ORLANDO POLICE DEPARTMENT POLICY AND PROCEDURE

1147.1, FACIAL RECOGNITION

EFFECTIVE:	3/19/2021
RESCINDS:	1147.0
DISTRIBUTION:	ALL EMPLOYEES
REVIEW RESPONSIBILITY:	CRIME CENTER SECTION COMMANDER
ACCREDITATION CHAPTERS:	
CHIEF OF POLICE:	ORLANDO ROLÓN

POLICY: It is the purpose of this policy that all Department members abide by the following guidelines set forth herein using facial recognition software/technology. The Orlando Police Department has established access and use of facial recognition software/technology to support the investigative efforts of law enforcement and public safety agencies. Facial recognition technology involves the ability to examine and compare distinguishing characteristics of a human face using biometric algorithms contained within a software application. Facial recognition is an investigative tool and **WILL NOT** be configured to conduct random facial recognition analysis on live or played back recorded video. This technology will provide many opportunities for the enhancement of productivity, increased crime solvability, effectiveness, and increased safety for both citizens and officers. This policy provides Orlando Police Department personnel with specific guidelines for the collection, access, use, dissemination, retention, purging of images, auditing, and related information applicable to facial recognition.

CONTENTS:

1. TERMS AND DEFINITIONS

For the purpose of this Policy, the following terms and definitions apply:

Audit: a review conducted by the Facial Recognition Administrator to include all use of facial recognition software/technology. The audit will include all user's activity, such as user log ins and log outs, each user's activity in detail, what commands were issued to the system, and what records or files were accessed.

Candidate images: the possible results of a facial recognition search. When facial recognition software compares a probe image against the images contained in a repository, the result is a list of most likely candidate images that were determined by the software to be sufficiently similar to, or most likely resemble, the probe image to warrant further analysis. A candidate image is an investigative lead **ONLY** and does not establish probable cause without further investigation.

Facial recognition: the automated searching for a reference image on an image repository by comparing human facial features of a probe image with the features of images contained in an image repository. A facial recognition search will typically result in one or more most likely candidate images.

Facial recognition administrator: member designated by the Chief of Police, or designee, to be the point of contact for facial recognition software/technology access, training, and audits.

Facial recognition software/technology: Third party software that uses specific proprietary algorithms to compare human facial features from one specific picture (probe image) to many others that are stored in an image repository to determine most likely candidates for further investigation

Facial recognition user: a member who has been approved for access and granted account access by the facial recognition administrator.

Investigative lead: any information which could potentially aid in the successful resolution of an investigation but does not imply positive identification of a subject or that the subject is guilty of a criminal act.

Probe image: any uploaded face image used by facial recognition software for comparison with the face images contained within a face image repository.

Repository: a location where a group of images of known individuals and biometric templates are stored and managed. An image repository is searched during a facial recognition search process whereby a probe image is used by facial recognition software for comparison with the images (or features within images) contained in the image repository.

RFI: request for information

RFI log: a credentialed log for the purposes of internal and external facial recognition data sharing and requests that documents name of the agency/requestor, name of the person completing the request, date and time the request was completed, case number and reason for the request. The RFI log may be a part of the software auditing process.

2. GENERAL INFORMATION

2.1 Facial recognition involves the ability to examine and compare distinguishing characteristics of a human face using biometric algorithms contained within a software application. This technology can be a valuable investigative tool to detect and prevent criminal activity, reduce an imminent threat to health or safety, assist in the identification of individuals who refuse to identify themselves when required to do so by law, and help in the identification of persons unable to identify themselves or deceased persons.

2.2 The use of facial recognition and access to data requires a legitimate law enforcement purpose. No member may use or authorize the use of or access to facial recognition for any other reason.

2.3 Probe photos are specifically limited to those obtained lawfully and exposed to public view.

2.4 Any uploaded Probe Image shall be that of an unknown person for the sole purpose of obtaining a possible identification and investigative lead in an official law enforcement investigation. The only exception to this requirement is if the uploading of a known Probe Image may result in additional investigative leads (such as the identification of potential alias', alias social media accounts, etc.)

2.5 The result of a facial recognition search shall only be considered as an investigative lead and **IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT OR PROBABLE CAUSE FOR ARREST**. Any possible connection or involvement of any subject to an investigation and must be determined through further investigation and investigative resources.

2.6 Only authorized facial recognition software users may access or use the facial recognition software/technology in support of investigative efforts.

2.7 A restricted number of Orlando Police Department members will be designated to have the ability to access facial recognition software/technology.

2.8 The Department may share facial recognition data or requests with any government entity that presents an authorized law enforcement or public safety purpose. External data sharing or requests shall be at the approval of the facial recognition administrator or designee documented via the RFI process. Any data sharing or request shall abide by this facial recognition policy. The Department assumes no responsibility or liability for the acts or omissions of other agencies.

