


# FLORIDA HIGHWAY PATROL POLICY MANUAL

	<b>SUBJECT</b> IDENTITY VERIFICATION and AUTHENTICATION	<b>POLICY NUMBER</b> 17.24
		<b>ISSUE DATE</b> 01/15/08
		<b>REVISION DATE</b> 02/16/17
		<b>TOTAL PAGES</b> 7

## 17.24.01 PURPOSE

To provide guidelines for the issuance, training and use of the Rapid ID Digital Fingerprint Device and digital camera devices when used for identification purposes.

## 17.24.02 POLICY

It is the policy of the Florida Highway Patrol to provide its members with the most current, cutting edge technology in the effort to apprehend criminals and fulfill its mission to provide the citizens of this state a safer Florida.

- A. The issuance and use of the Rapid ID Device (RIDDD) is intended to provide members with a specialized tool to assist in the positive identification of individuals under appropriate circumstances.
- B. RIDDD may be used in a variety of circumstances; however, members must be aware that there are specific requirements and guidelines for its use.
- C. The issuance and use of digital camera devices by members may facilitate the identification of persons when used with corresponding identification technology; however members must be aware there are specific requirements and guidelines for its use.

## 17.24.03 DEFINITIONS

- A. **DIGITAL CAMERA DEVICE** – For the purpose of this policy, this term means any Division issued device which has the ability to record images in digital format, and which is used for the purpose of identifying individuals. Examples may include stand-alone digital cameras and integrated devices such as mobile communications devices (e.g. tablets and smartphones), mobile data computers (MDC), etc.
- B. **RAPID ID DEVICE** – (RIDDD) A handheld, wireless supported scanning device that communicates via the Mobile Data Computer (MDC) to the Florida Department of Law Enforcement Rapid ID (FALCON) system. The device checks two 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 system.

- C. **REASONABLE SUSPICION** – Articulable facts when considered in the totality of the circumstances which are sufficient for a member, based on their knowledge, training and experience, to believe that a person is committing, has committed or is about to commit a crime.

#### **17.24.04 RESPONSIBILITIES**

- A. Authority to issue or approve RIDD and/or digital camera devices to members when used for identification purposes shall be vested in the Director or designee.
- B. Only devices which conform to the standards as set forth by the Florida Department of Law Enforcement and the Department will be approved.
- C. The Chief Training Officer at the Florida Highway Patrol Training Academy shall be responsible for overseeing the development and administration of the training process for assuring proficiency of instructors and operators with the RIDD. This shall include but not be limited to:
  - 1. Ensuring lesson plans and any necessary forms are developed based on manufacturer's recommendations, Florida Department of Law Enforcement guidelines and appropriate legal mandates.
  - 2. Ensuring that proficiency training is received by each user.
  - 3. Reviewing and revising all applicable training criteria on an as needed basis.
- D. Troop Training Coordinators shall ensure that each member provided a RIDD and/or digital camera device receives required training in the field and that:
  - 1. The original rosters and/or certificates are sent to the Chief Training Officer at the Training Academy
  - 2. A copy of the training rosters and/or certificates is placed in the member's troop personnel file, or the appropriate entry is made in the member's electronic transcript.
- E. Troop Commanders shall ensure that supervisory personnel who manage members equipped with RIDD and/or digital camera devices:
  - 1. Make certain that members follow established guidelines and procedures for the use and maintenance of the RIDD and/or digital camera device.
  - 2. Repairs and replacement of damaged or non-functional RIDD and/or digital camera devices are documented and performed as directed by the Chief Technology Officer.

3. All necessary statistical reporting requirements are being completed as required to ensure adequate program evaluation.
  4. On a monthly basis, reports involving cases in which the RIDD and/or digital camera devices played an integral part in making an arrest shall be forwarded up through the chain of command to the Office of Strategic Services.
- F. The Chief Technology Officer shall be responsible for overseeing the technology portion of the Rapid ID Program.
1. All RIDD units and/or digital camera devices purchased by the Department will be approved, inspected and installed as determined by the Chief Technology Officer.
  2. RIDD and/or digital camera devices in need of repair or replacement shall be brought to the attention, via the chain of command, of the Chief Technology Officer.

#### **17.24.05 PROCEDURES**

- A. Issuance of the RIDD and/or digital camera devices:
1. A RIDD and/or digital camera device will be issued only to members that have had training on their operation. Training shall include considerations and requirements for use of the device under various circumstances.
  2. All RIDD units and/or digital camera devices must be properly maintained in accordance with the manufacturer's recommendations as detailed in the training provided prior to use.
- B. Training
1. Prior to issuance of a RIDD and/or digital camera device for field use, members will complete a Division approved training course.
  2. Training will be based on manufacturer's recommendations and suggestions from the Chief Training Officer.
  3. Training will include at a minimum:
    - a. Setup and maintenance procedures
    - b. Proper use guidelines
    - c. Legal issues
    - d. Reporting requirements
    - e. Other issues as deemed necessary and established by the Chief

## Training Officer, Florida Highway Patrol Academy

### C. Guidelines for Use of the RIDD

1. The RIDD may be used in situations where the subject to be fingerprinted has given a knowing, willing and voluntary consent or permission for the member to use the device. This may include consent given during lawful encounters (e.g., traffic stops).
  - a. As with other forms of consent, the consent can be limited or withdrawn at any point by the subject.
  - b. If consent is withdrawn; use of the RIDD is **not** authorized and its use must stop immediately. Members may not force or coerce anyone to submit to the scan.
2. The RIDD may be used in situations where reasonable suspicion can be articulated that the subject to be printed has committed, or is about to commit a criminal act, when there is a justifiable and reasonable belief that such printing via the RIDD will either establish or nullify the subject's connection with that crime. The key here is that the use of the RIDD is used as quickly as possible after reasonable suspicion is established.
  - a. Failure to comply with the request to provide a RIDD scan 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 suspect crime and simply proceed with the investigation without the scan.
  - b. The RIDD may be used in situations where the subject to be printed would otherwise be required to give traditional fingerprint samples.

