces and clothing, where disease can spread to anyone who comes in contact with it for up to several days depending on the disease.

Masks have been in use by Berkeley Police and Fire Department personnel to protect themselves and the community for over a decade. Use of the mask is governed by Berkeley Police Policy #302, attached. Police use approved masks only "when the officer reasonably believes the person will spit, either on a person or in an inappropriate place." When a mask is used, a first responder is present at all times to monitor airway and mental status. Policy requires the mask to be removed if the subject vomits, is bleeding profusely from the mouth, or has difficulty breathing.

# Avoidance of Injury, Assault and Workers Compensation Claims

It is a violation of California Penal Code to spit at, spit on, or bite anyone, including police, fire and EMS personnel. Additional criminal charges may be sought if someone knowingly and intentionally inflicts an infectious or communicable disease onto another person (California Health & Safety Code Section 120290). Preventing individuals from committing criminal acts, especially if they are in a mental crisis, is a legitimate function of law enforcement. Use of a mask prevents these acts.

An incident wherein an officer is exposed to disease or pathogens can trigger a considerable post-event administrative process. Every officer who is spat upon may complete an injury report, and their supervisor completes a supervisor's report. These reports include a comments on injury prevention, and the application of a mask will likely be the first listed action that could have been taken to prevent injury. A separate City of Berkeley "Exposure" Report is completed. Employees may file a Worker's Compensation Claim if a pathogen is transmitted. Officers may seek medical treatment and lose time from work due to treatment. Depending on the nature and seriousness of the exposure, the officer may also seek a court order compelling the subject to provide a blood sample for testing at a medical facility, to disclose the presence of Infectious disease, so that the impacted employee and their physician can make informed decisions regarding treatment and care. These are significant and time-consuming processes, and can be impactful upon employees whose health the City is charged with protecting.

Staff agrees with the Mental Health Commission, in that Berkeley police officers are well-trained to deal with situations where people are in crisis. However, regardless of the reason for the behavior, when an individual spits at or upon officers, they are committing a crime and potentially spreading pathogens. The City has an obligation to enforce the law, provide working conditions for first responders that minimize the risk of illness and injury, and reduce the chances of disease transmission to its staff and community members.

# ENVIRONMENTAL SUSTAINABILITY

Not applicable

# RATIONALE FOR RECOMMENDATION

The City's current use of masks is well-governed by existing policy. Masks are considered best practice by law enforcement, fire personnel and EMS for use when individuals spit at or bite them in the field. Masks are used in these situations by Berkeley Police Officers, Berkeley Firefighters, Berkeley Paramedics and EMS mutual aid providers from neighboring Cities and the county's private transport provider.

# ALTERNATIVE ACTIONS CONSIDERED

N-95 masks and eye protection were considered but for reasons outlined in report, not recommended.

# CONTACT PERSON

[Name], [Title], [Department], [Phone Number]

Attachments: [Delete if there are NO Attachments]

1: (Title or Description of Attachment)

2: [Title or Description of Attachment]

# $1'_{-1}.1$

# Aerosol Transmissible Diseases/Pathogens

Below you'll find a list of diseases and pathogens which are to be considered aerosol transmissible pathogens or diseases for the purpose of 8 CCR 5199. Employers are required to provide the protections required by 8CCR 5199 according to whether the disease or pathogen requires airborne infection isolation or droplet precautions as indicated by the two lists below.

# Diseases/Pathogens Requiring Airborne Infection Isolation

- Aerosolizable spore-containing powder or other substance that is capable of causing serious human disease, e.g. Anthrax/Bacillus anthracis
- Avian influenza/Avian influenza A viruses (strains capable of causing serious disease in humans)
- Varicella disease (chickenpox, shingles)/Varicella zoster and Herpes zoster viruses, disseminated disease in any patient.
   Localized disease in immunocompromised patient until disseminated infection ruled out
- Measles (rubeola)/Measles virus
- Monkeypox/Monkeypox virus
- Novel or unknown pathogens
- "evere acute respiratory syndrome (SARS)
- amallpox (variola)/Varioloa virus
- Tuberculosis (TB)/ Mycobacterium tuberculosis-Extrapulmonary, draining lesion; Pulmonary or laryngeal disease, confirmed; Pulmonary or laryngeal disease, suspected
- Any other disease for which public health guidelines recommend airborne infection isolation

