Cocoa Beach Police Department

Standard Operating Procedure

Effective Date: September 20, 2022	**Replaces:** **Ammends:**	**Number:** 100.58
Subject: Biometric Identification Program		**Re-evaluation Date:** 2023
Distribution: ALL PERSONNEL	**Related Standards:**	

This order consists of the following numbered sections:

1. **PURPOSE**

   The purpose of this Standard Operating Procedure is to establish guidelines for using biometric identification technology by the Cocoa Beach Police Department.

2. **SCOPE**

   This policy applies to all employees of the Cocoa Beach Police Department (CBPD).

3. **POLICY**

   In 2002, the Pinellas County Sheriff's Office (PCSO) implemented facial recognition as a biometric tool used to identify or verify individuals as part of the law enforcement mission. The agency established and hosts one of the largest collaborative facial recognition systems in Florida and allows access to authorized law enforcement agencies. Facial Recognition is utilized in the Department of Detention and Corrections as part of the booking process. Facial recognition search capabilities are shared with other law enforcement users as well as partner agencies who actively contribute facial images to the database for law enforcement purposes only. The Face, Analysis, Comparison, and Examination System (FACESNXT) is hosted through FDLE's CJNET and access is only granted to authorized agencies.

4. **DEFINITIONS**

   A. Ambiguous Response – There was no definitive match using the submitted search prints. More than one possible match was found.

   B. Biometrics – Distinctive and measurable human characteristics that can be used to identify people apart from demographic data like name and date of birth. Fingerprints and facial features are examples of commonly used biometrics. Since biometrics are unique to individuals, they are more reliable in verifying identity than knowledge-based methods.

   C. Candidate List – A rank-ordered list generated from a facial recognition search.

   D. Enroll – The act of capturing a facial image, creating a template and entering the template into a facial recognition gallery.

   E. Facial Identification – A manual examination of the differences and similarities between facial images or between a live subject and facial images for the purpose of determining if they represent the same person. (FISWG).

   F. Facial Identification Scientific Working Group (FISWG) – A group of individuals whose mission is to develop consensus standards, guidelines and best practices for the discipline of image-based comparisons of human features, primarily face, as well as to provide recommendations for research and development activities necessary to advance the state of the science in this field.

   G. Facial Recognition – The automated searching of a facial image (probe) against a known collection resulting in a list of candidates ranked by computer-evaluated similarity score. This is commonly referred to as a one-to-many comparison (FISWG)

H. Facial Verification – The automated comparison of a facial image to a known standalone biometric sample, resulting in a computer-evaluated similarity score. This is commonly referred to as a 1:1 comparison. Also, the process of authenticating a person's asserted identity by comparing two image templates to answer the question, "Are these two images the same person?"

I. FBI RISC (Repository for Individuals of Special Concerns) System – A searchable database of individuals which includes Wanted Persons, Sexual Offender Registry Subjects, Known or appropriately suspected terrorists, and other persons of special interest.

J. Gallery – The FR system's database, which typically contains all known-person templates.

K. Hit Response – A "match" was found in the FDLE database of criminal records for the fingerprints submitted and the FDLE number is returned.

L. No Hit Response – No match was found in the FDLE database of criminal records.

M. Partnering Agency – An agency that actively contributes facial data to the Sheriff's Office FRS or whose authorized members conduct searches within the FRS.

N. Probe – The facial image or template searched against the gallery in an automated facial recognition system.

O. Rapid-ID – A fingerprint identification system that uses two fingers to search statewide criminal history records and return positive identification along with criminal history information on an individual.

P. State ID Number (also known as FDLE Number or SID number) – The sequential number assigned to an individual's record by the Florida Department of Law Enforcement (FDLE) which allows retrieval of an individual's complete, statewide criminal record.

Q. Statewide criminal history (also known as rap sheet) – A listing of an individuals' arrests, prosecutions, demographic data used by that individual in the criminal justice system and a "flag" when a DNA sample is on file for that individual.

R. Template – A set of biometric measurement data prepared by an FR system from a facial image.

S. Watchlist – a repository of unsolved probe images that is automatically compared to new photos submitted to the criminal arrest repository.

