

Civil Service Board Regular Meeting

Agenda August 3, 2021 @ 4:00 pm Public Safety Facility Ray Beary Community Room 500 N. Virginia Ave.

welcome

Agendas and all backup material supporting each agenda item are accessible via the city's website at <u>cityofwinterpark.org/bpm</u> and include virtual meeting instructions.

assistance & appeals

Persons with disabilities needing assistance to participate in any of these proceedings should contact the City Clerk's Office (407-599-3277) at least 48 hours in advance of the meeting.

"If a person decides to appeal any decision made by the Board with respect to any matter considered at this hearing, a record of the proceedings is needed to ensure that a verbatim record of the proceedings is made, which record includes the testimony and evidence upon which the appeal is to be based." (F.S. 286.0105).

please note

Times are projected and subject to change.

1.	Cal	l to Order		
2.	Consent Agenda			
	a.	Approval of minutes, July 6, 2021	1 minute	
3.	3. Staff Updates			
	a.	Police Department	5 Minutes	
	b.	Fire Department	5 Minutes	
4.	Citizen Comments (for items not on the agenda): Three minutes allowed for			

each speaker

5. Action Items

a. SOP'S

10 Minutes

- 1. SOP 195 Accreditation
- 2. SOP 392 Digital Evidence Procedures
- 6. Public Hearings
- 7. **Board Comments**
- 8. Adjournment

item type Consent Agenda

prepared by Kathleen Reed

board approval

strategic objective

subject Approval of minutes, July 6, 2021

motion / recommendation

background

alternatives / other considerations

fiscal impact

ATTACHMENTS: July 7, 2021 MINUTES.pdf meeting date August 3, 2021

approved by



Civil Service Board

Regular Scheduled Meeting

July 7, 2021 at 4:00 p.m.

Public Safety Complex

500 North Park Avenue | Winter Park, Florida

Regular Meeting

Meeting Minutes

Present

Kip Marchman, Chairman Steve Stutzer, Vice Chairman Pitt Warner, Chief Examiner Mary Daniels, Board Member Javier Rodriguez, Police Representative Police Chief Michael Deal Fire Chief Dan Hagedorn

Absent: Tod Meadors, Fire Representative

1. Meeting called to order

Chairman Marchman called the meeting to order at 4:00 p.m.

2. Consent Agenda

A. Approval of the June 1, 2021 Minutes

Motion made by Mr. Stutzer and seconded by Ms. Daniels to approve the minutes from the June 1, 2021 Regular Meeting. Motion carried unanimously with a 5-0 vote.

3. Staff Updates

A. Police Department Update

Chief Deal provided the following update:

- Two new officers started on June 28th, 2021.
- Three new officers to begin on July 26th, 2021.
- Three new officers to begin in September.
- Officer Veronica Muller to retire on August 15th, 2021.
- Officer Ricardo Delbrey to return from military duty in August.
- Officer Edison Williams remains on deployment.

B. Fire Department Update

Chief Hagedorn provided the following update:

- Department is currently monitoring storm Elsa.
- Hiring process begins on July 13th, 2021-Applicant must receive a passing score of 70% to move forward in the process.
- Currently the department has three vacancies.
- July 19th, 2021- four-part series profiling four employees will begin on social media.

A brief discussion was held regarding prioritizing hiring procedures.

4. Citizens Comments

None

5. Action Items (agenda taken out of order)

C. Revised Standard Operating Procedures

- SOP 115 Fiscal Activities
- SOP 130 Personal Appearance
- SOP 142 Workplace Discrimination/Harassment/Retaliation
- SOP 350 Lake Patrol Program

Division Chief Marcum presented SOP 115-Fiscal Activities, SOP 130 Personal Appearance; Sop 142-Worlplace Discrimination/Harassment/Retaliation and SOP 350 Lake Patrol Program. Division Marcum answered questions by board members and stated that it has been reviewed by Chief Deal, all Division Chiefs and approved by Legal Counsel, Erin DeYoung. • Mr. Rodriguez questioned SOP 130 regarding the issue of tattoos as it would relate to those members of the department who have were hired prior to the revision of SOP 130. A brief discussion was held.

