

## **CONTENTS**

This procedure consists of the following numbered sections:

- I. GENERAL PROCEDURES
- II. SUBMISSION, PROCESSING AND STORAGE OF DIGITAL MEDIA
- III. ADDING METADATA TO FILES
- IV. STORAGE (RETENTION) CATEGORIES
- V. SUBMISSION TO STATE ATTORNEYS OFFICE
- VI. DOCUMENT EXCHANGE PORTAL
- VII. AXON CAPTURE/CITIZEN

## **PURPOSE**

The purpose of this standard operating procedure is to establish guidelines used by the Punta Gorda Police Department (PGPD) for the production, processing, handling and storage of all digital media.

## **SCOPE**

This procedure shall apply to all Punta Gorda Police Department personnel.

## **DISCUSSION**

Digital media is one of the most important forms of documentation available to law enforcement. It is the policy of the Punta Gorda Police Department to ensure the highest degree of efficiency in the handling of police department digital media, as well as to protect the integrity of all police department digital submissions.

#### **DEFINITIONS**

- 1. **Axon Capture:** An application built for your smartphone to record photo, audio and video evidence. Evidence automatically tagged with GPS locations and metadata is synced to Axon Evidence.com.
- 2. **Digital Media:** For purposes of this procedure, digital media shall refer to digital photos, digital audio or digital video taken in relation to Punta Gorda Police Department business.
- 3. **Evidence Photo Label:** The label affixed to non-digital digital photographs utilized as evidence, pursuant to Florida State Statute (F.S.) 90.91. The evidence Photo Label is PGPD form EVI 245.

#### **PROCEDURE**

## I. GENERAL PROCEDURES

- A. Personnel will utilize the Axon Capture system on city issued smart phones to take digital photos, digital audio and digital video files. Select personnel (Crime Scene and Detectives) may have additionally assigned cameras to complete these functions. All personnel will upload these files into the Evidence.com system through Evidence Capture. Crime Scene or Detective personnel who utilize an additionally assigned camera may use Evidence Sync to upload files into Evidence.com. Files larger than 50 GB will need to be uploaded to a portable hard drive and submitted directly to the Evidence Unit.
- B. All personnel utilizing digital imaging equipment must do so only with the intent of producing clear and accurate representations of the people, places, or items captured. The expressed goal of the department is to use digital media as an efficient tool to produce images acceptable in court and for other legitimate police department purposes.
- C. Personnel will reproduce images that are faithful to the original image acquired unless enhancements are required to better reveal the detail that is already present but may be obscured by distracting background, poor definition, improper lighting or color contrast.
- D. Digital media shall not be utilized or altered with the intent to mislead, confuse or deceive.
- E. Personal phones shall not be used to process police department digital media.
- F. Digital media shall not be submitted as evidence via email.
- G. The creation of digital media will be noted appropriately in incident reports.
- H. All members processing digital media shall receive training during their field training program.

I. No member shall access digital media files that are not captured by them unless authorized by the Chief or designee, except for the purpose of doing a follow-up criminal investigation, approved auditing, or for the purpose of conducting an internal affairs investigation. This does not prevent an officer from reviewing digital media before writing a report or providing a statement regarding any event arising within the scope of his or her official duties.

## II. SUBMISSION, PROCESSING AND STORAGE OF DIGITAL MEDIA

- A. Evidentiary Digital Media: A Property Receipt shall be submitted for each Incident Report for which there are evidentiary digital media files. Digital media files will be tagged with the appropriate metadata and uploaded to Evidence.com prior to the end of each shift. The State Attorney's Office for the 20th judicial circuit will have access to Evidence.com for viewing of evidentiary tagged videos.
  - 1. Digital media files must be organized in sub-folders based on media type or media reference. (i.e. Body Camera Videos, Witness Statements, Scene Photos, etc.)
    - a. Exceptions include when there are 10 files or less.
    - b. Individual files within sub-folders should be free of duplication.
- B. Non- Evidentiary Digital Media: Non-evidentiary digital media shall be uploaded to Evidence.com and tagged with the appropriate metadata. Non-evidentiary digital media may be generated related to a field interview, parking violation, traffic crash, etc. Digital medial files will be uploaded to Evidence.com prior to the end of each shift.
- C. Photo Printing: Individual photos will only be printed upon request. Photos submitted for court (that are not transmitted electronically) will be printed on regular copy paper and shall be marked by the Evidence Technician with a stamp which certifies that the photo is a true copy.
- D. Officer's body worn cameras and in-car video cameras (SOP 1124.00 Body Worn Camera Procedures, SOP 516.00 In-Vehicle Audio and Video Recording) shall be the primary method for officers to capture video. Any additional supporting video may be captured via the officers department issued smart phone using Axon Capture. Videos taken with Axon Capture will be tagged with the appropriate metadata and uploaded to evidence.com prior to the end of each shift.