5. **PROCEDURE**

A. Designated members of the Department may utilize facial recognition for law enforcement investigations requiring identification or verification of subjects where a digital image is available. Facial recognition searches and comparisons may be performed through the user's web browser by accessing the Face Analysis, Comparison, and Examination System (FACESNXT). The FACESNXT application is available via the CJNET URL and is to be used to assist in law enforcement investigations. Information found through a facial recognition search is to be considered a "lead" for further investigation.

1. Supported Web Browsers: Internet Explorer 8 or later, Firefox, and Chrome are supported.
2. CBPD users may access FACESNXT via the CJNET URL.
3. All users are required to complete the online training modules prior to gaining access to the FACESNXT application.
4. Patrol users shall utilize their department-assigned digital camera or cell phone to capture face imagery of subjects of interest in accordance with this Directive.
5. Users may submit digital face images (probes) in JPG, BMP, and PNG file formats to FACESNXT.
6. Users shall include a reason for search. This reason shall be the associated case number for the subject of the facial recognition search.
7. Users may retrieve demographic information from subjects selected within the FACESNXT gallery.
8. Users may perform detailed side-by-side facial image comparisons on selected probe and gallery images to assist in match determination.
9. The user will make the determination of a match of the probe image to the gallery image(s).
10. Any information found through facial recognition search is for lead purposes only.
11. The FACESNXT system is subject to audit for statistical reporting. All user activity is logged.
12. If a user receives a potential match and requires facial verification of the match, the user shall contact their supervisor and / or other experienced FACESNXT user for assistance, as needed. If no match is found, the user shall utilize other investigative methods to determine identity.

B. General guidelines

1. Officers may utilize their department-assigned digital camera or cell phone to collect face images of individuals for a facial recognition search.
2. Facial Recognition will only be used for official law enforcement investigations.

3. Individuals will not be physically detained for the purpose of taking a photograph for facial recognition. Officers should ask for consent; this does not preclude an officer taking the photograph of a person in a public place provided the officer has not hindered the movement of the person.
    a) Physical force shall not be used for the purpose of taking a photograph.
    b) An individual in public shall not be stopped or told to pose for a photograph when it is not being done for a law enforcement investigation, i.e., a person in a motor vehicle shall not be required to roll down tinted windows or uncover their face just for the purpose of taking their photograph.
4. All photographs and search activity submitted to FACESNXT are logged and subject to audit.
5. All facial recognition investigations will be conducted with the safety of all officers and person(s) being photographed as the paramount concern.
6. A Field Interview Report (FIR) or Incident/Offense Report will be completed for every person photographed. All members shall attach a copy of the photograph to the Field Interview report. The officer will be responsible for completing any required report. The officer shall note in the FIR or Incident/Offense Report that a positive facial recognition match was or was not determined.
7. Officers will bring any problems with said equipment or FACESNXT application to the immediate attention of a supervisor.

C. All photographs taken as a result of a law enforcement investigation shall be attached to a case report,
i.e., a Field Interview Report (FIR), or as a subject link to an incident or offense report, pursuant to Department
policy.

D. All photographs or a copy thereof, must be retained, including those pursuant to Property and Evidence, and Records Management Departmental policies.

E. Officers are held responsible for control, security, and access to all facial recognition equipment and photographs in their possession.

F. FACESNXT is an investigative tool and any law enforcement action taken based on a submission to FACESNXT shall be based on the officer’s own identity determination and not solely the results of a FACESNXT search.

6. TRAINING FOR BIOMETRIC IDENTIFICATION SYSTEM USERS

All users are required to complete the online training modules prior to gaining access to the FACESNXT application. Users may review the provided training materials on how to use the FACESNXT application at any point in time, after gaining access to the system. Training materials may be found under the FACESNXT help menu section, titled “Refresher Videos.”

8. AGENCY ADMINISTRATOR RESPONSIBILITIES

The Department’s Agency Administrator is responsible to manage FACESNXT user accounts and immediately deactivate users as they are terminated, retire, or no longer need FACESNXT access. During quarterly audits, the CBPD Agency Administrator will review case numbers and review probe images to ensure no suspicious activity is identified. If suspicious activity is identified the administrator will notify the Chief of Police or designee.

Scott Rosenfeld
Chief of Police
City of Cocoa Beach

Date: 09/06/22