GREENVILLE POLICE DEPARTMENT POLICY AND PROCEDURES MANUAL		
Chapter 82	**Records**	
Date Initially Effective: 11/30/94	**By the Order Of: Mark Holtzman, Chief of Police**	
Date Revised: 04/17/17	**Date Reissued: 06/30/17**	**Page 1 of 10**

82.1.1 RECORDS COMPONENT

CALEA Standard: 42.1.3 82.1.1, 82.1.2, 82.1.3, 82.1.4, 82.1.5

Privacy and Security

It is the policy of the Greenville Police Department to have a Records Unit to meet the management, operational, and informational needs of the Department and to place accountability for the records function in a specific specialized component. The Records Unit is a component of the Logistics Division and is responsible for the records function of the Greenville Police Department. The Records Unit is in a secure area of the Police Department and is under the supervision of the Information Services Administrator.

The purpose of this directive is to establish guidelines for the security of Greenville Police Department records and files consistent with public record laws and for the overall operation of the Records Unit. Although most records are submitted electronically, the Records Unit still maintains the capability of scanning original records of documents into the Law Enforcement Records Management System (LERMS). Access to records shall be limited to authorized personnel in order to maintain security and to comply with North Carolina law. This procedure shall ensure the confidentiality, availability, access, and security of records maintained by the Greenville Police Department. The privacy and security of criminal history records shall be in accordance with the criteria set forth in FBI Criminal Justice Information Services (CJIS) Security Policy and North Carolina law regarding access and review.

Records Accessibility

Records information is accessible to all authorized personnel on a twenty-four (24) hour basis through LERMS. Access to all CJIS records in LERMS are governed by individual passwords that are changed every ninety (90) days as part of the overall network security policy maintained by the City of Greenville IT Department. In compliance with CJIS and City policy, passwords, at a minimum, must be six (6) characters in length, must contain at least three (3) of the following: one (1) uppercase character, one (1) lowercase character, one (1) special character or one (1) numerical value. Once records have been located by querying the computer system, authorized users have the option to print the selected report(s) at any police department printer/copier. All mobile computers using the LERMS or the corresponding mobile software are required to use two-level authentication in order to access CJIS records in compliance with the latest CJIS rules that can be found on the FBI's website. All CJIS related documents in LERMS are subject to Field Level Auditing. Access to the audit log is available to the Information Services Administrator and when requested to the Command Staff and Internal Affairs.

Records Function

Under the supervision of the Information Services Administrator, the functions of the Records Unit include, but are not limited to:

- *Report entry performed daily*:
  - Using the CAD/LERMS Merge Client: Merge all approved (accepted) cases, arrests, juvenile contacts, case supplements and field contact reports daily.
  - Using Interplat's eCrash Web Client: Approve all "supervisor approved" crash reports daily.

  - Using AOC's eCitation RMS module: Import all eCitations transmitted to AOC. This process writes the citations to a location on the corresponding server where they are imported automatically into the tickets module of LERMS.
- *Report Review:* The report review process will begin with shift supervisors who will review and approve all field case reports after they have been electronically submitted. The Records Unit will conduct another review of the electronically submitted reports. This final review will be for purposes of verifying that all documents submitted are accounted for and contain proper classification, disposition codes, and case numbers.
- *Report Access and Release:* The Records Unit will control the availability and confidentiality of all reports and records to the public. Records access shall be limited to authorized personnel. Information released to the public shall be in accordance with North Carolina General Statutes regarding public information. A process created by IT runs daily that publishes reports online in a redacted format approved by the GPD and CAO.
- *Records Maintenance:* The Greenville Police Department's LERMS maintains electronically all police reports and records identified in this directive.
- *Records Retrieval:* The Records Unit will use the case number reporting system for all filing and retrieval purposes. Information from state uniform citations is data entered and indexed by the defendant's name and citation number.
- *Records Expungement:* Process expungements as soon as possible in accordance with court orders.
- *Process Subpoenas for Records:* In accordance with NC State law, and in coordination with the City Attorney's Office, process subpoenas for records to ensure that the correct records are released.
- *Permits and applications;* Processing of various permits and taxi applications and renewals.
- *Collection of payments:* For fingerprints, permits, alarms, taxi license application, renewal fees and other items as needed for the department. Maintain cash and credit card receipts in accordance with accreditation standards and city finance regulations.
- *Enter Trespass/Consent agreements:* Once turned into records, these agreements are entered into the Alerts module of CAD and a copy forwarded to the appropriate Zone Commander.
- *Notary services:* Available to the department or citizens, as needed.

