POLICE NORTH PORT

STANDARD OPERATING PROCEDURE

302.02 FACIAL RECOGNITION TECHNOLOGY

Effective Date:	Revision Date:	Rescinds:	Amends:
May 9, 2022		NEW	

I. PURPOSE

The purpose of this procedure is to provide guidelines for the use of the Facial Recognition Software and to ensure that its use respects the privacy rights of citizens.

II. SCOPE

This directive applies to members of the North Port Police Department Investigative Units that utilize facial recognition technology.

III. DISCUSSION

Facial recognition technology can be a valuable investigative tool to detect and prevent criminal activity; reduce an imminent threat to health or safety; protect the public; help identify deceased persons or those unable to identify themselves and improve security and officer safety.

IV. POLICY

It is the purpose of this policy to provide agency personnel with guidelines and principles for the use of facial recognition technology. This policy will verify that all facial recognition uses are consistent with authorized purposes while not violating the privacy and civil rights of individuals.

V. DEFINITIONS

Facial recognition technology - a computer program/application capable of comparing specific physical features of a person depicted in an image against a database of images of persons identified through other means.

Facial recognition search result - an image returned by facial recognition technology that represents a potential investigative lead based on an algorithmic similarity to the submitted image.

Identification - a positive facial recognition search result which alone does not constitute probable cause for arrest. The search result shall be evaluated by the assigned case officer and requires investigative follow-up to corroborate the lead before any action is taken.

Face Analysis Comparison & Examination System (FACESNXT) - a facial recognition technology hosted by the Pinellas County Sheriff's Office in partnership with the Florida Department of Law Enforcement (FDLE) and the Florida Criminal Justice Network (CJNET).

VI. PROCEDURES

A. Authorized Uses for Facial Recognition Technology

1. When there is a reasonable suspicion that an identifiable individual:

a. Has committed a criminal offense;
b. is involved in a criminal offense;
c. is planning criminal activity that presents a threat to any individual or to the community.

2. Facial recognition technology can be utilized for an active or ongoing authorized criminal investigation, and to mitigate an imminent threat to health or public safety.

3. To assist in the identification of a person who lacks capacity or is otherwise unable to identify themselves (e.g. incapacitated, deceased, or otherwise at-risk person).
   - Note: In instances, where an individual's photo was taken without consent, the officer shall document the reason the person was unable to give consent and the purpose of the submission to a facial recognition system.
4. To investigate and/or corroborate tips and leads on authorized criminal investigations.

5. For comparison to determine whether an individual may have obtained one or more official state driver's licenses, or identification cards that contain inaccurate, conflicting, or false information.

6. To assist in the identification of potential witnesses and/or victims of crime.

7. To support law enforcement in critical incident responses.

8. For a person who an officer reasonably believes is concealing their identity and has a reasonable suspicion the individual has committed a crime

B. Considerations During Investigations

1. The agency considers the results, if any, of a facial recognition search to be advisory in nature and an investigative lead only. Facial recognition search results are not considered positive identification of a subject and do not, on their own, establish probable cause, without further investigation. Any possible connection or involvement of the subject(s) to the investigation must be determined through further investigative methods.

2. Original images shall not be altered, changed, or modified in order to protect the integrity of the image. Any enhancements made to an image will be made on a copy, saved as a separate image, and documented to indicate what enhancements were made, including the date and time of the change.

3. If potential matches are found, a confirmation of the identification shall be performed by the assigned case officer for verification.

4. Individuals may give consent to have an image captured for facial recognition during a consensual encounter.

5. Agency personnel shall not detain individuals without legal justification for the sole purpose of capturing an image to be used in facial recognition technology.

6. Information obtained by the use of any facial recognition technology should be considered criminal intelligence or investigative information in reference to the Release of Public Records.

7. Facial recognition technology shall be used for official law enforcement purposes and not used for:
   a. Personal use, queries not related to legitimate agency duties, sharing, copying, or passing of information to unauthorized personnel.
   b. Any purpose that violates Federal, state, or local laws.
   c. Harassing and/or intimidating any individual or group.
   d. Any other access, use, disclosure, or retention that would violate applicable law or agency policy.
   e. Facial recognition technology cannot be used to conduct surveillance of persons or groups based solely on their religious, political or other constitutionally protected activities, their race, ethnicity, gender, or sexual orientation.

C. Accountability

1. Supervisors reviewing cases where facial recognition technology is used to provide an investigative lead shall confirm the officer has conducted investigative follow- up to corroborate the lead before any action is taken.

2. Agency approved facial recognition technology must have a user activity logging system that is subject to audit for statistical reporting and accountability.
   a. Audits for facial recognition programs will be requested through the Intel Supervisor.
   b. The Intel Supervisor or designee will request the audit to be completed by the appropriate program administrator. Once completed, the Intel Supervisor or designee will provide the results to the requester of the audit.
   c. An annual review of commercial facial recognition technology usage by licensed operators shall be completed by the program administrator or designee.
      - NOTE: Users with periods of inactivity will be removed from the system and their license reissued to another user as needed.
   d. Public requests for facial recognition information will be handled in accordance with Florida State Statute.

3. Officers will only use agency authorized facial recognition technology. Any facial recognition technology used by the agency must meet the following minimum criteria:
   a. Facial recognition systems must have an accountability system that can be audited through a systems administrator.
   b. There must be training on an authorized facial recognition system prior to being used by agency personnel.

D. Training

1. The agency has authorized trained officers to only use Face Analysis Comparison & Examination System (FACESNXT) facial recognition systems.

2. Face Analysis Comparison & Examination System (FACESNXT)
   a. New users must obtain supervisor approval for access to FACESNXT.
   b. New users must complete the online user training prior to its use.
      - NOTE: FACESNXT program training and access is provided online and requested through the Pinellas County Sheriff's
   c. Usernames and passwords to FACESNXT will not be shared by agency personnel and must be kept confidential.

May 9, 2022

Approval Date

Todd R GARRISON

Todd R. Garrison

Chief of Police