	ROSENBERG POLICE DEPARTMENT	
	General Order 5.04 Body Worn Cameras and Other Electronic Equipment Usage	
	Effective Date: 02-27-2025	**Replaces: N/A**
	Approved:  Chief of Police	
	Reference: TBP 7.36	

I. POLICY

It is the policy of this department to ensure proper use of electronic computing and recording systems by establishing authorized uses and users; establishing protocols for storage, security, and retention; and prohibiting inappropriate uses of such equipment.

II. PURPOSE

To define and provide clear direction for the use and prohibited uses of department electronic computing and recording equipment, to provide for data security and retention periods, and to establish protocols for proper handling of digital evidence.

III. DEFINITIONS

Network Terminals – desktop, laptop, or other computers which connect to the department internal computer network.

Mobile Phones – Either department owned or personally owned cell phones or smart phones.

Mobile Video Recording – In-vehicle camera systems which are permanently mounted in department vehicles.

Body Worn Camera (BWC) – Officer worn digital audio or video recording device.

Digital Camera – a single purpose handheld camera designed to take digital photographs of scenes.

Automated License Plate Reader (ALPR) – Digital camera system that identifies and captures license plate numbers and locations.

Private Space – a location in which a person has a reasonable expectation of privacy, including a person's home.

Voluminous Request – includes:

1. A request for BWC recordings from more than five separate incidents,

2. More than five separate requests from the same person in a 24 hour period, or

3. A request(s) from the same person in a 24 hour period that constitute more than five total hours of video.

IV. PROCEDURES

The sections below define the procedures to be used and specific prohibitions regarding the use of specific equipment.

A. General Provisions

1. Any electronic documents, reports, audio or video recordings, images, emails, voice communications, and any other form of electronic data that is created while on or off duty, that is directly related to official department operations or investigations, whether created on personal or department owned equipment is considered a government record, is subject to public record laws, and must be preserved accordingly.

2. Any electronic documents, reports, audio or video recordings, images, emails, voice communications, and any other form of electronic data that is created while on or off duty, that is created on department owned equipment may be considered a government record, and may be reviewed and preserved if required. All department owned equipment and its use is subject to routine or specific review and/or investigation by department supervisors as needed to ensure appropriate use.

3. Use of personal electronic devices such as mobile phones and mobile phone cameras, for strictly personal use, not related to department operations while on-duty, is generally considered private unless the information would tend to show inappropriate activity. Off duty use of personal electronic devices is also generally considered private, unless the use results in a violation of department general orders or law.

4. In all cases where a formal departmental report (offense, incident, or use of force) is required and any form of digital evidence exists, the reporting officer will note that digital evidence exists in the report and identify the type of evidence and storage location.

5. Officers must review any recordings related to an incident involving them before being required to provide a statement about the incident.

B. General Prohibitions

1. Employees will not release, share, create or make copies of any electronic documents, reports, audio or video recordings, images, emails, voice communications, and any other form of electronic data that is created while

on or off duty, that is directly related to official department operations or investigations, whether created on personal or department owned equipment, unless specifically authorized by this order or the Chief of Police.

2. Employees will not use department owned equipment, electronic or otherwise, for personal benefit or to conduct personal business. Employees are allowed to use internet access for personal use during meal and other breaks, as long as the sites accessed are appropriate for public viewing. No video games will be played on department equipment or inappropriate websites visited.

3. Employees are reminded of their obligations under the department general orders and law. Inappropriate use of electronic devices or the release or posting of inappropriate, another parties private information, or governmental information usually deemed private, on the internet or various social media sites can lead to Internal Investigations and subsequent disciplinary action. Officers can also be questioned about these activities by defense counsels in criminal trials, potentially damaging the officer's credibility as a witness.

V. Body-Worn Cameras (Digital Audio/Video Recorders)

A. Department Issued Body-Worn Cameras (BWC)

1. These procedures do not apply to mounted in-vehicle audio/video systems covered elsewhere in the General Orders.

2. All digital multimedia evidence that is captured during the scope of an officer's duties is the property of the department and shall not be converted or copied for personal use. Accessing, copying, editing, erasing, or releasing recordings or depictions of recordings without proper approval is prohibited and subject to disciplinary action.

3. OFFENSE: Occupations Code 1701.659
   a. A peace officer or other employee of a law enforcement agency commits an offense if the officer or employee releases a recording created with a body worn camera under this subchapter without permission of the applicable law enforcement agency.
   b. An offense under this subchapter is a Class A Misdemeanor.