Juvenile Records

North Carolina law requires that all law enforcement agencies take special precautions to ensure those law enforcement records concerning a juvenile are protected against disclosure to any unauthorized person.

The Greenville Police Department's juvenile arrest and criminal history records shall be maintained in the agency's LERMS. These records are distinctly flagged in the 'juvenile' jackets and are separated from adult records. Juvenile arrest reports are completed electronically in the mobile version of the records management system (RMS) by officers in the field on the Juvenile Contact Form. In the unusual event a juvenile arrest report cannot be completed electronically it shall be recorded on the pink "Juvenile Contact Form" which is easily distinguished from other types of paperwork. Case investigations involving juveniles that are not completed electronically must contain the phrase "See Narrative" in the victim or suspect fields. Those not completed electronically, or any other physical documents that are included in a juvenile case file must be stored in a secure location within the records unit.

Juvenile photographs may be taken in certain circumstances with the appropriate Court Order using any digital imaging other than the mug imaging system. Photographs should be delivered to the Forensic Services Unit for storage in a separate folder in the Forensic Services Unit. Juvenile fingerprints may be obtained in certain circumstances with the appropriate Court Order. Juvenile fingerprint cards will be delivered to the Forensic Services Unit and notification made that they are associated with a juvenile case. Juvenile fingerprint cards will be stored in the Forensic Services Supervisor's office in a separate and secured filing cabinet.

Additional procedures relative to the collection, dissemination, retention, disposition and expungement of records, and identification pertaining to juveniles are contained in Chapter 44 of departmental policy and procedures.

Records Retention
The Greenville Police Department follows the guidelines set forth in the *North Carolina Municipal Records Retention and Disposition Schedule* for all records. Additionally, for rules that are the discretion of the municipality there is an endorsed copy of the City's Retention and Disposition Schedule maintained by the City Attorney's Office available on request.

Incident Based Reporting (IBR)
The Greenville Police Department participates in the North Carolina Uniform Crime Reporting System through the FBI Incident Based Reporting system (IBR). Statistical data is routinely uploaded monthly by Records Unit personnel. Using LERMS the Records Unit checks for and corrects any errors, prepares a submission file and uploads the information to the North Carolina State Bureau of Investigation (SBI). Submission of the IBR files shall be the responsibility of the Information Services Administrator or designee.

82.1.2 PROTECTING THE INTEGRITY OF COMPUTERIZED RECORDS

CALEA Standard: 82.1.6, 11.4.4

Audit of Central Records Access
The integrity and security of the central records files is dependent upon the access systems that provide control through a series of passwords and access codes. Employees are not permitted to use passwords, access a file, or retrieve any stored communication unless authorized to do so. The Information Technology Department of the City of Greenville maintains a current "Computer Security and Use Procedure". All employees of the Greenville Police Department are required to sign, acknowledge and comply with these procedures.

Specific requirements regarding computer access and passwords can be found in the Information Technology "Computer Security and Use Procedure".

Computer System Access
Computing resources, data, and information must be protected from unauthorized use, external intrusion, theft and accidental or malicious damage. To protect active sessions:

1. Close down active sessions and use a password protected screensaver to secure your terminal or workstation if you intend to leave it unattended or inactive. The example below is the correct way to immediately lock and unlock your workstation. (e.g., press Ctrl-Alt-Del keys, and then press Enter to lock the workstation. To unlock your workstation, move your mouse or press a key on the keyboard, press Ctrl-Alt-Del keys, then enter your password in the password field of the dialog box).
2. Logoff the network and shut down or lock your computer at the end of the working day and on weekends unless otherwise instructed.
3. Use secure network file locations to store all City data, unless there is a specific need or limitation requiring data to be stored on your computer's local hard drive (local drives are not backed up). Do not store sensitive information on your local hard drive unless it is protected by access controls. Contact the IT Department to discuss data encryption software options. Health information must be stored and protected on secure drives where backup, recovery, and retention are available and to meet HIPAA rules and regulations governing these electronic records.