Motion was made by Stutzer and seconded by Mr. Warner to approve the above listed SOP's. Ms. Daniels, Mr. Stutzer, Mr. Marchman and Mr. Warner voted yes and Mr. Rodriguez voted no. Motion carried with a 4-1 vote.

A. Police Applicant Interviews

The following new hire candidate, Jeffery Fowler was introduced by Chief Deal to members of the board. Mr. Fowler provided a brief background and responded to questions by board members. Motion was made by Mr. Warner and seconded by Ms. Daniels to certify Mr. Fowler. Motion carried unanimously with a 5-0 vote.

Next, Chief Deal introduced Nadia Terc to board members. Ms. Terc provided a brief background and responded to question by board members. Motion was made by Mr. Warner and seconded by Mr. Rodriguez to certify Ms. Terc. Motion carried unanimously with a 5-0 vote.

6. Board Comments

None

8. Adjournment

There being no further business the meeting was adjourned at 4:35 p.m.

Kenneth Marchman, Chairman Kathy Reed, Recording Secretary

item type Staff Updates

prepared by Kathleen Reed

board approval

strategic objective

subject Police Department

motion / recommendation

background

alternatives / other considerations

fiscal impact

meeting date August 3, 2021

approved by

item type Staff Updates

prepared by Kathleen Reed

board approval

strategic objective

subject Fire Department

motion / recommendation

background

alternatives / other considerations

fiscal impact

meeting date August 3, 2021

approved by

item type Action Items

meeting date August 3, 2021

approved by

prepared by Kathleen Reed

board approval

strategic objective

<mark>subject</mark> SOP'S

501 5

item list

- 1. SOP 195 Accreditation
- 2. SOP 392 Digital Evidence Procedures

motion / recommendation

background

alternatives / other considerations

fiscal impact

ATTACHMENTS: 195 Accreditation.pdf

ATTACHMENTS: 392 Digital Evidence Procedures.pdf

9

WINTER PARK POLICE DEPARTMENT STANDARD OPERATING PROCEDURE

Title:	Accreditation	SOP #: 195
Rescinds:		Amends:
Effective:	August 3, 2021	Pages: (03)
Attachments:		

195-1 PURPOSE:

The purpose of this policy order is to establishes an accreditation management system to include an which provides an overview of the program, the authority for administering the processes, and delineates the responsibilities of the agency and those directly involved in the accreditation process.

195-2 POLICY:

Accreditation is the certification by an independent reviewing authority that an entity has met specific requirements and prescribed standards. It is the policy of the Winter Park Police Department to achieve and maintain State accreditation status in an effort to maintain standards that represent current professional law enforcement practices, increase effectiveness and efficiency in the delivery of police services, establish and maintain standards which reduce liability for the agency and its members and ensure agency personnel are accountable to the citizens they serve. This will be accomplished by an ongoing endeavor by all members of the agency to abide by and exceed the standards developed by the Commission for Florida Law Enforcement Accreditation, Inc. (CFA).

195-3 BENEFITS:

Accreditation demonstrates to the community that the Winter Park Police Department is committed to providing services of the highest quality and assures that agency policies and procedures are in written form and available to all personnel.

Accreditation reduces the likelihood of liability suits and significantly assists in risk management.

Accreditation is a coveted award that symbolizes professionalism, excellence and competence. The community and Winter Park Police Department can take pride in their department knowing it represents the very best in law enforcement.

195-4 GOALS:

The goals of accreditation include:

- A. An increase in officer safety through enhanced training and equipment.
- B. Written policies and procedures which clearly guide employees in the performance of their duties.
- C. The participation in the process increases agency effectiveness and efficiency in the delivery of law enforcement services and increases law enforcement capabilities to prevent and control crime.
- D. Accreditation increases citizens' and employees' confidence in goals, objectives, policies, and practices of the Winter Park Police Department and increases cooperation and coordination with other law enforcement agencies throughout the area and the State of Florida.