Some examples would include:

    - (1) Probable cause criminal arrest situations.
    - (2) Required sentencing fingerprints for court.
    - (3) When a subject is issued a citation (if the citation requires fingerprint(s) to be affixed), a RIDD might be used to rapidly ensure the identity given by the subject matched his/her prints, since proof of his correct identity is already in question and is the cause for placing the print on the citation in the first place.
3. The RIDD 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.

- a. Members should be aware that the subject may be able to move to quash the subpoena.
  - b. Failure to honor a subpoena for RIDD 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.
4. The RIDD may be used in situations where the use of the device has been specifically authorized pursuant to a valid court order or warrant.
    - a. Where a court order or warrant requiring the use of the RIDD has been entered, reasonable and safe efforts to gain compliance may be employed.
    - b. Failure to comply may constitute contempt of court and may constitute obstruction of justice.
  5. Special care should be taken to ensure devices are not used for purposes that may lend themselves to the inference of improper "profiling."
  6. Use of the RIDD for random intelligence gathering or generalized investigation, with no focused purpose or other reason is **not** authorized. The device is not to be used for any unlawful purpose.
  7. Requests from outside agencies to fingerprint a suspect in custody shall be documented on the Field Interview Report or Arrest/Offense Report and forwarded to the member's supervisor. (As long as the requesting agency complies with the procedures set forth in this policy.)
  8. Guidelines cannot be written to encompass every possible application for the use of a RIDD. Members, therefore, should keep in mind the guidelines set forth in this policy to assist them in deciding whether the device may be used or not.
  9. 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 RIDD was justified under the circumstances.
  10. For additional information regarding the use of RIDD see the Florida Highway Patrol Standard Operating Procedures for Users of Rapid ID Device and Communications Personnel.
- D. Guidelines for use of digital camera devices and digital image(s) for identification purposes.
1. In circumstances permitted in this policy, members may use an issued digital camera device to obtain a person's digital image(s), and submit the

image(s) for the purpose of identification for individuals who are otherwise unable to be reasonably identified.

2. Identification of persons using digital image(s) through this technology may only be used for law enforcement purposes.
  - a. When available, a member should attempt to verify a person's identity utilizing law enforcement database record images and RIDD prior to using this technology.
  - b. Generally, all other readily available resources to identify an individual should be exhausted prior to using this technology.
  - c. When an arrested person is at a detention facility and remains unidentified, any readily available detention facility identification resources should be utilized prior to using this technology.
  - d. This technology may be used with persons suspected of identity theft or identification credential related crimes.
  - e. Digital image submissions for the purpose of identification will be directed to the Bureau of Criminal Investigations and Intelligence (BCII).
  - f. Taking photographs of arrestees and any evidence during mass arrests as outlined in the Florida Highway Patrol All Hazards Plan.
3. Requests from outside agencies to identify a suspect in custody shall be documented on the Field Interview Report or Arrest/Offense Report and forwarded to the member's supervisor. (As long as the requesting agency complies with the procedures set forth in this policy.)
4. Use of the digital camera device for random intelligence gathering or generalized investigation, with no focused purpose or other reason is **not** authorized. The device is not to be used for any unlawful purpose.
5. Safety Considerations
  - a. All digital images obtained for identification purposes should be taken at a safe location, giving consideration to the environment, number of subjects and subject factors, cooperation level, number of members, and other safety
  - b. Physical force shall not be used for the purpose of obtaining a digital image.
  - c. Individuals shall not be physically detained for the sole purpose of being photographed for identification purposes.
6. Members shall complete and submit a Field Interview Report for **every** person photographed for identification purposes.

7. Members shall not disseminate any identification image taken pursuant to this policy except to the extent permitted or required by policy and law.
  - a. Images taken as part of a law enforcement investigation may be attached to the appropriate report and/or electronic case file.
  - b. All identification images shall be promptly deleted from the digital camera device and members MDC as soon as feasible, once the image is uploaded successfully to the appropriate report and/or electronic case file.
  
8. Digital camera devices are versatile tools which may be used to document general investigations and/or intelligence in the course of law enforcement duties. The device is not to be used for any unlawful purpose. Some examples of acceptable use include:
  - (1) Documenting physical evidence relevant to and at crash scenes, specifically those involving serious bodily injury or death.
  - (2) Documenting information relevant to the submission of Field Intelligence Reports.
  - (3) When beneficial, documenting evidence and information relevant to other violations of law.
  - (4) Images having evidentiary value must be retained with the related case file and processed pursuant to the guidelines set forth in the FHP Evidence/Property Procedures Manual.