

*“Keep Orlando a safe city by reducing crime and maintaining livable neighborhoods.”*

**ORLANDO POLICE DEPARTMENT POLICY AND PROCEDURE**

**1151.0, USE OF FINGERPRINT SCANNERS**

EFFECTIVE DATE:	1/24/2024
RESCINDS:	N/A
DISTRIBUTION GROUP:	SWORN EMPLOYEES
REVIEW RESPONSIBILITY:	PROFESSIONAL STANDARDS DIVISION COMMANDER
ACCREDITATION STANDARDS:	N/A
RELATED LAWS:	N/A
RELATED POLICIES:	N/A
CHIEF OF POLICE:	ERIC D. SMITH

CONTENTS:

1. PURPOSE
2. POLICY
3. DEFINITIONS
4. PROCEDURES
  - [4.1 Equipment](#)
  - [4.2 Proper Use](#)
  - [4.3 Improper Use](#)
5. FORMS AND APPENDICES

**1. PURPOSE**

The purpose of this policy is to establish guidelines for the use of the Rapid Identification System to rapidly confirm a positive identification and criminal history if electronic fingerprints of the subject/suspect exist in Florida’s criminal fingerprint identification system.

**2. POLICY**

It is the policy of the agency to provide agency personnel with a specialized tool to assist in the positive identification of individuals under appropriate circumstances, in an effort to prevent crimes, apprehend criminals, and fulfill its mission to provide a safe community for our citizens and enhance officer safety.

**3. DEFINITIONS**

Rapid ID Device (RIDDD): A handheld, Wireless Supported Scanning device that communicates to the Florida Department of Law Enforcement Rapid ID (FALCON) system. The device checks fingerprints obtained from suspects roadside against wants and warrants and can provide positive identification and a Criminal History if electronic prints exist in the Florida Department of Law Enforcement’s Rapid ID (FALCON) system.

Rapid Identification System: A combination of hardware and software that enables an officer to access arrest data, including photos, via fingerprints. The system is sufficient to establish probable identification for arresting someone on a warrant.

Scanning: The procedure of placing a finger on the glass of the fingerprint reader so that the captured image of the print may be compared to the data in the archive.

## 4. PROCEDURES

### 4.1 EQUIPMENT

#### 4.1.1 EQUIPMENT REQUIREMENTS

All RIDD units must be properly maintained in accordance with the manufacturer's recommendations as detailed in the training protocol and in accordance with department policy. Only FDLE-approved and registered devices may be used for the purposes of obtaining a fingerprint roadside.

#### 4.1.2 EQUIPMENT AND TRAINING REQUIREMENTS

The Special Projects/Technology Liaison Officer shall be responsible for overseeing the development, implementation, and maintenance of the RIDD program. **This shall include ensuring training and any RIDD devices are developed based on the manufacturer's recommendations, Florida Department of Law Enforcement guidelines, and appropriate legal mandates.**

The Special Projects/Technology Liaison will issue the RIDD to the end user, appropriately track the issue of the device for required accountability and coordinate repairs/replacement of damaged or non-functional equipment with the vendor. The Special Projects/Technology Liaison will also be responsible for the collection of all statistical reporting as required to ensure adequate program evaluation and documentation of device successes.

RIDD will be issued only to members who have received department training on the operation of the device. The use of a RIDD device by a member who has not received department training is strictly prohibited.

All RIDD training will be documented in accordance with department policy and training protocols and will be reviewed every two years by the CJIS Agency Coordinator for any necessary changes and updates.

RIDD devices in need of repair or replacement shall be brought to the attention, via email, to the Special Projects/Technology Liaison Officer.

### 4.2 PROPER USE

The RIDD may be used in situations where the subject to be printed has given a knowing and intelligent voluntary consent/permission for the use of the device. This may include consent during lawful encounters or consent during various administrative interactions. As with other forms of consent, the consent can be limited, or withdrawn, at any point. If consent is withdrawn, the use of the RIDD is not authorized and cannot be compelled.

The RIDD may be used in situations where reasonable suspicion can be articulated that the subject to be printed:

1. Has committed, is committing, or is about to commit a criminal act, AND
2. When there is a justifiable and reasonable belief that such printing via the RIDD will either establish or negate the subject's connection with that crime, AND
3. The use of the RIDD is carried out **expeditiously**.

**Failure to comply with the request to provide RIDD under these circumstances may constitute a form of obstruction; however, it may be more appropriate to use the failure to comply as further evidence of suspicion for the suspected crime and simply proceed with the investigation toward an appropriate resolution or charge.**

The RIDD may generally be used in situations where the subject to be printed would otherwise be mandated to give traditional fingerprint samples.

Some samples would include:

- a. Probable cause criminal arrest situations.
- b. When a subject is issued a citation (if the citation requires print(s) to be affixed), a RIDD might be used to rapidly ensure the identity given by the subject matched his or her prints, since proof of correct identity is already contemplated by affixing a print(s) to a citation and a requirement to give accurate information.
- c. When, during a lawful *Terry* stop, the subject has provided a false name or refused to provide a name, and the subject's name is needed to complete the purpose of the investigation.
- d. The Rapid ID may be used in situations where the use of the device has been specifically authorized pursuant to a valid subpoena; however, if the subpoena is not for immediate compliance, the subject should be allowed to appear for fingerprinting at the future time indicated on the subpoena.
  1. Failure to honor a subpoena for Rapid ID use should be addressed in court and not be handled by attempting to force compliance via enforcement actions at the time of the refusal to comply.
  2. The Rapid ID may be used in situations where the use of the device has been specifically authorized pursuant to a valid court order. Where a court order requiring the use has been ordained, reasonable and safe efforts to gain compliance may be employed. Failure to comply may constitute contempt of court and may constitute obstruction of justice.

Any specialized non-standard use of the RIDD requires supervisory approval. Examples of non-standard use may include but are not limited to, identifying an unconscious, deceased, or otherwise incapacitated person (amnesia, dementia, Alzheimer's, or other condition affecting memory) who cannot be identified by any other means.

Requests from an outside agency to fingerprint a suspect in custody may be accommodated with supervisory approval. The requesting agency must comply with the procedures and use restrictions set forth in this policy.

In situations where use of the RIDD is authorized, members are required to adhere to vendor and Rapid ID practices when using the device. This includes ensuring the device is properly logged in to, proper Reason Fingerprint Codes are utilized, and the device is properly cleaned and maintained to facilitate an accurate scan.

#### **4.3 IMPROPER USE**

The use of the RIDD device for random or generalized investigative or intelligence gathering, with no focused case is not authorized. Members are expected to be able to justify, based on these guidelines, training, experience and assessment of the circumstances, how they determined that use of the Rapid ID Device was justified under the circumstances.

## **5. FORMS AND APPENDICES**

N/A