# Diseases/Pathogens Requiring Droplet Precautions

- Diphtheria pharyngeal
- Epiglottitis, due to Haemophilus influenzae type b
- Haemophilus influenzae Serotype b (Hib) disease/Haemophilus influenzae serotype b-Infants and children
- Influenza, human (typical seasonal variations)/influenza viruses
- Meningitis
  - Haemophilus influenzae, type b known or suspected
  - · Neisseria meningitidis (meningococcal) known or suspected
- Meningococcal disease sepsis, pneumonia (see also meningitis)
- Mumps (infectious parotitis)/Mumps virus
- Mycoplasmal pneumonia.
- Parvovirus B19 infection (erythema infectiosum)
- Pertussis (whooping cough)
- Pharyngitis in infants and young children/Adenovirus, Orthomyxoviridae, Epstein-Barr virus, Herpes simplex virus
- .1eumonia
  - Adenovirus
  - Haemophilus influenzae Serotype b, infants and children

- Meningococcal
- · Mycoplasma, primary atypical
- Streptococcus Group A
- Pneumonic plague/Yersinia pestis
- Rubella virus infection (German measles)/Rubella virus
- Severe acute respiratory syndrome (SARS)
- Streptococcal disease (group A streptococcus)
  - Skin, wound or burn, Major
  - · Pharyngitis in infants and young children
  - Pneumonia
  - · Scarlet fever in infants and young children
  - · Serious invasive disease
- Viral hemorrhagic fevers due to Lassa, Ebola, Marburg, Crimean-Congo fever viruses (airborne infection isolation and respirator use may be required for aerosol-generating procedures)
- Any other disease for which public health guidelines recommend droplet precautions

# CHAPTER LISTING

Additional Resources

- 11.1 Aerosol Transmissible Diseases/Pathogens
- 11.2 Aerosol Transmissible Pathogens Laboratory
- 11.3 Aerosol Transmissible Disease Vaccination Recommendations for Susceptible Health Care Workers
- 11.4 Resources

# UNITED STATES DEPARTMENT OF LABOR

APC9

English | Spanish

Find It in OSHA

Q

A TO Z INDEX

OSHA \* WORKER \* EMPLOYER \* STANDARDS \* ENFORCEMENT \* CONSTRUCTION TOPIC \* NEWS/RESOURCES \* DATA \* TRAINING \*

Safety and Health Topics / Bloodborne Pathogens and Needlestick Prevention

# Bloodborne Pathogens and Needlestick Prevention

Bloodborne Pathogens Menu

# Overview

What are bloodborne pathogens?

Bloodborne pathogens are infectious microorganisms in human blood that can cause disease in humans. These pathogens include, but are not limited to, hepatitis B (HBV), hepatitis C (HCV) and human Immunodeficiency virus (HIV). Needlesticks and other sharps-related injuries may expose workers to bloodborne pathogens. Workers in many occupations, including first responders, housekeeping personnel in some industries, nurses and other healthcare personnel, all may be at risk for exposure to bloodborne pathogens.

What can be done to control exposure to bloodborne pathogens?

In order to reduce or eliminate the hazards of occupational exposure to bloodborne pathogens, an employer must implement an exposure control plan for the worksite with details on employee protection measures. The plan must also describe how an employer will use engineering and work practice controls, personal protective clothing and equipment, employee training, medical surveillance, hepatitis B vaccinations, and other provisions as required by OSHA's Bloodborne Pathogens Standard (29 CFR 1910.1030). Engineering controls are the primary means of eliminating or minimizing employee exposure and include the use of safer medical devices, such as needleless devices, shielded needle devices, and plastic capillary tubes.

General Guidance	Enforcement	Hazard
Provides information on the revised standard.	Highlights directives and letters	Recognition
More >	of interpretation related to bloodborne pathogens and needlestick prevention.	Provides references that aid in recognizing workplace hazards associated with bloodborne
	Moxe >	pathogens.
		More >
Evaluating and	Standards	Additional
Controlling	Bloodborne pathogens and	Resources

Evaluating and	Standards	Additional		
-	Standards	Additional		
Controlling	Bloodborne pathogens and	Resources		
Exposure	needlesticks are addressed in specific OSHA standards for	Provides links and references to additional resources related to bloodborne pathogens and		
Provides information for	general industry.			
evaluating and controlling bloodborne pathogens and	More >	needlestick prevention.		
needlestick hazards.		More >		
More >				

Workers' Rights

#### Workers have the right to:

- Working conditions that do not pose a risk of serious harm.
- Receive information and training (in a language and vocabulary the worker understands) about workplace hazards, methods to prevent them, and the OSHA standards that apply to their workplace.
- Review records of work-related injuries and illnesses.
- Fite a complaint asking OSHA to inspect their workplace if they believe there is a serious hazard or that their employer is not following OSHA's rules. OSHA will keep all identities confidential.
- Exercise their rights under the law without retallation, including reporting an injury or raising health and safety concerns with their employer or OSHA. If a worker has been retallated against for using their rights, they must file a complaint with OSHA as soon as possible, but no later than 30 days.

