NEW SMYRNA BEACH POLICE DEPARTMENT
NEW SMYRNA BEACH, FLORIDA

POLICY AND PROCEDURE DIRECTIVE

TITLE:	**RECORDS**
NUMBER:	**26-1**
EFFECTIVE:	**8/14**
REFERENCE:	
RESCINDS/ AMENDS:	**34-1**
REVISED:	**8/22**
ATTACHMENTS:	**GENERAL-RECORDS-SCHEDULEGS01-SL GS2-2017** **SOP\CJIS SECURITY 26-2-2.DOC** **IT NETWORK POLICY.PDF** **FSS 119; FSS 119.07; FSS 316.066; FSS 985.11; FSS 943.059**

A. PURPOSE

The purpose of this directive is to establish guidelines and procedures for police records maintenance.

B. POLICY

It shall be Department policy to create and maintain records, through reports of criminal activity, investigations, stolen, found, recovered, and evidentiary property along with any other actions performed by Department personnel. Events may be electronically inputted directly into the records management system or on a paper report format for input into the RMS. Primary reports used by the New Smyrna Beach Police Department, regardless of the format, to document public safety events are:

1. Offense/ Incident Report
2. Supplemental Report
3. SA-707 Charging Affidavit
4. State Crash Report
5. Notices to Appear (NTAs)

The Records Section is responsible for record's maintenance, data processing, report disposal, control and retrieval of all department records.

The Records Section Supervisor shall be the custodian of all records. Records shall be maintained in accordance with Public Records and Federal Guidelines relating to Uniform Crime Reporting and the policies and procedures of the Department.

Regardless of format (electronic or paper), records are always accessible to members with appropriate access privileges.

All documents stored within the Department's Records Section that are public record and otherwise not excluded by State law, are available to citizens for inspection during the normal operating hours of the Records Section. Copies

of documents shall be furnished to citizens upon request. Charges for copies shall be made in accordance with the Records Section Standard Operating Procedure Fee Schedule.

It shall be the policy of the New Smyrna Beach Police Department that all personnel will abide by the **Florida Records Retention schedules** regardless of format (paper, electronic, digital).

C. PROCEDURES

26.1.1 Report Accountability

1. Generate an Offense/Incident Report for any call for service at the officer's discretion.
2. Document all verified criminal acts reported, to include traffic accidents.
3. Request a case number from the Communications Section.

    - The Volusia Sheriff's Office (VSO) Communications Section assigns a separate computer generated number, also referred to as a "P" number to every call for service received. All reports will be filed numerically according to "P" numbers and case numbers when generated by the CAD system.

4. When a complete report is required, a case number is requested and generated by CAD. The reporting officer will enter the case number on each page of the report or accompanying document(s).
5. Reports will be reviewed and compared against the CAD calls for service transmittal by the shift supervisor and by the Records Section to ensure that a record has been made for each call for service requiring a report and that it contains information required for UCR reporting.
6. A supervisor, prior to submitting reports to Records, will review all incident, crash, arrest, other miscellaneous reports and property receipts. Said review is indicated by initial, signature, or electronic approval.
7. As appropriate to the format, Supervisors will check reports for neatness, spelling, grammar, completeness, and accuracy. Any report that is not approved will be returned for correction.
8. Generally, reports will be completed prior to the end of the shift. When this is not possible, a summary report will be provided of the incident and the report will be completed as outlined in this directive under the heading 'Incomplete Reports.'

26.1.2 All records itemized above are stored in the Record Management Database and/or hard copy filed by case number. All records will be maintained in an orderly and accurate manner by assigned section personnel.

1. The Records Section will maintain report attachment submissions. All such documents shall bear the case number and will be filed sequentially by case number.
2. Original documents are maintained within the Records Section and shall be removed from the area only by subpoena or authorization of the Records Supervisor.

26.1.3 Authorized agency members may access computerized records information via work stations and/or laptop units at any time. The Records Supervisor, Records personnel, Command Staff, Accreditation Manager, Administrative Services Manager and those authorized by Command Staff are the only individuals authorized to access the Records Department.

1. The Records Section is accessible to the public Monday through Friday from 8:00 a.m. to 5:30 p.m. Records is closed on weekends and holidays.

    - Employees will utilize the window located in the hallway to request information or copies of documents from the Records staff during business hours.