195-5 THE PROCESS:

An agency must apply to the Commission for Florida Law Enforcement Accreditation, Inc. (CFA) to participate in the accreditation process. Once application has been made, the agency is required to demonstrate compliance with all applicable mandatory standards and not less than 80% of applicable non-mandatory standards. Proof of compliance with the standards is determined by an assessment team sent by the Florida Law Enforcement Commission, conducting an on-site review of the agency's own policies, procedures and practices. The three (3) days assessment is conducted by practicing law enforcement professionals from around the State. During the review period, the assessment team reviews accreditation files, interviews agency personnel, participates in patrol ride-alongs and inspects the agency facility to determine if practice falls in line with written policy and applicable standards. Agencies accredited remain accredited for a period of three (3) years. After the three (3) year period, they must be reviewed again to maintain reaccredited status.

195-6 ACCREDITATION MANAGEMENT:

The Chief of Police shall determine who serves as the Accreditation Manager. This position shall be considered the facilitator, manager and coordinator for agency personnel to assist them in complying with the professional standards mandated by CFA. In relation to the accreditation process, the Accreditation Manager shall be responsible for:

- A. Ensuring all accreditation standards are adequately and appropriately integrated into agency policy and practice.
- B. Recommending agency policy revisions in response to added, modified or deleted accreditation standards.

- C. Keeping their supervisor chain-of-command-updated on the status of the agency's accredited status;
- D. Building agency electronic accreditation files and ensuring standard files contain all necessary and proper written directives and proofs of compliance.
- E. Ensuring agency members are familiar with and educated on accreditation standards and CFA.
- F. Preparing agency personnel and standard files for both the mock and onsite assessments; and
- G. Preparing for and coordinating all aspects of the mock and on-site assessments, and
- H. Keeping aware of the latest developments in the accreditation process by attending Florida Police Accreditation Coalition (FLA-PAC) meetings.

Each agency employee will cooperate with and provide the Accreditation Manager with support in matters affecting accreditation.

195-7 TRAINING:

- A. All employees of the Winter Park Police Department will be familiar with the accreditation processes, including the history and background of accreditation, the agency's involvement in the process, and the goals and benefits of accreditation. Familiarization with the accreditation process will be provided to as follows:
- B. All newly hired employees (to include sworn members, civilian personnel and volunteers) will be given an overview of accreditation during orientation, complete a training presentation and be required to pass a written test.
- C. All personnel will be briefed prior to mock and on-site assessments.
- D. Any newly appointed Accreditation Manager shall be required to complete CFA's New Accreditation Manager training course within one year of appointment. The training shall be documented. If a newly appointed Accreditation Manager has already completed the training, prior to their appointment, they must be able to provide the training documentation and will be exempt from having to complete the required training a second time.

Drafted: KG08-14 /revised: KG08-21

Alichandra

Chief of Police

WINTER PARK POLICE DEPARTMENT STANDARD OPERATING PROCEDURE

Title:	Digital Evidence Procedures	SOP #: 392
Rescinds:		Amends:
Effective:	August 3, 2021	Pages: (06)
Attachments:	"A" Start Page "B" End Page	

392-1 PURPOSE:

The purpose of this directive is to establishes guidelines and procedures for the proper collection, handling, preservation, processing and transfer of digital evidence items including photographs, video recordings, audio recordings, other electronic data, and other digital media.

392-2 POLICY:

It is the policy of the Winter Park Police Department that strict guidelines be followed when collecting, processing, and extracting items of digital evidence to insure their integrity, reliability, and admissibility in court in accordance with Florida State Statutes. Any collection, processing, and extracting of digital evidence should be conducted in a forensically sound manner.