For additional information, see OSHA's Workers page.

#### How to Contact OSHA

Under the Occupational Safety and Health Act of 1970, employers are responsible for providing safe and healthful workplaces for their employees. OSHA's role is to ensure these conditions for America's working men and women by setting and enforcing standards, and providing training, education and assistance. For more information, visit www.osha.gov or call OSHA at 1-800-321-OSHA (6742), TTY 1-877-889-5627.

# CAUTIONS

If you are stuck by a needle or other sharp or get blood or other potentially infectious materials in your eyes, nose, mouth, or on broken skin, immediately flood the exposed area with water and clean any wound with soop and water or a skin disinfectant if svallable. Report this immediately to your employer and seek immediate medical attention.

CDC: Emergency Meedlestick Information also provides immediate access to treatment protocols following blood exposures involving HIV, HBV and HCV, including the Clinicians' Post Exposure Prophylaxis Hotline (PEPline) at 1-888-448-4911.





OSHA's Ebola webpage provides a comprehensive source of Information for protecting workers from exposure to the Ebola virus.

# Highlights

- Most Frequently Asked Questions Concerning the Bloodborne Pathogens Standard
- Quick Reference Guide to the Bloodborne Pathogens Standard
- Comparison of Universal Precautions, Standard Precautions, and Transmission-based Precautions
- FDA, NIOSH and OSHA Joint Safety Communication on Blunt-Tip Surgical Suture Needles. (May 30, 2012).

# Related Topics

- Dentistry
- Healthcare
- Medical and First Ald
- Nursing Homes and Personal Care Facilities

# UNITED STATES CEPVET 480T OF LABOR

Occupational Safety and Health Administration 200 Constitution Ave NW Washington, DC 20210 \$\infty\$ 800-321-6742 (OSHA) TTY www.OSHA.gov

# **FEDERAL GOVERNMENT**

White House
Severe Storm and Flood Recovery Assistance
Disaster Recovery Assistance
DisasterAssistance.gov
USA.gov
No Fear Act Data
U.S. Office of Special Counsel

#### OCCUPATIONAL SAFETY AND HEALTH

Frequently Asked Questions
A - Z Index
Freedom of Information Act
Read the OSHA Newsletter
Subscribe to the OSHA Newsletter
OSHA Publications
Office of Inspector General

# **ABOUT THE SITE**

Freedom of Information Act Privacy & Security Statement Disclaimers Important Website Notices Plug-Ins Used by DOL Accessibility Statement

Law Enforcement Services Manual

# Handcuffing and Restraints

#### 302.1 PURPOSE AND SCOPE

This policy provides guidelines for the use of handcuffs and other restraints during detentions and arrests.

#### 302.2 POLICY

The Berkeley Police Department authorizes the use of restraint devices in accordance with this policy, the Use of Force Policy and department training. Restraint devices shall not be used to punish, to display authority or as a show of force.

#### 302.3 RESTRAINTS

# 302.3.1 USE OF RESTRAINTS

Only members who have successfully completed Berkeley Police Department approved training on the use of restraint devices described in this policy are authorized to use these devices.

When deciding whether to use any restraint, officers should carefully balance officer safety concerns with factors that include, but are not limited to:

- (a) The circumstances or crime leading to the arrest.
- (b) The demeanor and behavior of the arrested person.
- (c) The age and health of the person.
- (d) Whether the person may be pregnant.
- (e) Whether the person has a hearing or speaking disability. In such cases, consideration should be given, safety permitting, to handcuffing to the front in order to allow the person to sign or write notes.
- (f) Whether the person has any other apparent disability.

