



GENERAL OPERATIONS			1106.00	
<div><div></div><div>DRIVER AND VEHICLE INFORMATION DATABASE (DAVID)</div><div></div></div>				
ISSUED: 03-28-1997	EFFECTIVE: 04-06-1997	REVISED: 07-09-2024	REVIEWED: 10-19-2023	PAGES: 10

## CONTENTS

This procedure consists of the following numbered sections:

- |                                 |  |
|---------------------------------|--|
| I. GENERAL                      | VII. SECURITY OF INFORMATION                                       |
| II. ACCESS TO DAVID             | VIII. SYSTEM ADMINISTRATION  |
| III. TRAINING                   | IX. QUARTERLY QUALITY CONTROL REVIEW                               |
| IV. AUTHORIZED USE OF DAVID     | X. DRIVERS PRIVACY PROTECTION ACT (DPPA) AND PUBLIC RECORDS ACCESS |
| V. UNAUTHORIZED USE OF DAVID    |  |
| VI. MISUSE OF DAVID INFORMATION |  |

## SCOPE

This procedure shall apply to all agency personnel accessing or using information obtained from the state Driver and Vehicle Information Database (DAVID).

## DISCUSSION

The DAVID system provides important personal information, vehicle information, and photographs useful for criminal investigations and for other law enforcement-related purposes. The database may be accessed through the Internet. The system requires an assigned login and password. As a result, the physical security of the computer must be maintained and the Windows-based computer password must be relied upon to prevent unauthorized access to DAVID. Driver's license and vehicle records privacy laws form the basis for this policy. This policy is based on the provisions of the Memorandum of Understanding (MOU) form issued by the Florida Department of Highway Safety and Motor Vehicles (DHSMV), dated 12/18.

## DEFINITIONS

1. **Driver and Vehicle Information Database (DAVID):** A driver's license and vehicle registration database maintained by the Florida Department of Transportation, Division of Highway Safety and Motor Vehicles.
2. **Driver's Privacy Protection Act (DPPA):** United States Code regulating the use of driver's license information (18 United States Code § 2721 et seq.).
3. **Florida Criminal Justice Network:** A limited-access website operated by the Florida Department of Law Enforcement that provides various resources and database access to criminal justice agencies (<http://www.flcjin.net>).
4. **Florida Department of Highway Safety And Motor Vehicles (DHSMV):** The Florida state agency responsible for computerized driver's license, vehicle, and traffic crash records. For purposes of this standard operating procedure, the Florida DHSMV is the "provider agency" for DAVID information.
5. **Highly Restricted Personal Information:** As defined in the DAVID memorandum of understanding, an individual's photograph or image, Social Security number, and medical or disability information.
6. **Primary Point of Contact (POC):** Agency member or employee designated by the Chief of Police to manage and supervise the DAVID system at the agency level.
7. **Personal Information:** Information found in the motor vehicle or driver record which includes, but is not limited to, the subject's driver identification number, name, address, telephone number, and medical or disability information. Personal information does not include information related to vehicular crashes, driving violations, and driver's status (18 USC § 2721 definition).

## PROCEDURE

- I. **GENERAL:** Agency personnel accessing and using information obtained from the state Driver And Vehicle Information Database (DAVID) will comply with the Driver's Privacy Protection Act (18 United States Code, Title 1, Chapter 123, Section 2721 et seq.) and [F.S. 119.0712](#) and the information safeguards stated in the Memorandum of Understanding (MOU) executed with the Florida Department of Transportation, Division of Highway Safety and Motor Vehicles (DHSMV) as outlined in this procedure. Information obtained under the provisions of the MOU will only be disclosed to persons to whom disclosure is authorized under Florida law and federal law.

## II. ACCESS TO DAVID

- A. Access to the DAVID system will be provided to all sworn and civilian employees within the department with the exception of the Executive Assistant to the Chief of Police, the Property and Evidence Technician, and the Accreditation and Administrative Services Specialist. Other personnel may be granted access with approval from the Chief of Police.
- B. Access will be provided via Internet connection to specific computers with appropriate software.
- C. Access to the Florida Criminal Justice Network will be required to access the website for the DAVID system with an agency issued user name and password.
- D. Users are not authorized to access another user's account.
- E. Access and Use Procedures
  - 1. Department members needing access to DAVID for official use will meet with the Primary Point of Contact for a review of the DAVID system.
  - 2. The member will sign the user confidential acknowledgement and criminal sanctions acknowledgement. The forms will then be forwarded to the Employee Development Coordinator for inclusion in the agency training files.
  - 3. The agency Primary Point of Contact will add the member, assign the roles, enter the status of the member and create a temporary password for the member.
  - 4. Once the member signs onto the website at <https://david.flhsmv.gov/> the member shall be required to change the temporary password, take the DAVID training and complete the test questions.
  - 5. When assistance is required, the member shall contact the agency Primary Point of Contact.
  - 6. All members who are eligible to access DAVID shall log into the DAVID system a minimum of once every 90 days to ensure that the account stays active. The member shall complete all reoccurring training required by the DAVID system within the required time frame.
  - 7. Documentation generated from the DAVID system will be shredded when no longer useful, if not placed in official files.
  - 8. When using computers with DAVID access, particularly laptop computers, members will ensure that non-releasable highly sensitive personal information is not visible to the public, or to prisoners/passengers during transport.