#### III. ADDING METADATA TO FILES

A. Procedure: Use Axon Capture or Axon Evidence Sync to attach metadata, such as ID, title, and retention category, to the files you create. Metadata can also be added through Evidence.com after the files have been uploaded.

- 1. ID: Select the ID box and type the case ID that you want to apply to the evidence file. The vast majority of submissions should have an ID number. Any submission that has a corresponding ID number shall be documented. Identification (ID) for digital photographs, digital audio and digital video shall be the complete incident report number (i.e. 23-01940). If an incident report number does not exist then a Computer Aided Dispatch (CAD) event number shall be used (i.e. 2023-024743). Category OFFICER Test / Training / Accidental / Personal Break receives an ID number of 23-00000.
- 2. Title: Select the Title box and type the title that you want to apply to the file. Otherwise the system default title will be applied.
- 3. Category: Select the category you want to apply to the file. Category detail procedures are in Section IV Storage (Retention) Categories.

## IV. STORAGE (RETENTION) CATEGORIES

- A. Members shall be responsible for reviewing digital photographs, digital audio and digital video in the Axon Capture phone app or Axon Sync computer program. Members shall assign the appropriate Storage Category (Retention Categories) in the Evidence.com system. All appropriate retention categories shall be selected for each file. Retention is based upon the highest retention category selected. Officers are only to utilize the OFFICER categories.
  - 1. Administrative (Admin Only): Any digital files identified by the Command Staff as files needing to be retained by the department. (Until Deleted)
  - 2. Assisting Other Agency: Any digital files captured while assisting other agencies with calls where the Punta Gorda Police Department is not the primary agency. (60 weeks)
  - 3. Death Investigations (Non-Evidentiary): Any digital files related to non-criminal death investigations. (180 Days)
  - 4. Documents (Non-Evidentiary): Any digital files related to a case that are necessary for a case file, but have no evidentiary value. (Until Deleted)
  - 5. Evidence: Any digital files that are evidentiary in a criminal case. A property receipt must be submitted for all evidence. (Until Deleted)
  - 6. Field Interviews: Any digital files related to a field interview. (Five Years)
  - 7. Investigation (Non-Evidentiary): Any digital files related to non-criminal cases or cases where it has not yet been determined that a crime has been committed. If it is

- determined during the investigation that a crime was committed it is up to the officer to re-categorize the media as "Evidence" and submit a property receipt. (180 Days)
- 8. Other: Any digital files that do not fit into another category and do not need to be retained longer than 90-days. (90 Days)
- 9. Pursuit / Use of Force / Officer Injury: Any digital files related to a vehicle pursuit, use of force, or injury to an officer. (5 Years)
- 10. Statements (Non-Evidentiary): Any digital files related to statements taken for a case, but that have no evidentiary value. (Until Deleted)
- 11. Taser Log (Admin Only): All Taser Logs uploaded during routine reviews, accidental discharges, or field deployments. Taser logs saved due to a use of force should be labeled as "Pursuit/Use of Force/Officer Injury." (One Year)
- 12. Test/Training/Accidental/Personal Break: Any digital files related to tests, training, accidents, or personal breaks. (90 Days)
- 13. Traffic Stop: Any digital files related to a non-criminal traffic stop. (90 Days)
- 14. Traffic Crash: Any digital files related to a non-criminal traffic crash. (90 Days)
- 15. Trespass: Any digital files related to a non-criminal trespass case. (14 Months)
- 16. Welfare Check (Baker/Marchman Act): Any digital files related to any non-criminal welfare check or any Baker Act or Marchman Act. (90 Days

## V. SUBMISSION TO THE STATE ATTORNEY'S OFFICE

- A. All files in document format (to include but not limited to case reports, affidavits and written statements) should be submitted through the Document Exchange Portal (DEP).
- B. "Digital Media" such as photos, audio recorded statements, and video recordings may be submitted through the DEP or Law Enforcement Agency (LEA) established AXON account. If avoidable, digital media should not be transmitted via digital disc either CD or DVD.
- C. All Body Camera and or/In-Car Videos must be transmitted to the SAO through the LEA established AXON account. Digital media exceptions include:
  - 1. Forensic Child Interview / Child Protection Team (CPT) Video File(s) should be transmitted through the DEP. Due to the confidential nature of these items, such files should not be transmitted through Axon / Evidence.com or any other media platform.