#### 302.3.2 RESTRAINT OF DETAINEES

Situations may arise where it may be reasonable to restrain an individual who may, after brief investigation, be released without arrest. Unless arrested, the use of restraints on detainees should continue only for as long as is reasonably necessary to assure the safety of officers and others. When deciding whether to remove restraints from a detainee, officers should continuously weigh the safety interests at hand against the continuing intrusion upon the detainee.

#### 302.3.3 ALTERNATIVE MEANS OF RESTRAINT

Alternative Means of Restraint include but are not limited to:

- (a) Handcuffing the person with their hands in front of their body.
- (b) Handcuffing the person with multiple sets of linked handcuffs.
- (c) Use of the entire WRAP system.

Law Enforcement Services Manual

# Handcuffing and Restraints

- (d) Use of the WRAP's ankle strap
- (e) Use of plastic handcuffs, aka "flex cuffs"
- (f) Use of an ambulance gurney with five point straps

# 302.3.4 RESTRAINT OF PREGNANT PERSONS

If a person's hands cannot be restrained behind their back because of pregnancy, officers will attempt to accommodate the person's condition by using alternative means of restraint.

No person who is in labor, delivery or recovery after delivery shall be handcuffed or restrained except in extraordinary circumstances and only when a supervisor makes an individualized determination that such restraints are necessary for the safety of the arrestee, officers or others (Penal Code § 3407; Penal Code § 6030).

# 302,3,5 RESTRAINT OF JUVENILES

A juvenile under 14 years of age should not be restrained unless he/she is suspected of a dangerous felony or when the officer has a reasonable suspicion that the juvenile may resist, attempt escape, injure him/herself, injure the officer or damage property.

## 302.3.6 NOTIFICATIONS

Whenever an officer transports a person with the use of restraints other than handcuffs, the officer shall inform the jail staff upon arrival at the jail that restraints were used. This notification should include information regarding any other circumstances the officer reasonably believes would be potential safety concerns or medical risks to the subject (e.g., prolonged struggle, extreme agitation, impaired respiration) that may have occurred prior to, or during transportation to the jail.

# 302.4 APPLICATION OF HANDCUFFS OR PLASTIC CUFFS

Handcuffs, including temporary plastic flex cuffs, may be used only to restrain a person's hands to ensure officer safety.

Although recommended for most arrest situations, handcuffing is not an absolute requirement of the Department. Officers should consider handcuffing any person they reasonably believe warrants that degree of restraint. However, officers should not conclude that regardless of the circumstances, every person should be handcuffed.

In most situations handcuffs should be applied with the hands behind the person's back. When feasible, handcuffs should be applied between the base of the palm and the ulna bone of the wrist. When feasible, handcuffs should be double-locked to prevent tightening, which may cause undue discomfort or injury to the hands or wrists.

In situations where one pair of handcuffs does not appear sufficient to restrain the individual or may cause unreasonable discomfort due to the person's size, officers should consider alternative means of restraint.

Law Enforcement Services Manual

# Handcuffing and Restraints

If the person being handcuffed is on the ground or in a prone position, then as soon as possible after being handcuffed, the person should be placed in an upright sitting position or on their side for respiratory recovery and to mitigate the potential for positional asphyxia,

Handcuffs should be removed as soon as it is reasonable to do so or after the person has been searched and is safely confined within a detention facility.

#### 302.5 APPLICATION OF SPIT MASKS

Spit masks are temporary protective devices designed to prevent the wearer from transferring or transmitting fluids (saliva and mucous) to others.

Spit masks may be placed upon persons in custody when the officer reasonably believes the person will spit, either on a person or in an inappropriate place. They are generally used during application of a physical restraint, while the person is restrained, or during or after transport.

Officers utilizing spit masks should ensure that the spit mask is applied properly to allow for adequate ventilation and that the restrained person can breathe normally. Officers should provide assistance during the movement of restrained individuals due to the potential for impaired or distorted vision on the part of the individual. Officers should avoid co-mingling individuals wearing spit masks with other detainees.

Spit masks should not be used in situations where the restrained person is bleeding profusely from the area around the mouth or nose, or if there are indications that the person has a medical condition, such as difficulty breathing or vomiting. In such cases, prompt medical care should be obtained. If the person vomits while wearing a spit mask, the splt mask should be promptly removed and discarded. Persons who have been sprayed with oleoresin capsicum (OC) spray should be thoroughly decontaminated, including hair, head and clothing prior to application of a spit mask.

Those who have been placed in a spit mask should be continually monitored and shall not be left unattended until the spit mask is removed. Spit masks shall be discarded after each use.