9. Members will report misuse of personal information to a Command Staff Officer immediately through the chain of command.

### III. TRAINING

- A. New users will receive training prior to accessing DAVID records. Training may be conducted individually using a field training method or on-line. The training will be designed to ensure the user operates the system properly and understands the privacy safeguards. A review of this standard operating procedure will be included in the training.
- B. If the terms of the MOU or user guidelines in this procedure are changed, a new signed annual acknowledgment will be completed by each user. Notification and training, if necessary, will precede the acknowledgment.

### IV. AUTHORIZED USE OF DAVID INFORMATION: Consistent with 18 United States Code, Title 1, Chapter 123, Section 2721 et seq and [Florida Statute 119.0712](#), DAVID information may be used for:

- A. Criminal and traffic investigations;
- B. Distribution of photographs of missing persons (adults or children) to the public to aid in their recovery;
- C. Investigation of child neglect, not necessarily criminal;
- D. Child placement background investigations;
- E. Agency employment driver's license background checks or status checks;
- F. Agency internal investigations into DAVID misuse or to otherwise aid in internal investigations;
- G. An aid in locating persons to be served legal (civil and criminal) process;
- H. Identification for prisoner transfers;
- I. Driver and motor vehicle history;
- J. Citizen Status or residency verification;
- K. Verification of identity or background checks for agency volunteers or contractors; and
- L. Providing notice to the owners of towed or impounded vehicles.

M. Proper reason codes shall be used when running queries in DAVID.

**V. UNAUTHORIZED USE OF DAVID:** Per Florida Statutes DAVID information can only be used for legitimate business purposes only. Unauthorized use of DAVID includes:

- A. Queries not related to official law enforcement or judicial purpose;
- B. Queries not related to official business purpose;
- C. Improper dissemination (sharing, copying, distributing) of information to unauthorized persons; and
- D. Personal Use.

## **VI. MISUSE OF DAVID INFORMATION**

- A. Misuse of DAVID resources is a violation of department policy and is covered in Standard Operating Procedure [304.00 – Standards of Conduct](#).
- B. Misuse of personal information from DAVID will be reported to a Command Staff Officer who shall immediately notify the Chief of Police. The Chief of Police or their designee will immediately notify DHSMV, and the individual whose personal information was compromised, of any unauthorized access, distribution, use, modification, or disclosure. The statement to DHSMV must provide the date and the number of records affected by any unauthorized access, distribution, use, modification, or disclosure of personal information. Further, the requesting party agrees to comply with the provisions of section [501.171, Florida Statutes](#). The Parties agree that any subsequent changes to this law will be binding upon both parties.
- C. Misuse of DAVID includes but is not limited to:
  - 1. Looking up addresses for personal use;
  - 2. Release of deceased date of individuals when information is obtained via DAVID;
  - 3. Checking your own or family member's driving record;
  - 4. Looking at photos of friends, relatives, or self;
  - 5. Looking up celebrities or politicians;
  - 6. Copying information to supply to the public; and
  - 7. Posting information where is it exposed to the public.

8. DAVID users shall not run their own information for any reason.

**VII. SECURITY OF INFORMATION:** Agency personnel and authorized users will:

- A. Not retain DAVID records, except as required as part of an official report, nor provide them to any third party. DHSMV does not consider the courts and State Attorney's Office as third parties;
- B. Protect access or destroy the information obtained in such a way that unauthorized persons cannot review or retrieve the information; and
- C. The police department will not interface DAVID to a third party.

**VIII. SYSTEM ADMINISTRATION**

- A. The Administrative Services Supervisor shall:
  1. Ensure the implementation and maintenance of appropriate internal controls of personal data obtained through DAVID to protect the data from unauthorized access, distribution, use, modification, or disclosure.
  2. Serve as the Point of Contact to perform the related duties as it pertains to DAVID.
  3. Prepare and send the annual affirmation statement to the Chief of Police for approval.
  4. Send the approved annual affirmation statement to DHSMV via United States Mail, to comply with annual reporting requirements no later than 30 days after the anniversary date of the MOU. The form or format as provided by DHSMV will be used, if provided. This should be included with the annual attestation.
- B. The Primary Point of Contact will:
  1. Approve and assist personnel in obtaining access to the system at the agency level;
  2. Update user access permissions upon termination or reassignment of users within one (1) working day and immediately update user access permissions upon discovery of negligent, improper, or unauthorized use or dissemination of information;
  3. Ensure compliance with the terms of the MOU and applicable laws by ensuring compliance with this standard operating procedure;
  4. Ensure new users are properly trained and the required forms are completed and submitted;

5. Monitor access to the information and conduct documented quarterly quality control reviews (see paragraph VIII of this procedure);
6. Cooperate with any external audits ordered by the agency or DHSMV;
7. Report misuse to the Chief of Police, who will be responsible for ensuring DHSMV is notified; and
8. Scan all original documentation except as otherwise specified.