- a. The aforementioned files should be uploaded to the DEP in Windows Media Viewer (wmv.) format for all arrest cases, warrant requests, and agency reviews using the following description: "Video (Child Interview Victim Initials)", Document Type: "Investigation", and Sub Type: "Video CPT".
- 2. Data extractions from cellular phones, other mobile devices, hard drives, and/or other digital data storage device(s).
  - a. It is the responsibility of Law Enforcement to specify the existence of such data evidence within respective original case (or supplemental) reports. By default, Law Enforcement must submit data extractions specific to "pertinent evidence" to the case to the SAO for review. If additional data files from the associated data extraction(s) exist, it should be noted within the respective report that it is available for inspection. Entire (whole) data extractions (beyond pertinent evidence) shall only be submitted to the SAO for review after specific request by the SAO.
  - b. Pertaining to transmission for review, in-part and in-whole, refer to the guideline below:
    - i. in part (pertinent evidence): after review by law enforcement, with the exclusion of explicit materials, and after files are identified as pertinent evidence, extracted data evidence may be provided through electronic means via the DEP.
    - ii. in whole (all data files): with the exclusion of explicit materials, must be transmitted on a separate hard disk or hard drive.
- D. Digital Media and Investigative Reports shall be transmitted at the same time, even when different platforms (such as the DEP or AXON) are utilized for submission.

# VI. **DOCUMENT EXCHANGE PORTAL:** The conditions of the DEP Process are as follows:

- A. Guidelines for the DEP will be provided by the Criminal Justice Information System programmers.
- B. The Participants will be responsible for the creation of their user accounts and delegate accounts, deactivation of their accounts, maintenance of correct e-mail addresses for their accounts, and resetting forgotten passwords. Each Participant will be responsible for ensuring there is no unauthorized access to the DEP. Each Participant is responsible for the training requirement for their staff.

Revised: 02-21-2024

C. Accounts that have not been used within 180 days will be deactivated.

- D. All documents sent from SAO to Participant will be available on the portal for retrieval for 30 days. If the DEP is unavailable, Parties will exchange information in an alternative method.
- E. The Participants agree to have up to-date and active anti-malware installed on their systems.
- F. Either Party may terminate this agreement by providing 30 days written notice. The Participant may terminate this agreement by delivering written notice to the SAO Executive Director.
- G. Participants agree to adhere to all CJIS policies as set forth in the CJIS Security and FDLE CJIS Criminal Justice User Agreement.
- H. Participants are FDLE CJIS recognized Criminal Justice Agencies and attest that the information will remain confidential. Should any employee violate this confidentiality, they will be disciplined accordingly.
- I. Participants agree to adopt and adhere to appropriate and reasonable quality assurance procedures to ensure only complete, accurate, and valid case information is transmitted through the document portal.
- J. The document file format preferred is PDF with DOCX as a second choice and video format preferred is MP4.
- K. In the event that case information may include items having evidentiary value by virtue of their physical state or condition, or are otherwise not suitable for electronic transmission, the SAO will accept such case information in a physical format.
- L. Participants agree to maintain active FDLE CJIS Criminal Justice Agreements and have adopted written policies and procedures governing the use, maintenance, and protection of confidential case information. Any Participant that violate such policies and procedures are subject to appropriate agency discipline.
- M. Training: All training to utilize the DEP will be handled by Criminal Justice Information Systems (CJIS) at CJISWEBHELP@CA.CJIS20.ORG.

Revised: 02-21-2024

#### VII. AXON CAPTURE/CITIZEN

A. Axon Citizen makes it easy for law enforcement agencies to securely receive evidence submissions from the community and manage that media in Evidence.com. Axon Citizen

- for Officers allows officers to send out individual invites to witnesses directly from Axon Capture or Evidence.com.
- B. Invites may be sent to an email address or text message phone number. All invites must contain appropriate metadata as outlined in Section III.
- C. Community members upload files and Evidence.com notifies the portal creator about the new submission.
- D. Triage submissions to determine what to accept and decline. All accepted submissions from the citizens must be accompanied by a property receipt.

#### **APPROVED**

PAMELA R. SMITH, CHIEF OF POLICE

**STAFF REVIEW DATES:** 10-23-1995, 03-05-1996, 01-30-1998, 10-13-2000, 08-02-2002, 08-23-2005, 10-04-2007, 01-22-2009, 03-13-2012, 04-16-2013, 03-24-2014, 09-09-2016, 07-31-2018, 07-28-2020, 06-15-2023

**REVISION DATES:** 10-23-1995, 03-05-1996, 03-22-1996, 01-30-1998, 10-13-2000, 08-02-2002, 08-23-2005, 10-04-2007, 01-22-2009, 03-13-2012, 04-16-2013, 03-24-2014, 09-09-2016, 07-31-2018, 02-27-2019, 07-28-2020, 10-27-2020, 10-28-2021, 01-07-2022, 06-15-2023, 09-26-2023, 02-21-2024