## 302.6 APPLICATION OF THE WRAP

The WRAP is a temporary restraining device comprised of a veloro strapped leg panel, torso harness, ankle strap and backside handcuff carabiner. The device immobilizes the body into a straight-legged seated position. Used properly, it restricts a subject's ability to do harm to oneself or others. Officer safety is enhanced and the risk of injury to the subject is reduced.

In determining whether to use the WRAP, officers should consider:

- (a) Whether the officer or others could be exposed to injury due to the assaultive or resistant behavior of a suspect.
- (b) Whether it is reasonably necessary to protect the suspect from his/her own actions (e.g., running away from the arresting officer white handcuffed, kicking at objects or officers).

Law Enforcement Services Manual

# Handcuffing and Restraints

- (c) Whether It is reasonably necessary to avoid damage to property (e.g., kicking at windows of the patrol unit).
- (d) Whether conventional methods of restraint have failed.

# 302.6.1 GUIDELINES FOR USE OF THE WRAP

When applying the WRAP, the following guidelines should be followed:

- (a) If practicable, officers should notify a supervisor of the intent to apply the WRAP. In all cases, a supervisor shall be notified as soon as practicable after the application of the WRAP.
- (b) Once applied, absent a medical or other emergency, restraints should remain in place until the officer arrives at the jail or other facility or the person no longer reasonably appears to pose a threat. Restraint straps should be checked frequently for tightness, and adjusted as necessary, until the WRAP is removed. The harness straps should never be tightened to the point they interfere with the person's ability to breath.
- (c) The restrained person should be continually monitored by an officer while the WRAP is in use. The officer should ensure that the person does not roll onto and remain on his/her stomach:
- (d) The officer should look for signs of distress such as sudden quiet or inactivity, complaints of chest pain, change in facial color, complaint of extreme heat, vomiting, and/or labored breathing, and take appropriate steps to relieve and minimize any obvious factors contributing to this condition.
- (e) Movement of the person can be accomplished in three ways, depending on the level of their cooperation. The person can be carried, allowed to stand and shuffle walk or be transported in a vehicle.
- (f) Once secured, the person should be placed in a seated or upright position, secured with a seat belt, and shall not be placed on his/her stomach for an extended period, as this could reduce the person's ability to breathe.
- (g) If in custody and transported by ambulance/paramedic unit, the restrained person should be accompanied by an officer when requested by medical personnel. The transporting officer should describe to medical personnel any unusual behaviors or other circumstances the officer reasonably believes would be potential safety or medical risks to the subject (e.g., prolonged struggle, extreme agitation, impaired respiration).

# 302.6.2 DEVICE REMOVAL

Based on the prisoner's combativeness or level of aggression, officers should employ appropriate control techniques and tactics when removing restraint devices.

# 302.6.3 THE ANKLE STRAP

The ankle strap is one part of the WRAP restraint system. The ankle strap may be used alone, without the rest of the WRAP system to restrain the legs of a violent or potentially violent person when it is reasonable to do so during the course of detention, arrest or transportation. Use of the ankle strap should follow the same considerations listed in 302.6 and guidelines listed in 302.6.1.

Law Enforcement Services Manual

# Handcuffing and Restraints

# 302.7 APPLICATION OF AUXILIARY RESTRAINT DEVICES

Auxiliary restraint devices include transport belts, waist or belty chains, transportation chains, legingers and other similar devices. Auxiliary restraint devices are intended for use during long-term restraint or transportation. They provide additional security and safety without impeding breathing, while permitting adequate movement, comfort and mobility.

Only department-authorized devices may be used. Any person in auxiliary restraints should be monitored as reasonably appears necessary.

# 302.8 REQUIRED DOCUMENTATION

If an individual is restrained and released without an arrest, the officer shall document the details of the detention and the need for handcuffs or other restraints in an MDT, incident or case report.

If an individual is arrested, the use of restraints other than handcuffs shall be documented in the related report. The officer should include, as appropriate:

- (a) How the suspect was transported and the position of the suspect.
- (b) Observations of the suspect's behavior and any signs of physiological problems.
- (c) Any known or suspected drug use or other medical problems.