2. Supervisors have access to Records when records personnel are not present.
3. Access to the records section is controlled by proximity cards. Access doors are locked at all times. Citation books and sensitive files are maintained in locked file cabinets. Files and computer screens are not viewable from areas outside of the records section.

D. REPORT DISTRIBUTION

26.1.4 Public records request shall be forwarded to the Custodian of Records who shall release, or authorize the release of information requested in accordance with the **FSS Chapter 119**.

1. Records released to the public shall be redacted in accordance with the appropriate Florida Statute. *(Example, victims of sex crimes, certain juvenile records, etc.)*
2. Crash records shall be released in accordance with **FSS 316.066**

26.1.5 Reports, other than active confidential reports, may be distributed to agency components as needed or requested.

1. Active confidential reports are distributed on a need to know basis with the approval of the appropriate Division Commanding Officer, Deputy Chief or Chief of Police.
2. Reports are routed directly to Records via RMS once reviewed and approved by the Patrol Sergeant. Patrol Sergeants will inform Command staff of cases involving Use of Force via BlueTeam.
3. All reports will be reviewed by the CID Sergeant for investigative assignment and follow-up.

26.1.6 Distribution of reports to organizations outside of the agency:

No member shall distribute any record or type of record to any person, agency or business outside the NSBPD without authorization through the Records Supervisor, Support Services Division Commanding Officer or the Chief of Police. A request of any type of record shall be approved prior to distribution. Records personnel shall facilitate the distribution of records within the department and to organizations outside the agency as follows:

1. Charging documents and related records are forwarded to the State Attorney's Office.
2. Juvenile arrests will be forwarded to the State Attorney's Office Juvenile Division pursuant to the State Attorney's Office.
3. Notices to Appear are forwarded to the Clerk of Court.
4. Complaint affidavits for traffic charges will be sent to the State Attorney.
5. Arrest data will be entered into the computer and forwarded to FDLE, utilizing the FBI UCR format.
6. Crash reports (paper) are forwarded to the County Engineer and the State.
7. Driver Improvement, Florida Department of Highway Safety – Tallahassee.
8. Domestic Violence Reports to the Domestic Abuse Council in accordance with FS.

E. JUVENILE FINGERPRINTS & PHOTOGRAPHS

26.1.7 Juvenile criminal records shall be collected, disseminated and retained in compliance with **FSS 119.07** and **FSS 985.11**.

1. If a juvenile commits a crime that is not a felony or a misdemeanor listed by **FSS 985.11** and photographs or fingerprints are taken, the photographs and fingerprints must be marked "Juvenile Confidential" and, if retained by the agency, placed in a separate file so they are not accidently disclosed to the public. A juvenile who has committed multiple crimes may require multiple files.
2. Access to, dissemination of, and retention of juvenile fingerprints and/or photographs shall be in accordance with **FSS 985.11** or upon an order of the court.
3. Nothing shall prohibit the storage of juvenile traffic offenses, non-arrest field interview cards or other non-criminal reports that may be open to inspection in the same manner as similar adult records.
4. Juvenile criminal records may be purged in accordance with Schedule GS2. The Records supervisor shall make the determination as to which records are to be purged and the method of disposition, in compliance with applicable law.
5. The Records supervisor shall authorize access to any sealed juvenile records in accordance with **FSS**

943.059(4). If the record has been expunged, the requestor will be advised there is no record.

6. Records Section Responsibilities:

- The collection, dissemination and retention of reports concerning juveniles, excluding juvenile referrals. Dissemination shall be in accordance with Florida Statutes.
- Expungements.
- Disposition of records when juveniles reach adult age.
- Provisions for access to records when appropriate.
- Forward felony arrest and enumerated misdemeanor fingerprint cards to the State.

F. RMS & COMPUTER SECURITY

26.1.8 The following apply to Desk Top and Mobile Computers. Additional CJIS security requirements are delineated in the Department's CJIS Compliance Policy, **Standard Operating Procedure 26-2(2)**. Email, internet access and use shall be accordance with the **City's Internet Access & E-mail Policy & Procedures** and **Information Technology Security Policy.**

