	SFASU POLICE DEPARTMENT	
	Policy 5.3 Computer and Electronic Equipment Usage and Data Security	
	Effective Date: 04/25/19	**Replaces:**
	Approved: John Fields, Jr. Chief of Police	
	Reference: IACLEA 9.1.7a, b & c	

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. It states the protocols for storage, security, and retention. It also establishes what uses of such equipment are prohibited and what constitutes inappropriate use of such equipment.

II. PURPOSE

It is the purpose of this policy to define and provide clear direction as to the allowed uses and the prohibited uses of departmental and personal 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

A. Network Terminals: Desktops, laptops, or any other electronic devices that connect to the department's internal computer network.

B. Mobile Digital Computers (MDC): In-vehicle computers or any other electronic devices that in some manner connect to the Internet, department computer networks, or other service, such as TCIC, that provides officers with data or allows officers to conduct field reporting or communications with other officers or the department.

C. Mobile Phones: Either department owned or personally owned cell phones or smart phones.

D. Body Cameras / Digital Media Recorders (DMR): Video/Audio recordings made via a camera system that is worn by police personnel.

E. Mobile Video Recording: In-vehicle camera systems that are permanently mounted in department vehicles.

F. Digital Media Recorder (DMR): Officer-worn digital audio or video recording device.

G. Digital Camera: A single-purpose, handheld camera designed to take digital photographs.

IV. PROCEDURES

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

A. General Provisions

1. Any electronic document, report, audio, or video recording, image, email, voice communication, or any other form of electronic data 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 to be a government record. As such, it is subject to public record laws, and it shall be preserved accordingly.

2. Anything that is created on department-owned equipment, whether or not it is directly related to official department operations or investigations, may be considered a government record, and may be reviewed and shall be preserved as required by state law or department policy. This includes any electronic document, report, audio or video recording, image, email, voice communication, and any other form of electronic data created while on or off duty.

3. All department-owned equipment and its use are subject to routine or specific review and/or investigation by department supervisors as needed to ensure appropriate use.

4. On-duty use of any electronic device, such as a mobile phone or phone camera, for strictly personal purposes not related to departmental operations 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 departmental general orders or state or federal law.

5. All employees that directly access the TCIC/NCIC database will be trained in the appropriate level of access.

6. If any form of digital evidence exists, formal departmental reports will include a notation that such evidence exists, including the type of evidence and the storage location.

7. The Chief of Police may release DMR and/or MVR data for institutional student and employee disciplinary proceedings if approved by General Counsel.

B. General Prohibitions

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

3. Employees are allowed to access the internet for personal use during meal and other breaks as long as the sites accessed are appropriate for public viewing.

4. No video games will be played on department equipment.

5. No inappropriate websites will be visited.

6. Inappropriate use of electronic devices or the release or posting on the internet or various social media sites of another party's private information, or governmental information usually deemed private can lead to internal investigations and subsequent disciplinary action.

7. An officer can be questioned about his/her internet activities by defense counsels in criminal trials, potentially damaging the officer's credibility as a witness.

V. DEPARTMENT NETWORK TERMINALS

A. Security

1. The department has a number of computers, and other devices, 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 will gain 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, such as by closing and locking a door, or by visible monitoring of the computer.

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 all access to certain files only as required.

B. Required Access

1. All employees are required to sign in to the network at least twice each workday (at the beginning and end of their shifts).

2. Employees must read and respond to all department emails and training assignments.

3. Employees who discover network terminals in need of repair will notify the administrative sergeant as soon as possible.

VI. MOBILE DIGITAL TERMINALS / COMPUTERS – MDT/MD

A. The Mobile Data Terminal/Computer (MDT/MDC) is a part of the radio system, which uses frequencies licensed by the FCC. Rules concerning proper radio procedures also apply to use of the MDT.

B. Messages (1) will not be personal, (2) will not contain derogatory references to other persons or agencies, and (3) will not contain any text that a reasonable person would find offensive.

C. Using the MDT/MDC, field officers may signal (1) receipt of a call for service, (2) arrival at the scene of a call, (3) request for assistance, and (4) clear from a call, but they shall also do so by voice communications so that other field units and supervisors will be kept aware of ongoing operations.

D. Because messages sent with the CAD/MDT system slow the system's response time, only concise, work-related messages may be transmitted. Personnel are urged to use abbreviations to help keep the messages brief.