All digital evidence which needs to be examined will be properly maintained and secured by an examiner during processing. Examiners shall adhere to chain of custody through proper documentation (to include date, time, method of transfer, receiving person's name and responsibility, reason for the transfer and the location of the pending examination (e.g. digital forensic analysis, CID). Digital evidence shall be initially submitted to Property and Evidence or Digital Forensic Specialist and recorded as such.

It is the examiner's responsibility to ensure that their evidence is properly secured and returned to Property and Evidence upon completion or during periods of time when the processing of evidence will not occur (i.e., vacation). Evidence will be secured in a locked room, with restricted access, and returned to Property and Evidence in a timely manner.

392-3 DEFINITIONS:

Archival Storage Server – A secure storage drive used for maintaining and storing of digital evidence.

Cloud Storage Server – A secure remote storage server (or multiple servers) typically accessed over the Internet or through a dedicated private connection, used for maintaining and storage of digital evidence.

CAFEWeb – *Computer Aided Forms Entry* – the department's report writing and records management system

CD-R – a non-rewritable compact disc used to store digital files

Digital Camera – any camera that stores single images or videos on digital media

Digital Data – data that represents other forms of information (such as images, videos, recordings, extractions, etc.) using specific machine language systems.

Digital Device – A device or item that can receive, store, process, or send digital information. This includes, but is not limited to, cell phones, computers, laptops, tablets, desktops, etc.

Digital Evidence - For purposes of this policy, a device or item that can receive, store, process, or send digital information. This includes, but is not limited to cell phones, computers (laptops, tablets, desktops), PDA's, thumb-drives, hard-drives, and memory cards.

Digital Forensics - A component of forensic science encompassing the extraction and analysis of evidence from digital devices.

Digital Forensic Specialist – Member of the department assigned and trained to conduct forensic examinations of from digital devices.

Digital Media – Storage media that may be removed (and replaced) from a camera or other digital device. This media may be in various forms including but not limited to secure digital (SD) cards, compact flash cards, USB drives, CDs, floppy diskettes, hard drives, etc.

Format – The standard structure by which data is organized in a file. This standard structure is denoted by a file extension such as .jpg, .wav, .mp3, etc.

Image Enhancement – Any process intended to improve the visual appearance of an image.

Recorder – any sound capturing device capable of digitally storing audio recordings.

392-4 REQUESTS FOR DIGITAL EVIDENCE PROCESSING

- A. When requesting an item to be processed by Property & Evidence or sent to another law enforcement entity, please email evidencerequest@cityofwinterpark.org with the following information:
 - 1. Case number
 - 2. Victim
 - 3. Defendant/Suspect(s)
 - 4. Tag number and item description
 - 5. Process being requested
 - 6. Briefly describe case circumstance/brief synopsis
- B. Requests specifically for digital forensic examinations shall be sent via email to the Digital Forensic Specialist as soon as possible. Members who send a request for a digital forensic examination shall provide the proper legal authority (such as consent to search form, search warrant, etc.) with their request.

392-5 BEST EVIDENCE RULE

Digital photographs, video recordings, and audio recordings are admissible as evidence in court so long as the following criteria are met:

- A. The photograph or recording has not been modified from its original state, and
- B. The authenticity of the image or recording can be verified by the photographing member or a reliable witness if called upon at a later time.

392-6 DIGITAL PHOTOGRAPHY-CAMERA PROCEDURES:

Members shall only use department issued digital cameras devices to take photographs.

Each department member shall receive training in the operation of department issued cameras.

The following procedures shall be adhered to when using digital camera devices for photography:

- A. Preparing the camera:
 - 1. Ensure that the media device is free of all personal and non-case related material. Photographs from multiple incidents may be recorded on the same media device if necessary, but must be submitted as soon as possible prior to the end of the member's tour of duty.
 - 2. Select the highest possible image resolution setting to aid in capturing the most detailed images possible. Images are to be captured in .jpg format at all times.

