ST. PETERSBURG POLICE DEPARTMENT	DATE OF ISSUE	EFFECTIVE DATE	NUMBER
GENERAL ORDER	June 2025	Immediately	**V.3:09**
	Distribution: All Employees		

Subject: **DIGITAL CRIMES AGAINST CHILDREN**

Index as:
- Chatting
- Child Pornography
- Child Sexual Abuse Material (CSAM)
- Coercion
- ICAC Data Systems (IDS)
- National Center for Missing and Exploited Children
- NCMEC
- Peer to Peer
- Production/Transmission of Child Pornography
- Sexting
- Sextortion
- Sexually Explicit Image
- Transmission of Harmful Materials to Minors
- Traveling to Meet a Minor

Accreditation Standards: 43.1.5

Cross Reference:
- G.O. II-35, Employee Assistance Program
- G.O. III-06, Juvenile Procedures
- G.O. III-14, Property and Evidence
- I.O. V.3:07, Human Trafficking
- I.O. V.5:17, Victim's Right/Victim Assistance Unit
- CAPP SOP I-02, Organization, Responsibility and Job Descriptions
- §§ 775.0847, 827.071, 827.072, 828.126, 847.0135, 847.0137, 847.0138 Florida Statutes

Replaces: New Policy

This Order serves as the guidelines and procedures for investigating digital crimes against children. It consists of:

I. Policy
II. Purpose
III. Definitions
IV. Department-Reported Digital Crimes Against Children Investigations
V. National Center for Missing and Exploited Children (NCMEC) Tips
VI. Undercover Chat Operations
VII. Evidence Handling
VIII. ICAP Safety and Accountability Measures

I. POLICY

It is the policy of the St. Petersburg Police Department to actively investigate technologically facilitated crimes against children, ensuring that all investigations are property planned and conducted pursuant to the safety of agency members and the community as directed by the procedures established in this order.

II. PURPOSE

A. The internet and social media have become ubiquitous as part of daily life, and as such, evidence of digital crimes has become more prevalent and necessary for criminal investigations. Interaction with digital devices creates a trail of evidence in a wide variety of crimes. Juveniles are at an ever-increasing risk via exposure to the internet and social media from online predators who are adept at exploiting children.

B. The Department recognizes the need to maintain investigators with specialized training and equipment necessary to conduct the type of investigation necessary in order to properly respond to and prevent the online exploitation of children.

C. Additionally, this order serves to outline ways to maintain safe and accountable practices of collecting, viewing, and storing illegal sexually explicit material.

III. DEFINITIONS

A. Internet Crimes Against Children (ICAC) Task Force – The United States Department of Justice program created to help State and local law enforcement agencies enhance their investigative response to offenders who use the Internet, online communication systems, or other computer technology to sexually exploit children.

B. National Center for Missing and Exploited Children (NCMEC) – A private, nonprofit organization established in 1984 by the United States Congress. Electronic Service Providers (ESP's) send flagged images to NCMEC which generate cyber tips.

C. ICAC Data Systems (IDS) – The program used to manage, track, assign, forward and close tips coming from NCMEC.

D. Child Sexual Abuse Material (CSAM) – Images and/or videos which show a person who is a child and engaged in or is depicted as being engaged in explicit sexual activity.

E. Coercion – Enticing or luring any person by fraud or deceit.

F. Peer-to-Peer (P2P) Investigations – A self-initiated case by a sworn member trained in accordance with the ICAC task force guidelines to use software platform account designated by the Department of Justice.

G. Sexually Explicit Image (§ 847.001, Florida Statutes) – Any image depicting nudity or depicting a person engaging in sexual conduct.

H. Sexting (§ 847.041(1) (a), Florida Statutes) – A minor commits the offense of section if they knowingly:

1. Uses a computer, or any other device capable of electronic data transmission or distribution, to transmit or distribute to another minor any photograph or video of any person which depicts nudity and is harmful to minors, or

2. Possesses a photograph or video of any person that was transmitted or distributed by another minor which depicts nudity and is harmful to minors. A minor does not violate this paragraph if all of the following apply:
   a. The minor did not solicit the photograph or video.
   b. The minor took reasonable steps to report the photograph or video to the minor's legal guardian or to a school or law enforcement official.
   c. The minor did not transmit or distribute the photograph or video to a third party.

IV. DEPARTMENT-REPORTED DIGITAL CRIMES AGINST CHILDREN INVESTIGATIONS

A. On Scene Investigation

The majority of digital crimes against children investigations originate as NCMEC tips received by detectives through IDS. However, suspicion and/or evidence of digital crimes against children may be reported to police or become evident during the investigation of another crime. If so, officers will:

a. Make every effort to document the following information in the incident report:
   1) Time, date, and (if applicable) location CSAM was transmitted, posted, or viewed
   2) All phone numbers used to send and/or receive CSAM
   3) All social media platforms along with usernames and passwords related to CSAM
   4) All communications (text messages, emails, direct messages, etc.) related to CSAM
   5) A description of the of the CSAM image(s) but ***WILL NOT*** take photos or upload pictures/videos of CSAM to evidence.com.