4. The Chief of Police will designate an individual to manage the receipt and storage of BWC data. The manager will routinely save data as necessary to long term storage media. Data not identified as necessary will be deleted after 90 days.

5. Officers issued a Body-Worn Camera shall use the device as required below.

B. Usage required by uniformed officers assigned to Patrol and Community Relations Divisions:

1. During any citizen contact outside the officer's vehicle.

2. During any interview with a victim, witness, or suspect.

3. During any field or eyewitness identification.

4. During any enforcement contact when outside the officer's vehicle.

5. During building searches, and alarm responses.

6. If activated for any of the above reasons, the recording shall continue until the conclusion of the incident, the officer has left the scene, or a supervisor has authorized (verbally) that a recording may cease. Should approval be given to cease the recording, the officer will state the reasons why the recording is being stopped and the name of the supervisor that granted the approval prior to deactivation.

C. Usage required by officers or detectives assigned to the Criminal Investigations Division, Operations Division, or any other plain clothes assignments.

1. When conducting photo arrays outside of an interview room setting.
2. During follow-up investigations where contact is expected and/or made with a victim, suspect, or witness. An audio recording device is acceptable when wearing the BWC is impracticable.
3. During special operations or surveillance activities, the BWC should be kept readily available, should enforcement action become necessary.
4. During any uniformed assignments or extra employment, employees shall adhere to the BWC usage requirements listed for uniformed officers.

D. Prohibitions

1. Officers shall not intentionally create digital recordings of other employees during routine, non-enforcement-related activities unless the recording is required by a court order or is authorized as part of an administrative or criminal investigation.

2. Officers shall not intentionally create digital recordings of activities in areas where a reasonable expectation of privacy exists, unless the recording is made while the officer is legally in the area due to section B above.

3. Officers shall not knowingly record undercover officers or confidential informants.

4. Officer shall not record strip searches.

5. Officers shalt not record conversations with other agency personnel that involve tactics or strategy that could compromise the safety of the officers or the public.

6. Officers shall not use a departmental device to record any personal activities.

7. Officers shall not allow any non-sworn personnel to view the recorded data without the permission of the officer's supervisor.

8. Uploading of any data to any social media sites is prohibited.

9. Officers will not wear privately owned body-worn cameras while on duty.

E. Officer Responsibilities

1. Officers issued a department owned body-worn camera shall attend training and demonstrate proficiency with the recording and transfer of recorded data.

2. Any other personnel who will come into contact with video and audio data obtained from the use of a BWC shall attend training.

3. Officers shall inspect the device at the beginning of each shift to ensure proper operation, including sufficient battery life and recording medium.
    a. Any device found deficient at any time will be reported to the officer's supervisor who will issue a replacement if available.

4. Officers shall wear the BWC in the approximate center of the chest.

5. An officer who does not activate a BWC in response to a call must include in the officer's incident report or otherwise note in the case file the reason for not activating the camera.

6. Any BWC data created will be downloaded or copied to the appropriate department storage location before the end of shift.

7. While much of the recorded data will not be needed – as in a building search where nothing is found or a citizen contact that did not result in any action; any data that an officer believes is evidence, is recorded during a use of force or pursuit, or is likely to be needed for any other purpose such as a potential employee complaint, should be noted in official reports. If the recording may be needed and no report is made, the officer should contact the BWC data manager so the data may be flagged and kept secure as needed.

F. Supervisor's Responsibilities

1. Supervisors will attend department training on the use, retrieval, and storage of data, using BWCs.

2. Supervisors will take such action to ensure data from BWCs are transferred and stored properly and in a timely manner.

3. Supervisors will remind officers of rules regarding BWC evidence on a regular basis.

4. Upon receipt of a formal or informal complaint, the supervisor investigating the complaint shall ensure all related videos are properly retained in the WatchGuard Evidence Library.

5. Supervisors shall retain any and all BWC and dash camera videos when completing a use of force report, pursuit report, employee injury report and for any fleet accident.

G. Release of Information Recorded by Body-Worn Cameras

1. The procedure for open records requests from the public for information recorded by a body-worn camera is outlined in Occupations Code 1701.661 and must include:
    a. The date and approximate time of the recording,
    b. The specific location where the recording occurred, and
    c. the name of one or more persons known to be a subject of the recording

2. Any portion of a video made in a private space, or of a recording that constitutes a misdemeanor punishable by a fine only and does not result in an arrest may NOT be released without written authorization from the person who is the subject of the recording.