- B. Taking photographs:
 - 1. Photograph a completed START page (Attachment "A") prior to taking any other photographs. Use a pen or marker broad enough to be clearly visible. This image will signify the beginning of the series.
 - 2. Take all necessary photographs, adjusting device settings and zoom if needed. Do not delete any photos from the device.
 - 3. Photograph a completed END page (Attachment "B") prior to taking any other photographs. This image will signify the final image in the series.
 - 4. Officers Members are never authorized to edit, alter or delete original images captured, regardless of image quality. All images shall be submitted whether conspicuously deficient in image quality or of excellent quality.

Field Contact Card photographs need not be surrounded by START and END pages. Photographs for Field Contact Cards and Trespass Warnings may be taken in a lower resolution setting, as to allow for the photograph to be electronically attached to the case, via the records management system.

C. Preserving images:

All images will be kept regardless of perceived image quality or relevance in order to maintain the sequential order of the images on the media. Under no circumstances will an image be altered, deleted or erased.

The images from the removable storage media device will be downloaded directly to either the Department's designated archival storage server or into the CafeWeb system. If multiple cameras devices were used to photograph the same crime scene, and the images were uploaded onto the server, the images from each media device must be stored in separate directories for clarity later. Each directory's title should include the case number and the photographer's Department ID number-name.

- 1. Remove the media from the camera, and insert it into the designated media card reader.
- 2. Images will then be uploaded into the CAFÉ system, or transferred to the archival storage server from the removable storage media device and placed in the appropriate folder on the server. This server will be denoted on the member's computer by being named by a drive letter as set forth by the City's IT Department (i.e. "QX:", "Z:") and will serve as the "master disk". Files stored on the master disk cannot be altered or deleted by members, and remain until they have met appropriate retention requirements for destruction.

- 3. Upon completion of the transfer, the files will be examined to confirm that all of the images were completely and accurately transferred to the storage server.
- 4. A contact sheet of the transferred images may be made from the media card for the case file if needed.
- 5. The image files should be deleted from the removable media device once their presence on the server has been validated.
- D. Security of Images:
 - 1. Image Storage
 - a. All activity conducted in the CAFÉ system is tracked and archived, which will display a user upon request should images be altered or deleted.
 - b. Images stored on the secure network drive require a username and password to access.
 - 2. Access to secure storage will be restricted to the following:
 - a. Evidence personnel will have full access to read, write, and delete images.
 - b. Members of the Investigations Division will have full-access to create folders, write, and read all stored image files.
 - c. Remaining sworn members will have limited access to create folders, write, and read only the images that they transfer.
 - d. Access to modify process images will be granted to members specified by the Chief of Police or his/her designee.
 - e. Personnel specified by the Chief of Police or his/her designee will have access as necessary to perform hardware/software maintenance tasks.

f. Other personnel having authorization from the Investigations Division Commander. Those personnel will have read-only access.

- E. Working with images:
 - 1. The principal of image enhancement is to render an image clearer for analysis or interpretation. Whether or not any enhancement performed on an image is saved is at the discretion of the person performing the enhancement.
 - 2. No image enhancements will be performed prior to transferring onto the archival storage server. In-camera image alteration is similarly prohibited.