3. ACCESS, SECURITY, AUDITING AND RETENTION

3.1 Access to or disclosure of facial recognition search results will be provided only to individuals within the Orlando Police Department who are authorized to have access and have completed applicable training. Authorized access to the Orlando Police Department facial recognition software will be granted only to personnel whose positions and job duties (investigations, intelligence and analysts) require such access. Access shall be granted by the facial recognition software administrator, only with the approval of the Investigative Services Bureau Commander via the requesting user's Chain of Command.

3.2 The facial recognition administrator shall grant and audit all user access, following the required account approval.

3.3 All facial recognition users shall be required to have individual access for use of the facial recognition software/technology.

3.4 Approved facial recognition operators will analyze, review, and evaluate the quality and suitability of probe images, to include factors such as the angle of the face image, level of detail, illumination, size of the face image, and other factors affecting a probe image prior to performing a face recognition search.

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

3.6 Resulting images, if any, shall be manually compared with the probe image by the person conducting the comparison. In accordance with training, any candidate image that is incompatible with a probe shall be removed from the candidate image list.

3.7 All facial recognition investigative queries and requests shall be maintained in accordance with policy. Any upload of a probe image, query or request shall include the name of the agency/requestor, name of the person completing the request, date and time the request was completed, case number and reason for the request. This information will be logged, tracked and available for auditing and review.

3.8 Quarterly, the facial recognition administrator or designee shall conduct an audit of the facial recognition system and the RFI log to assure compliance with this policy. The audit will include a summary of how the audit was completed, findings of the audit to include any identified policy violations, need for revisions, or actions taken to address any violations or revisions.

3.9 The Orlando Police Department complies with the Florida's Public Records Law. All records created or gathered under this policy will be retained for the time period required by the Florida Records Retention Schedules published by the Department of State, Division of Archives and Records Management. In addition to disclosure described in Section 3.1, any records gathered under this policy will also be disclosed, upon request, unless the records qualify as active criminal intelligence or other appropriate exemption(s) allowed by the Public Records Law.

3.10 The Orlando Police Department and all authorized facial recognition users shall comply with all requirements stipulated in any Memorandum of Understanding related to any facial recognition software/technology. Any questions or clarification regarding an MOU should be directed to the Crime Center and Forensics Section Commander, or the Police Legal Advisor's office

4. AUTHORIZED USE OF FACIAL RECOGNITION SYSTEMS

4.1 Any and all use of a facial recognition shall be for official law enforcement use only and considered law enforcement sensitive information. The provisions of this policy are provided to support the following authorized uses of facial recognition information.

a) A reasonable suspicion that an identifiable individual has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal conduct or activity.
b) An active or ongoing criminal or homeland security investigation.
c) To mitigate an imminent threat to health or safety through short-term situational awareness surveillance or other means.
d) To assist in the identification of a person who lacks capacity or is otherwise unable to identify themselves (such as incapacitated, deceased, or otherwise at risk).
e) To investigate and/or corroborate tips and leads.
f) To assist in the identification of potential witnesses and/or victims of violent crime.
g) To support law enforcement in critical incident responses

5. UNAUTHORIZED USE OF FACIAL RECOGNITION SYSTEMS

5.1 The Orlando Police Department strictly prohibits access to and use of any facial recognition system, including dissemination of facial recognition search results, for the following purposes:

a) Non-law enforcement (including but not limited to personal purposes).
b) Any purpose that violates the U.S. Constitution or laws of the United States, including protections of the First, Fourth, and Fourteenth Amendments.
c) Prohibiting or deterring lawful individual exercise of other rights, such as freedom of association, implied by or secured by the U.S. Constitution or any other constitutionally protected right or attribute.
d) Harassing and /or intimidating and individual or group.
e) Any other access, use, disclosure, or retention that would violate applicable law, regulation, or policy.

5.2 Facial recognition software shall not be used to obtain similar images to a subject for the purpose of using them as filler images in a photographic line up.

5.3 The Orlando Police Department **DOES NOT** connect any facial recognition system to any interface that performs live video surveillance, including surveillance cameras, drone footage, and body-worn cameras.

6. TRAINING

6.1 Training will be provided to all authorized users of facial recognition software/technology. This training will be arranged and documented by the facial recognition administrator and account access will not be created or provided until training has been completed.

6.2 Training will cover both the use of facial recognition software/technology and a specific review and acknowledgment of all elements of this policy.

6.3 The use of the facial recognition software/technology includes the following:

a) an authorized user accesses their individual account
b) the authorized user shall enter the required information to support the authorized use of facial recognition satisfying an official law enforcement purpose
c) a lawfully obtained probe image of a subject meeting the required authorized use is uploaded to the system
d) the software automatically compares the probe image to candidate images within the repository
e) results of the comparison are returned and provide a potential investigative lead

6.4 Updated training shall be identified with any policy revisions or updates in facial recognition software.