b. Collect the device (phone, computer, tablet, etc.) containing CSAM. Devices containing CSAM may be seized, however, consideration should be given when the device belongs to a cooperative victim. With supervisor approval, the Digital Forensics Unit may be consulted to coordinate evidence collection.
c. If possible, the officer will:
   1) Place in airplane mode
   2) Turn off Bluetooth and Wi-Fi
   3) If detectives do not respond, place on charger as soon as possible
d. Document in report all changes made to device's settings (as listed above)

B. Supervisor Notifications

1. The investigating officer will notify the patrol supervisor prior to leaving the scene.

2. If there is evidence of CSAM, the patrol supervisor will notify the Internet Crimes Against Person (ICAP) supervisor or the on-call Investigative Services Bureau (ISB) supervisor prior to the officer leaving the scene.

3. The supervisor, ICAP/ISB, will determine whether a detective will respond to the scene.

C. Follow Up Investigation

The detective assigned the case will:
a. Review the case and take necessary steps to preserve all forms of physical and digital evidence.
b. Coordinate with the Digital Forensic Unit, as necessary, to conduct in person follow up interviews and potential evidence collection.
c. Keep the assigned State Attorney informed of all pertinent case information.
d. Update IDS with appropriate information.

V. NATIONAL CENTER FOR MISSING AND EXPOITED CHILDREN (NCMEC) TIPS

A. Cyber tips reported to NCMEC will typically be received through ICAC Data Systems (IDS) and assigned to a detective by the ICAP supervisor.

B. Upon receipt of the tip, the assigned detective should obtain a Department case number and submit an incident report for each tip.

1. If multiple tips are linked together, the assigned detective will determine if additional incident reports are needed.

2. If after reviewing the tip, the assigned detective determines that no incident report is necessary and the tip can be closed, the detective will notify the ICAP supervisor and add notes to IDS. This may be tips where:
   a. There is no prosecutorial merit, or
   b. The offense occurred outside the jurisdiction

C. Follow-up notifications to NCMEC is required by updating the status of the cyber tip.

VI. UNDERCOVER CHAT OPERATIONS

A. The ICAP supervisor will be notified of any planned undercover chat operations. Only members authorized by the ICAP supervisor will participate.

B. All chats will be preserved using capture software in accordance with evidence preservation procedures recommended by ICAC task force.

C. Any photographs used by the detective during the undercover investigation intended to be introduced to the suspect or transmitted to the internet must be approved by the ICAP sergeant or above.

D. Photographs considered contraband or pornographic in nature will not be used or disseminated in any way.

E. Prior to meeting with an internet suspect, sworn members will attempt to identify all involved suspect(s) and determine the meeting location. The meeting location will be scouted prior to the meeting to determine any safety hazards to the officer, public, and suspect, or other variable, which may affect the outcome of the meeting.

F. The incident report and all photographs used and collected during the investigation will be included with the case packet when requested by the State Attorney's Office for prosecution.

G. Detectives will not conduct a Peer to Peer (P2P) investigation without successful completion of the ICAC task force P2P training.

VII. EVIDENCE HANDLING

A. Evidence will be collected according to G.O. III-14, Property and Evidence, with special attention to sections VII and VIII.

B. Under no circumstances should photographs of CSAM be taken with a Department-issued cell phone or uploaded to Evidence.com

C. Detectives assigned cases involving CSAM will store all case files and digital evidence on a Department-approved media storage platform.

1. CSAM will not be stored to portable storage devices (i.e. external hard drives, thumb drives) without supervisor approval.

2. During the course of an investigation, the State's Attorney Office may request copies of CSAM for trial purpose and an external storage device may be necessary. Such requests will be handled case-by-case with supervisor approval, and properly documented.

VIII. ICAP SAFETY AND ACCOUNTABILITY MEASURES

A. Due to the toxic and mentally taxing nature of viewing CSAM, detectives will, as much as reasonably possibly, follow the guidelines below. The ICAP supervisor will be notified of exceptions.

1. No CSAM will be viewed more than absolutely necessary for case documentation.
   Cases involving excessive amounts of CSAM images will be coordinated with the State Attorney assigned to the case. The number of images viewed should be reasonable for the number of charges likely prosecuted.

2. Detectives will make every attempt to view and document CSAM for their assigned cases at the same time, in an effort to reduce number of weekly exposures.

3. CSAM will not be viewed within the last two (2) hours of the workday.

4. Detectives will make at least one (1) other detective aware when they are viewing CSAM. The second detective does not need view the CSAM but must be present.

5. Detectives will not view CSAM outside working hours.

A. Detectives will only use Department-approved off-network computers to download and view CSAM. The off-network computers will remain in the ICAP workspace at Department Headquarters, unless approved by the ICAP supervisor.

B. If a detective begins to experience any adverse symptoms related to the viewing of CSAM, they will immediately notify the ICAP supervisor.

C. It is recommended for detectives to undergo regular preventative psychological counseling in order to help mitigate the effects of viewing CSAM. See G.O. II-35, Employee Assistance Program for available resources.

_____
Anthony Holloway
Chief of Police