- 3. Digital image enhancement will be completed only as needed. In order to preserve the original integrity of each photograph, the original photograph will not be processed in any way. Any enhancements will be made to a copy of the original file. Under no circumstances will a processed image be substituted for the original.
- 4. Files in the JPG format that are to be processed/enhanced will be first saved as a TIF file before proceeding.
- 5. Techniques common to traditional darkrooms and digital imaging stations such as, but not limited to, image levels, cropping, dodging, burning, color balancing, sharpening, and contrast adjustment that are used to achieve an accurate recording of an event or object, will be considered standard processing steps. Specific digital techniques, including resizing (with or without interpolation) or enlargement of the image or any part, may be utilized to improve the image quality and accommodate the processed images printed size.
- 6. Digital image enhancements will be documented in a supplement to the original offense/incident report to describe what actions were taken and by whom. This will ensure that no original evidence is destroyed in the enhancement process.
- F. Distribution of images:
 - 1. Images shall be printed on an as-needed basis for trial and on-going investigations. Emphasis shall be placed on electronic transfer/digital image transmission of duplicate images whenever possible. All duplicate images shall be copied in an unaltered native file format as that of the original.
 - 2. All requests for printed or duplicate images for the State Attorney's Office, nonlaw enforcement personnel, private attorneys, insurance companies, private citizens and others shall be determined on a case-by-case basis and handled through the **Property & Evidence Section** proper public request procedures/tasking sheet procedures. Emphasis shall be placed on electronic transfer/ digital image transmission or duplication of images via disks or CD's, whenever possible.
 - 3. All requests for printed or duplicate images from Public Defenders or Private Attorneys must be accompanied by a copy of an Answer to Demand for Discovery from the State Attorney's Office. These requests are handled through the Property & Evidence Section.

392-6 DIGITAL RECORDER PROCEDURES:

Members shall only use department issued digital recording equipment.

A. Preparing the recorder:

- Ensure that the media device is free of all personal and non-case related material. Recordings from multiple incidents may be captured on the same media device if necessary, but must be submitted as soon as possible prior to the end of the member's tour of duty.
- 2. Record at the highest possible quality to aid in capturing the most detailed audio and/or video possible.
- B. Preserving recordings:

All recordings will be kept regardless of perceived quality or relevance, in order to maintain the integrity and continuity of the recording in court. Under no circumstances will a recording be altered, deleted, or edited in any way.

- 1. Transfer the recording directly to an appropriate secondary digital media source. such as a DVD cassette tape, VHS tape, or compact disc, or directly to the Q drive.
- 2. Verify that the recording transferred correctly to the secondary digital media source.
- 3. Use a permanent marker (such as a Sharpie) to write the case number, date, and any other relevant information on the secondary source, and place it into a protective case where applicable.
- 4. Submit the secondary source in accordance with department evidence guidelines.
- 5. The recordings may be deleted from the primary media device once their presence on the secondary source has been validated.

392-7 COMPUTER AND CELL PHONE EXTRACTIONS

- A. Digital Forensic Specialist:
 - 1. The department will assign additional duties to a member as a Digital Forensic Specialist (DFS) whose duties, in addition to their normal function include the following:
 - a. Conduct forensic examinations of a variety of digital devices to include but not limited to cell phones, computers (laptops, tablets, desktops), thumb drives, hard drives, and memory cards.
 - b. Assist in the collection of data in cases involving digital evidence.
 - c. Act as an educational and training resource for the Department and the community.
 - d. Respond as needed after hours when notified by supervisor.

- e. Provide technical assistance in the proper safeguarding and collection of electronic/digital evidence.
- 2. The DFS shall not conduct any investigative actions or inquiries outside the scope of assisting a sworn officer in an official criminal investigation.
- 3. After every device examination, the DFS will prepare an extraction report for the investigating officer/detective.
- B. Investigative Procedures:
 - 1. These procedures are for electronic devices to be collected for evidentiary purposes during a criminal investigation. Department personnel shall not allow anyone to manipulate a digital device that will be seized as interacting with the device may overwrite, delete, or alter its contents.
 - 2. Information on a digital device that is suspected of containing evidence shall only be recovered/obtained by personnel who have reviewed the training in accordance with preserving data. The DFS is the only authorized personnel at our agency who can conduct an extraction. If the DFS is unable to conduct the extraction, then the device can be submitted to a surrounding agency. Consult your DFS for further information regarding other agencies.
- C. Device Collection
 - 1. When collecting digital devices, members should take the proper precautions as follows:
 - a. Computers (Desktops/Laptops): If the computer is shut down, do not turn it on. If the computer is powered up, do not shut it down. Check the monitor to determine if there is any information that may require photographic documentation. Unplug the power cable from the rear of the computer, not from the wall outlet. All Power cables for all computers must be collected.
 - b. Cell phones/Tablets/Mobile Devices: if the device is shut down, do not turn it on (remove sim card if applicable and tape to rear). If the device is powered on, do not shut it down. If the device is on, then place the phone in airplane mode, turn off Bluetooth; and WIFI.
 - c. These items should be submitted to evidence in accordance with department policy. When submitting a device, do your best to obtain the serial number, make, model, and owner of the device. Determine if there is any biohazard material on the device and handle accordingly. Document this information in

