


|   |   |
|---|---|
| <br><b>City of Dublin</b><br><b>POLICE</b> | <b>Policy and Procedure: 303.24</b>       |
|   | Facial Recognition Technology             |
|   | Last Revision Date: 06/25/2025            |
|   | Last Review Date: 06/25/2025              |
|   | Effective Date: 06/25/2025                |
|   | Standard Reference: None                  |
|   | Approved by: Justin Páez, Chief of Police |

## PURPOSE

The purpose of this policy is to establish clear guidelines for the responsible, ethical, and lawful use of facial recognition technology (FRT) by the Dublin Police Department. This policy is designed to enhance public safety, support criminal investigations, and increase the efficiency of law enforcement operations, while also protecting individual rights, and privacy. The department recognizes the sensitive nature of biometric data and is committed to ensuring that FRT is used in a transparent, accountable, and non-discriminatory manner.

## POLICY

The Dublin Police Department uses facial recognition technology (FRT) for lawful investigations. Authorized personnel may use FRT for identifying suspects, locating missing persons, or verifying identities in criminal cases. FRT is not used for real-time surveillance or predictive policing without reasonable suspicion. All FRT usage will be documented, audited, and reviewed annually to ensure policy compliance and maintain public trust.

## PROCEDURE

### I. PERMISSIBLE USES

- A. FRT shall only be used for official law enforcement purposes, including official investigations and public welfare uses. FRT shall only be utilized to:
  - Identify a person when there is reasonable suspicion that the individual has committed, is committing, or is planning the commission of a crime in any active or ongoing criminal investigation.
  - Identify an individual who is being lawfully detained and officers are unable to identify.
  - Mitigate an imminent threat to public safety or a significant threat to life.
  - Identify a crime victim who is otherwise unknown.
  - Identify a person who is suffering from a mental or physical disability impairing their ability to communicate or be understood, or a person who is incapacitated and unable to identify themselves.
  - Identify a deceased person.
  - Identify a missing person or witness to criminal activity.

- B. Authorized users shall only utilize FRT for any one or multiple of the listed permissible uses in support of their own investigation, an investigation for another Dublin Police Officer, or when officially requested to assist another law enforcement agency for a permissible use.

## **II. RESULT CONFIRMATION**

- A. A result provided by the Facial Recognition Technology (FRT) shall not be used as the sole source for the positive identification of a person. A positive result or facial recognition match cannot be considered probable cause to file a criminal charge or make an arrest without further confirmation of the identification. Any positive FRT identification should be regarded as a lead that must be corroborated by additional means. Investigative tactics, including but not limited to physical evidence confirmation, photo line-ups, data evidence confirmation, suspect and witness interviews, and review of similar incidents/arrests of the subject may be employed to verify the identity indicated by a positive FRT result.

## **III. PROHIBITED ACTIVITIES**

- A. The following uses of the FRT system are strictly prohibited:
  - Identification of a person participating in constitutionally protected activities in public spaces unless there is an articulable investigative purpose.
  - Using the FRT system to conduct a lineup or make an identification without independent and reliable evidence beyond the facial recognition lead.
  - Harassing and/or intimidating any individual or group.
  - Any personal purpose.

## **IV. DATA SECURITY, STORAGE, ACCESS AND RETENTION**

- A. Users shall comply with administrative rules and regulations. FRT data and information shall only be used for criminal justice purposes and administrative review.
- B. Any requests for information gathered using FRT technology will be handled in accordance with Dublin Police Department Policy 501.01, "Agency Records".
- C. Information gathered through FRT will only be shared with other law enforcement agencies for law enforcement purposes.
- D. The Dublin Police Department does not host servers for FRT generated data. Users may download FRT data from FRT software to a locally hosted network.
- E. The retention period of FRT generated data is subject to the FRT software company's data retention policy.
- F. Retention of locally downloaded FRT data is subject to City of Dublin Records Retention Schedule. Facial recognition data needing to be retained as part of an investigation shall be downloaded (PDF) from the FRT database and retained with the case file by Evidence.com.

**V. TRAINING**

- A. Authorized users will receive training on the operation of the FRT before gaining access to the application.

**VI. DOCUMENTED REVIEW**

- A. A Deputy Chief or their designee shall conduct a documented annual review of the search log audit and the outcomes.
- B. The Chief of Police or their designee may periodically inspect the FRT software system to ensure that safeguards and requirements are being met.

**REFERENCE:**

None

**CROSS REFERENCE TO FORMS:**

None

**REPLACES:**

N/A