June 4, 2019

To: A. Greenwood, Chief of Police

From: Kevin Walker, Occupational Health and Safety Officer

City of Berkeley Human Resources Department

Re: Occupational Safety Perspectives; Consequences of Bites, Exposure

The information presented below is from an occupational safety perspective for protection against human bites. It examines consequences of exposures to human bites and fluids and considers the potential outcomes and the use of protective measures.

Human saliva is known to contain as many as 50 species of bacteria with almost 10<sup>8</sup> microbes/ml. The reason these injuries are so prone to infection is that, for example, the extensor tendon and the Metacarpophalangeal (MCP) joints of the hands are relatively avascular structures and thus have a very limited ability to fight infection. This is one of the reasons why human bites are believed to have higher rates of infection than other injuries. Medical attention for bite injury ranges in cost from the relatively low cost first aid, to the extremely high cost of surgical repair and recovery.

A search of medical literature revealed studies that document the seriousness of human. bites and infection. In a multicenter study of infected human bites 50 patients were studied and four cultures, including one anaerobic culture, were obtained from each patient, it was discovered that aerobic species alone were isolated in 44% of the wounds, anaerobes alone were isolated in 2% and both aerobes and anaerobes were isolated in 54% of the wounds.<sup>2</sup> The most common aerobic isolates were Streptococcus, Staphylococcus and Eikenella species. Streptococcus anginosus was the most common pathogen isolated and was found to contaminate 52% of human bites. Exposure to saliva alone is not considered a risk factor for viral transmission. although HIV may be present in the saliva (infrequently and at low levels). Salivary inhibitors render the virus non-infective in a majority of the cases,3 Therefore, transmission of HIV is a risk when there is blood in the mouth of the person who bites and there is a breach in the skin of the victim.4 Also, it is not uncommon for individuals to bite the inside of their cheek, lips or tongue to create a mouth full of blood as a weapon against officers. While the infectious nature of saliva/spittle can be debated, the infectious potential of blood cannot be challenged.



Human Resources Department

Human bites generate sufficient force to damage subcutaneous tissues and structures including muscle, nerves and ligaments. Bite wounds are serious because of the potential of infection and mechanical damage. The human bite has been measured to generate at a maximum of 265 psi which is enough to severely damage soft tissues. A bite that removes flesh creates a serious injury requiring surgery. One bite to the eye can easily result in blindness or other disabling injury.

We have to consider the cost of a bite. A human bite injury can be life-changing for an employee and can result in significant cost to the City. A City of Berkeley patrol officer sustained a severe bite injury that caused damaged nerves and severed tendons, required considerable surgery and infection control and even after medical intervention ultimately resulted in disability, including loss of dexterity and sensation to fingers and permanent loss of functional grip strength. As a result of that incident alone, the City paid over \$245,000.00 in workers compensation cost.

It is important that the City continue to provide officers with access to tools to safely carry out their job as well as protect lives.

Optimization and utilization of law enforcement tools is foundational in BPD's training program to protect the public and officers as well as control cost. Although the likelihood is small that a single exposure to bodily fluids or from splt will result in contracting a disease, we have to keep in mind that our officers are likely to experience multiple exposure to bodily fluids from spltting, saliva and blood throughout their career, so use of tools to minimize exposure during the multitude of interactions with the public is vital.

Unlike chemicals and hazardous materials, there are no time-weighted averages set by regulatory agencies (Cal OSHA, NIOSH, and ACGIH) on exposures to disease causing microorganisms. Thus, universal precautions are exercised, vaccinations are administered, sanitization methods are carried out and protective equipment are employed to prevent and reduce the potential of exposures. The Spit Hood is a pragmatic protective device that prevents exposures to pathogens and averts costly injuries. To discontinue its use will elevate the risk of catastrophic injuries among the City's emergency services personnel.



# References:

- A.Perron AD, Miller MD, Brady WJ. Orthopedic pitfalls in the ED: Fight bite, Am J Emerg Med 2002;20:114-7
- Talan DA, Abrahamian FM, Moran GJ, Citron DM, Tan JO, Goldstein EJ, et al. Clinical presentation and bacteriologic analysis of infected human bites in patients presenting to emergency departments. Clin Infect Dis. 2003;37:1481–9
- 3. Richman KM, Rickman LS. The potential for transmission of human immunodeficiency virus through human bites. J Acquir Immune Defic Syndr. 1993;6:402–6
- Smoot EC, Choucino CM, Smoot MZ. Assessing risks of human immunodeficiency virus transmission by human bite injuries. Plast Reconstr Surg. 2006;117:2538–9