Café along with the status of the phone and any manipulation you had to do (I.E. turning on airplane mode, turning off wifi and Bluetooth). Also, attempt to get a pin code for the phone.

- Members shall ensure that any physical evidence (such as fingerprints, DNA, etc.) is collected from the device or a request for evidence processing is made prior to its submission into evidence.
- 2. Prior to any forensic examination taking place, the DFS will ensure the following:
 - a. The device to be examined is verified (ie. description, serial number, etc..).
 - b. Legal authority for the search has been obtained and is properly documented. A copy of the documentation (ie. search warrant, consent form, etc.) is required. These legal documents should be obtained and provided by the case Officer/Detective. The case Officer/Detective will also complete the returns for the search warrant obtained in a timely manner.
- 3. Preservation of Evidence
 - a. Digital evidence will be handled in a manner consistent with the preservation of evidence as outlined in SOP 390 or the Winter Park Evidence Submission Manual.
 - b. The DFS shall ensure the chain of custody of any evidence submitted for forensic examination is maintained and documented during the examination process. Evidence will be properly secured at all times while in DFS custody.

C. Release of Evidence

- 1. Evidence obtained as a result of a digital forensic examination will be released in accordance with established policy. No media shall be released from law enforcement custody that contains child pornography unless it meets release criteria established in section FSS 755.0847.
- 2. Regarding the release of recovered digital evidence/information:
 - a. The DFS shall, at the direction of the lead investigator, prepare evidence to be released or presented to the court (copies of media, evidence files, EnCase reports, etc.).
 - b. The DFS shall coordinate with the case detective regarding access or release of evidence and other information to the court.

392-8 BODY WORN CAMERA RECORDINGS:

Refer to SOP #: 393, Body Worn Cameras for procedures relating to the handling and storage of digital recordings from body worn cameras.

392-9 ONLINE REPORTING DIGITAL EVIDENCE PROCEDURES:

- A. Digital photographs, audio, videos, or documents received from citizens in the form of online report submissions will be stored according to the procedures established in Section 392-5C for digital evidence.
- B. In the event that a citizen submits digital media data in an online report that is considered obscene or otherwise inappropriate to store on CafeWeb or the Q drive, the Criminal Investigations supervisor or designee shall do the following:
 - If the digital data is considered evidence as part of a documented Department case, the Criminal Investigations supervisor or designee shall transfer the evidence from the online report to a secondary digital media source such as DVD or compact disc, verify that the evidence transferred properly to the secondary digital media, and then submit the secondary digital media in accordance with department evidence procedures.
 - 2. If the digital data provided in the on-line report is not part of the Winter Park Police Department case evidence, the Criminal Investigations supervisor or designee shall transfer the evidence digital data from the online report to a secondary digital media source such as DVD or compact dise, verify that the evidence transferred properly and submit the secondary digital media in accordance with department evidence procedures. to the secondary digital media, and then seal the media in a paper envelope and store it in Criminal Investigations secured files according to records retention requirements.

<mark>392-10 TRAINING</mark>

- A. Those members conducting digital evidence processing shall have initial training on the subject. Training may be accomplished in-house or through an outside vendor.
- B. Those members who conduct digital evidence processing shall be provided refresher training to ensure proficiency in new techniques and equipment. Refresher training shall occur a minimum of once every three (3) years.

Drafted: TP01-06 /filed: 392.doc /revised: MV01-08,04-08 /revised: JL11-11 /revised: KWR,TV05-20

Alinane Dear

Michael Deal Chief of Police