E. There is NO EXPECTATION of privacy concerning sending or receiving messages via the CAD/MDT system.

F. Except in emergency situations or in single-key response to dispatched calls or enquiries, the driver of the vehicle will not utilize the MDT/MDC keyboard while the vehicle is in motion. Drivers will pull to a safe location before utilizing the keyboard.

VII. MOBILE VIDEO RECORDING SYSTEMS

A. The use of a Mobile Video Recording (MVR) system provides persuasive documentary evidence and helps defend against civil litigation and allegations of officer misconduct. Such evidence is often used in court cases, and can help in determining the guilt or innocence of accused people.

B. General Procedures

Officers assigned the use of these devices shall adhere to the operational objectives and protocols outlined herein so as to maximize the effectiveness and utility of the MVR and the integrity of evidence and related video documentation.

1. It shall be the responsibility of this department to ensure that the audio-video recording equipment is properly installed according to the manufacturer's recommendations.

2. MVR equipment shall automatically activate when emergency equipment (lights) or a wireless transmitter is operating.

3. The system may also be activated manually from the control panel affixed to the interior of the vehicle (IACLEA 9.1.7a).

4. Placement and operation of system components within the vehicle shall be based on officer safety requirements.

5. All officers shall successfully complete this department's approved course of instruction prior to being deployed with MVR systems in operational settings.

6. Inspection and general maintenance of MVR equipment installed in departmental vehicles shall be the responsibility of the officer assigned to the vehicle.

7. Prior to beginning each shift, the assigned officer shall perform an inspection to ensure that the MVR is performing in accordance with the manufacturer's recommendations covering the following matters:
    a. Remote activation of system via transmitter
    b. Windshield and camera lens free of debris
    c. Camera facing intended direction
    d. Recording mechanism capturing both audio and video information, that is, the system plays back both audio and video tracks.
    e. Input information into the system to personalize the recording.

8. Malfunctions, damage, or theft of in-car camera equipment shall be reported to the immediate supervisor prior to placing the unit into service.

9. Mandatory Use:
    a. All official contacts whether on a call or officer initiated
    b. Traffic stops (to include, but not limited to, traffic violations stranded motorist assistance, and all crime-interdiction stops)
    c. Priority responses
    d. Vehicle pursuits
    e. Prisoner transports

10. When the MVR is activated, officers shall ensure that the audio portion is also activated so that all events are properly documented. Officers are encouraged to narrate events using the audio recording, which will provide the best documentation for pretrial and courtroom.

11. Officers using the transmitters that are individually synchronized to their individual MVR shall activate both audio and video recordings when responding in a support capacity in order to obtain additional perspectives of the incident scene.

12. When officers park patrol units in the vicinity of Parking Garage #2, MVR(s) will download automatically to the server which is maintained by the SFA IT department.

13. Officers shall not erase, alter, reuse, modify, or tamper with MVR recordings.

14. When the MVR is activated to document an event, it shall not be deactivated until one of the following has occurred:
    a. the event has been concluded;
    b. the incident or event is of such duration that the MVR may be deactivated to conserve recording times;
    c. the officer decides that deactivation will not result in the loss of critical documentary information; and
    d. the intention to stop the recording has been noted by the officer either verbally or in a written notation (IACLEA 9.1.7a).

15. Supervisor Responsibilities:
    a. All recordings are maintained on the server.
    b. The supervisor shall periodically check the server to ensure recordings are being downloaded.
    c. Supervisors who are informed or otherwise become aware of malfunctioning equipment shall ensure that authorized personnel make repairs in a timely manner.
    d. Supervisors shall conduct periodic reviews of officer-assigned media in order to periodically assess officer performance (IACLEA 9.1.7b).
    e. Supervisors will assure proper functioning of MVR equipment and determine if MVR equipment is being operated properly.
    f. Supervisors will identify recordings that may be appropriate for training.
    g. Supervisors shall conduct weekly reviews of personnel who are newly assigned MVR equipment in order to ensure compliance with departmental policy.
    h. Supervisors shall conduct quarterly reviews.
        i. Minor infractions (not criminal in nature) discovered during the routine review of recorded material should be viewed as training opportunities and not as routine disciplinary actions.
        ii. Should the behavior or action persist after it has been informally addressed, the appropriate disciplinary or corrective action shall be taken.

i. Supervisors shall ensure that adequate recording media is on hand and available for issuance.