Passwords
Guard your password carefully. Adhere to the following guidelines:

- Do not reveal passwords to anyone. If required to disclose current password to an authorized computer technician for system maintenance or troubleshooting, change your password immediately after maintenance is complete.
- Do not write down and post or store passwords near a workstation, under the keyboard or mouse pad, or other areas where they could be found and used.
- For new accounts, change passwords upon first login or upon password reset for the account.
- Change passwords immediately if it is suspected that they have been compromised.

- Change passwords every ninety (90) days. If greater security is required, change passwords more frequently. (Network passwords will expire automatically after ninety (90) days.)
- Change default passwords supplied with new software packages immediately after the software installation.
- After five unsuccessful network login attempts (invalid user ID and/or password), the system will lock the user ID account. Contact the help desk if this occurs.

The following guidelines for choosing passwords should be used:

- Passwords must be composed of at least six (6) characters. If the computer software in use does not support six (6) character passwords, use the largest number of characters possible.
- The password must not contain a user name or surname(s) and avoid using easily guessed passwords such as those derived from initials, user ID, address, telephone number, license plate of your car, date of birth, spouse's name, children's names, pet's name, etc.
- Passwords should be difficult to guess. A password must contain one letter in upper case (A, B, C…Z), one letter in lower case (a, b, c…z) and one digit (0, 1, 2…9) at a minimum.
- Do not reuse any of the previous four (4) passwords.
- If prompted to save passwords while using Internet Explorer, select "No".
- The sign on procedures require the user to enter a name and password. The password is entered invisibly on the screen. Access to the menu selections are assigned to a particular user by the IT Department in conjunction with information provided by the Police Department Information Services Administrator. The Information Technology Department (IT) monitors, on a regular, recurring basis, authorized passwords and access codes, and observes for evidence of security violations.

The Information Services Administrator or designee shall notify the IT Department as necessary to remove a user from the mainframe system and to disable the User Profile. The Information Services Administrator or designee shall provide necessary information to the IT Department when a user will be replaced.

Outside Computer Software and Data

Section X and XI of the City of Greenville "Computer Security and Use Procedure" govern the introduction of computer software and data into agency controlled computer systems and hardware.

Software

All employees shall comply with all legal obligations that relate to software copyright and licensing agreements. The City of Greenville provides a standard suite of supported software for use. If you require additional software, the following applies:

- IT support staff are responsible for the purchase, installation, and configuration of software/hardware for the City. Software intended for use on City of Greenville servers and other shared resources must be submitted for testing and verification to IT support staff before installation.
- Installation of any software must be approved by IT Support.
- Do not create or use an unlicensed copy of software

Virus Prevention and Detection

Any file received from an unknown source should be considered highly suspicious and deleted without opening. The following guidelines must be followed to minimize the impact of viruses:

- Ensure that installed virus protection software is not deliberately disabled or prevented from running.
- Never open links received in e-mail, unless certain of the origin of the link.
- Scan all flash drives, CDs, DVDs or other media. This includes media last used on a home computer, and media obtained from business partners, training agencies, service technicians and vendors.
- Scan all software and electronic documents acquired from third parties and external networks.
- Report the suspicion of any virus to the IT support staff immediately.

Files Backup and Storage
Citywide computing systems backup and storage provisions are handled according to the "Information Technology Backup Strategy".

82.2.1 FIELD REPORTING SYSTEM

CALEA Standard: 82.2.1, 82.2.2, 82.2.3

The Greenville Police Department Field Reporting System is electronically housed in the Law Enforcement Records Management System (LERMS). The following forms are utilized:

- Case Report
- Case Supplement
- Arrest Report
- Juvenile Contact
- Field Contact

Specific Reporting Requirements
Information required on all initial field reports of criminal activity is defined by the LERMS system. Specific information requirements parallel reporting requirements by the FBI Incident Based Reporting (IBR) system. Informational items should be documented with all information that is provided to the employee completing the report. Exceptions are informational incidents reported on the case report form where crimes did not occur but the event was determined to need documentation. The data entered, while it would not report to the IBR system, will adhere to the same rules.