3. An officer or employee who receives a voluminous request is considered to have promptly produced the information if the officer or employee takes the actions required under Government Code 552.221 before the 21st business day after the date of receipt of the request.

H. Access to Recordings

1. Employees will have access to BWC recording through back-office client software to facilitate the production of reports and for administrative purposes. The level of access for each employee will be assigned by the Technology Administrator based on the employee's current assignment.

I. Off-Duty Employment

1. Officers working extra employment shall use their body worn cameras in compliance with this policy.

VI. DEPARTMENT NETWORK TERMINALS

A. Security

1. The department has a number of computers throughout the department that have access to the department network. All employees will be issued a unique password to allow access to the system.

2. Employees will safeguard their password to ensure no other person has access using their password.

3. Employees will not leave a computer connected to the network with their password, if they are not physically able to prevent access (by closing and locking a door, or by visible monitoring).

4. Employees are responsible for all access to the network using their password.

5. The department will assign appropriate security levels within the network to allow access to certain files only as required.

6. Employees are responsible to secure the screen on their mobile terminal prior to exiting their patrol vehicle and while conducting prisoner transports. The employee is responsible to ensure law enforcement sensitive information and CJIS information being displayed on their computer screen is not visible to the public or individuals being transported in the vehicle.

B. Required Access

1. All employees are required to sign-in at least twice each workday (at the beginning and end) to the network and read and respond to all department emails, and training assignments.

2. Employees who discover Network Terminals in need of repair will notify the IT HelpDesk as soon as possible.

VII. MOBILE TELEPHONES

A. Department Issued Cell Phones

1. Cell Phones are issued by the department to increase the level of communication between field officers and the department as well as citizens.

2. Cell phones are only to be used for appropriate departmental activities.

3. Employees are allowed to use department cell phones for emergency and short personal calls during breaks. The department regularly inspects cell phone usage records for inappropriate activity.

B. Personally Owned Cell Phones

1. The department allows employees to carry personally owned cell phones when their use does not negatively impact department operations.

VIII. CELL PHONE CAMERAS

A. Departmental Cell Phones

1. Cell phone cameras, both still and video, may be used to record department activities only when another more suitable camera or recording devices is unavailable.

2. Activities may include victim, witness, or suspect information, crime scenes, field and eyewitness identifications, witness statements, etc.

3. All activities recorded on cell phone cameras will immediately be transferred to departmental records systems as soon as the incident can be concluded and no later than the end of shift.

B. Personal cell phones will not be utilized for neither still nor video, to record department activities.

IX. DIGITAL CAMERAS

A. Department Issued Cameras

1. Personnel assigned to Crime Scene Investigations are assigned appropriate camera systems for recording crime scenes and incidents.

2. Field Officers are assigned field cameras to record images and data beneficial to an investigation when Crime Scene personnel do not respond.

3. Department issued cameras will not be used for any personal use.

4. All images or data recorded will be transferred to appropriate departmental media or storage before the end of shift.

X. LICENSE PLATE READER SYSTEM (TBP 7.36)

A. Data Storage and Retention

ALPR data is stored securely on the Flock Safety cloud servers in compliance with CJIS regulations. Flock Safety reads back to DPS every 24 hours and retains the data for 30 days. 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 discovery request or other lawful action to produce records. In those circumstances, the applicable data should be downloaded onto portable media and booked into evidence.

B. Security and Access to Data

The Chief of Police will appoint an ALPR Program Manager who will be

responsible for the maintenance of the system including the creation, deletion of access accounts with approval of the Chief of Police. The ALPR data collected will be secured and will only be accessible to persons approved by the Chief of Police. Individuals authorized to access the data will be provided with login credentials to gain access to the information. The ALPR Program Manager is responsible for training those granted access to the system, and ensuring its proper use.

C. Data Usage

1. The ALPR data is Law Enforcement intelligence information, and is restricted to the investigation of criminal offenses or the locating of wanted persons only.
2. If practicable, the officer should verify an ALPR notification through the appropriate law enforcement databases before taking enforcement action that is based solely on an ALPR alert. The officer must review the details of the alert and determine whether any action is necessary, based on their evaluation. Reasonable suspicion or probable cause is not required before using an ALPR.
3. All ALPR data shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date, and time.
4. If a question arises about the usage of the LPR data, that question will be referred to the Program Manager and the Office of the Chief for resolution. Any non-Law Enforcement usage of the data is strictly prohibited.

XII. E-MAIL POLICY

All police department employees will follow the City of Rosenberg email communication policy designated by Human Resources and Information Technology Department.