1. Use of Email

- Access codes and user passwords are assigned to employees after they have completed computer training or have been certified for NCIC/FCIC computer access.
- Passwords must be a minimum of six (6) characters in length. These passwords must use a least two (2) of the four (4) character types, those being lower case letters, upper case letters, numbers and special characters (special characters are: Shifted number keys, colon, quote marks, question mark, etc.).
- Access to add, modify, or delete records is given, taken away or modified based upon a user's assignment, transfer, promotion, demotion or termination. The System Administrator disables access codes and user passwords of separated employees from the system.
- Users are prompted every ninety days to change their passwords and cannot gain access to the system until the change is made. The System Administrator in response to a known or suspected security breach may change access codes and user passwords at any time.
- User name and password integrity is an automated system. Access is tiered requiring multiple sign in. Users are allowed three attempts to correctly enter their user name and password. After the third attempt the system automatically disables the account and requires a system administrator to re-enable the account.
- The System Administrator/IT will investigate all access violations as they occur or are identified.
- The System Administrator/IT (city and county) is responsible for server maintenance, data back-up and secure storage of data.

2. Internet Access

- Internet access is controlled through individual user accounts and computer system passwords. It is the responsibility of the employee to protect the confidentiality of their account. The protection of password information is detailed in the "Computer system and network access passwords," section of this document.

3. Installation of Software

- Employees shall not install, modify, remove or use any software, to include altering internal settings on a City owned or operated computer system unless Information Systems or the System Administrator authorizes it.
- The Network is protected with installed anti-virus software and firewall protection.

4. Access Restriction

- Access to IT resources is restricted to authorized employees and shall be used exclusively for official Department business only. To ensure compliance with FBI CJIS Security Policy and all rules, regulations, policies, and procedures established for CJNET, FCIC/NCIC, III and NLETS, only documented, authorized personnel will be granted access to the various CJI resources. All authorized users will be bound by the security requirements as set forth in Section III of the User Agreement with FDLE. Unauthorized use of IT resources shall be grounds for discipline or revocation of privileges and may be grounds for termination.
- Computer access shall be disabled by system administrators no later than seven (7) calendar days from the day that a NSBPD member ends their employment.

5. Authorize Use

- Authorized users of IT resources shall ensure CJI is physically protected through access control measures in accordance with applicable policies. All employees, vendors, and service providers are required to sign a confidentiality form stating they will not discuss CJI
- Any breaches of this directive, any computer security or access and use violations will subject the user to disciplinary action, up to and including termination, and/or revocation of computer privileges.

6. Personally Identifiable Information (PII)-Any information pertaining to an individual that can be used to distinguish or trace a person's identity.

- New Smyrna Beach Police Department will ensure the appropriate access, use, handling, storage and dissemination of Personally Identifiable Information in accordance with **FSS 817.568** and **FSS 943.125**.

G. FIELD REPORTING

26.1.9 Every incident in one or more of the following categories will be reported. An individual event number, also known as a "P" number shall be assigned to each incident:

1. Citizen reports of crimes;
2. Citizen complaints;
3. Incidents resulting in an employee being dispatched or assigned;
4. Criminal and noncriminal cases initiated by officers;
5. Incidents involving arrest, citations, or summonses.

26.1.10 The computerized Records Management System has a provision for populating the basic incident report, as well as, specialized reports or supplements (e.g. vehicle report, property report, supplemental report, etc.).

26.1.11 Members who initiate cases or complaints that are received extrinsic to the Dispatch Center are responsible for contacting dispatch and requesting a case number.

26.1.12 Dispositions for all calls for service, whether received or self-initiated, shall be recorded either by CAD/RMS or written reports and filed with Records.

26.1.13 Completed reports shall conform to current reporting forms and format, whether electronically or paper completed. Electronic reports are menu driven and to include mandatory fields that must be completed by the reporting officer. Paper forms will be completed by recording the required information in the corresponding blocks.

1. Incident reports: procedure to complete and required information are delineated in **Copperfire's Report Module**;

2. SA707 Complaint Forms are completed in accordance with State Attorney and VSO policy;
3. Traffic Crash reports: procedure to complete and information requirements are delineated in the **DHSMV Traffic Crash Manual**. Electronic crash reports are completed in accordance with **TraCS Florida Crash Report User Guide**;
4. Traffic Citations: procedure to complete and information required is delineated in the DHSMV's **Citation Completion Guide.**

26.1.14 Completed reports are submitted (electronic or paper) to the appropriate supervisor for review and approval before submission to records.

1. Supervisors will review all reports. Initials, signature or electronic approval indicates review and approval. Rejected reports are returned to the submitting member for correction.

Revised: BSS 8/22

Approved: **Signature of File**
Chief Mike Coffin