## IX. QUARTERLY QUALITY CONTROL REVIEW

A. The Primary Point of Contact will perform the quarterly quality control review.

1. The POC shall do the following to satisfy the MOU Quarterly Quality Control Review:
  - a. Compare the DAVID Users by Agency report with the agency user list.
    - 1) Reconcile any differences to ensure state and agency records are consistent.
  - b. Keep a record of any new user or inactivated users since the last Quarterly Quality Control Review.
    - 1) Update any users/user information as needed, document the reason for the change in access, and the date the change is made.
  - c. Monitor usage to ensure proper, authorized use and dissemination.
    - 1) Randomly select a sample of users and run an audit report for a period during the quarter.
    - 2) Look for any misuse, including but not limited to reason codes, running siblings, spouses, ex-spouses, celebrities and political figures.
    - 3) Look at the times of day the data was accessed, repeated runs of same record and unexplained access to the Emergency Contact Information (ECI).
  - d. Ensure that all current users are appropriately trained, authorized, and have current acknowledgment forms on file. This may be accomplished by comparing the list of authorized users with a current employee roster.
  - e. Complete and retain the DAVID audit form, and the quarterly quality control review report.

- f. Forward the complete audit report detailing the above requirements to the Chief of Police for review and approval.
- B. The POC shall ensure that personnel have been deactivated within one (1) day of termination or reassignment.
- C. The POC shall provide a summary of any incident reports, memorandums, or other documentation related to system misuse or improper disclosure of information;

#### **X. DRIVER'S PRIVACY PROTECTION ACT (DPPA) AND PUBLIC RECORDS ACCESS**

- A. Unauthorized Use and Release: Information obtained from the DAVID system will not be used for any purposes not specifically authorized by this procedure (consistent with the MOU). Unauthorized use includes, but is not limited to, queries not related to a legitimate business purpose; personal use; and the dissemination, sharing, and providing this information to unauthorized persons.
- B. Release of Information: Agency personnel and authorized users will protect and maintain the confidentiality and security of personal information from driver license, motor vehicle, and traffic crash records received from DAVID in accordance with the MOU and applicable state and federal law. Information obtained from the DAVID for criminal investigative purposes and criminal intelligence (normally exempt and confidential under [F.S. 119.071](#)) may only be released:
  - 1. In the furtherance of official duties and responsibilities, including apprehension of suspects;
  - 2. For print, publication, or broadcast if the agency determines that such release would assist in locating or identifying a missing or endangered person; or
  - 3. To another governmental agency in the furtherance of its official duties and responsibilities.
- C. All other public records requests for DAVID information will be referred to the originator of the records, the DHSMV.
- D. User Acknowledgements: All DAVID users will be instructed of, and acknowledge in writing:
  - 1. The confidential nature of the information; and
  - 2. The criminal sanctions specified in state law for unauthorized use of the data.

E. Emergency Contact Information (ECI): All DAVID users will be instructed as part of their field training and evaluation program of the sensitive nature of the release of Emergency Contact Information.

1. ECI contained in a motor vehicle record is confidential and exempt from [s. 119.07\(1\)](#) and s. 24(a), Art. I of the State Constitution; and
2. Without the express consent of the person to whom such emergency contact information applies, the emergency contact information contained in a motor vehicle record may be released to law enforcement agencies for purposes of contacting those listed in the event of an emergency.
  - a. ECI may be released to a receiving facility, hospital, or licensed detoxification or addictions receiving facility pursuant to s. 394.463(2)(a) or s. 397.6772(1)(a) for the sole purpose of informing a patient's emergency contacts of the patient's whereabouts.
3. In accordance with the Memorandum of Understanding with the State of Florida (DHSMV) an emergency only includes serious injury, death, or other incapacitation. ECI information shall not be released or utilized for any purpose, other than those listed above, including developing leads or for criminal investigations.

**APPROVED**



**PAMELA R. SMITH, CHIEF OF POLICE**

**STAFF REVIEW DATES:** 06-12-2009, 07-21-2011, 07-03-2013, 10-28-2014, 10-03-2016, 05-28-2019, 10-19-2023

**REVISION DATES:** 06-12-2009, 07-21-2011, 07-03-2013, 10-08-2013, 10-28-2014, 10-03-2016, 05-28-2019, 07-10-2019, 07-25-2019, 08-03-2022, 10-19-2023, 07-09-2024