16. Technicians' Responsibilities
    a. CID personnel shall be responsible for duplication of all recorded media.
    b. Recorded media may only be degaussed/erased pursuant to a court order, or in accordance with established retention guidelines of at least 90 days (IACLEA 9.1.7b & c).

VIII. MOBILE TELEPHONES

Personally Owned Cell Phones: The department allows employees to carry personally owned cell phones when their use does not negatively impact department operations.

IX. CELL PHONE CAMERAS

A. Personal Cell Phones

1. Personal cell phones, both still and video, may be used to record department activities only when another more suitable camera or recording device is unavailable.

2. If any department activity is recorded using a personal cell phone, a department supervisor will be notified immediately.

3. All activities recorded on cell-phone cameras will be transferred immediately to departmental records systems as soon as the incident can be concluded and no later than the end of shift. Appropriate information technology staff will be consulted regarding the safest transfer method.

4. After transfer to departmental media, all parts of the activity recorded will be permanently deleted from the personally owned cell phone prior to end of shift. Department supervisors may require proof of deletion.

X. 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.

B. Personally Owned Cameras

1. No employee will carry a personally owned camera on duty unless authorized in writing by the Chief of Police.

2. If a personally owned camera has been authorized in writing by the Chief of Police, the employee will report any use of the camera during a police incident to his/ her supervisor immediately and shall transfer the data to department media before the end of shift.

3. After transfer to departmental media, all parts of the activity recorded will be permanently deleted from the personally owned camera prior to end of shift. Department supervisors may require proof of deletion.

XI. DIGITAL MEDIA RECORDERS (Body Worn Audio/Video Recorders)

Note: These procedures do not apply to mounted in-vehicle audio/video systems, which are covered elsewhere in this order.

A. Department Issued Digital Media Recorders DMR.

1. 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.

2. The Chief of Police will designate an individual to manage the receipt and storage of DMR data. The DMR manager will routinely save DMR data as

necessary to long-term storage media. DMR data not identified as necessary will be deleted after 90 days (IACLEA 9.1.7b).

3. DMR data that contains evidence in criminal investigations shall be maintained until the final court disposition has been issued (includes the completion of all appeal processes), and felony evidence shall be maintained until the statute of limitations has passed. DMR evidence related to specific investigations such as homicides and sexual assaults, shall be maintained indefinitely (IACLEA 9.1.7c).

4. Officers issued a DMR shall use the device as required in B below.

B. When usage is required. NOTE: If the DMR is activated for any of the reasons listed below, the recording shall continue until the incident is complete or the officer has left the scene.

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 the officer is outside his/her vehicle.
5. During building searches and alarm responses (IACLEA 9.1.7a).

C. Prohibitions

1. Officers shall not intentionally create digital recordings of other employees in areas where a reasonable expectation of privacy exists.

2. Officers shall not intentionally create digital recordings of citizens' activities in areas where a reasonable expectation of privacy exists, unless the recording is made while the officer is legally in the area for one of the situations listed in section B above. Officers should be aware that under certain circumstances, e.g. victims or suspects in various stages of undress, the officer may consider stopping the recording and will explain the stopped recording in the report.

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

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

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

6. Uploading of any DMR data to any social media site is prohibited.

7. Officers may use DMRs only in-patient care areas of hospitals or emergency rooms when the recording is for official business.

8. To the extent possible, officers will attempt to prevent the recording of non-involved individuals.

D. Officer Responsibilities

1. Officers issued a department-owned DMR shall attend training, and they will demonstrate proficiency with the recording and transfer of recorded data.

2. Officers shall inspect the device at the beginning of each shift to ensure proper operation, including sufficient battery life and recording medium.

3. Any device found deficient at any time will be reported to the officer's supervisor who will issue a replacement if one is available.

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

5. 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 might be evidence or is likely to be needed for any other purpose, such as a potential employee complaint, should be noted in official reports. All recorded data will be held in accordance with applicable laws

E. Supervisor's Responsibilities

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

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

3. Supervisors will ensure that DMR data has been deleted from personally owned devices before officers leave shift.

4. Supervisors will remind officers of rules regarding DMR evidence on a regular basis.