Records that document police activity shall include the following information:

- Date and time of the initial reporting
- Name (if available) of the citizen requesting the service, or the victim's or complainant's name
- Nature of the incident
- Nature, date and time of action taken (if any) by law enforcement personnel

Police officers investigating traffic collisions shall follow the procedures set forth in Chapter 61, TRAFFIC governing the use of report forms.

Records Repository
The Greenville Police Department's LERMS maintains a repository of records filed sequentially by incident numbers that includes:

- Incident reports
- Case reports
- Arrest reports
- Crash reports (DMV 349)
- Towed vehicle reports

Reporting Requirements
The following categories of incidents occurring within the jurisdiction of the Department shall be documented in reports, and/or entered into the Computer Aided Dispatch (CAD) system:

- Citizen reports of crimes
- Citizen complaints
- Citizen requests for service when a police officer is dispatched; an employee is assigned to investigate; or an employee is assigned to take action later
- Criminal and non-criminal cases initiated by law enforcement officers
- Incidents involving arrests, citations, or summons

A record shall be made of actions taken by law enforcement personnel in any of the above described circumstances, whether in response to a request for service or for self-initiated actions.

Case Numbering System
The Computer-Aided Dispatch (CAD) system generates a case number system with the following provisions:

- The CAD system is designed to automatically assign a sequential unique number (incident number) to all incidents that also serve as a sequential unique case number to incidents of law enforcement service requiring a case investigation, traffic investigation and/or arrest report.
- The CAD numbering system is designed to ensure that all cases receive a number and that numbers are neither omitted nor duplicated.

Report Submission Procedures
In order to generate a report in the LERMS, an employee should be assigned to a call in the CAD system. Utilizing the reporting system, employees will electronically generate the type of report they will complete. Officers will complete the mandatory fields for the respective form and save the report. Once the report has been completed, employees will use the 'error check' function in the system. If necessary, employees should correct any returned errors. After an error check has been completed, the employee will utilize the 'submit' function to electronically forward the report for supervisory review.

Report Review Procedures
Every report will be reviewed by a supervisor in a timely manner in accordance with Greenville Police Department Policy and Procedures. The supervisor who reviews the report will place his/her electronic signature on the report to indicate the supervisor has reviewed the report and has approved its contents for Departmental purposes. Supervisors shall check reports for accuracy and completeness. Reports not approved will be returned to the police officer completing the report for required corrections. Supervisors will either select "approve" or "reject" before the report is submitted electronically to the Records Unit as verification that they have reviewed the report. Electronically approved reports are automatically forwarded to the Records Unit and normally merged into the LERMS by the next business day. The records unit may reject a report to the reporting employee or supervisor.

82.2.2 DISTRIBUTION OF REPORTS AND RECORDS

CALEA Standard: 82.1.1, 82.2.4

The Records Unit personnel shall process reports and records by merging the original documents into the LERMS storage system. After the record is merged it is permanently stored in the LERMS storage system in accordance with NC Records Retention laws.

Internal Distribution
The Special Investigations Supervisor and the Criminal Investigations Supervisors shall utilize their assigned computers to review reports and records for follow-up assignment. Supervisors will screen all cases and make case assignments in accordance with Greenville Police Department Policy and Procedures, Chapter 42.

External Distribution
Copies of police reports will be provided to law enforcement/criminal justice agencies upon request. The information contained in the police report must be needed for performance of their official law enforcement duties. The only exception to this rule is the Special Investigations case files.

The release of information from the Special Investigations case files must be authorized by either the investigating officer or the Special Investigations Supervisor.

The Greenville Police Department shall release the following records to the public upon request:

- Select pages of case reports
- Redacted arrest reports

- Redacted NC DMV-349 Crash reports

Requests for audio and video recordings must abide by N.C.G.S. 132-1.4A and follow the procedures described in departmental policy Chapter 83.

Requests for reports can be made in person, through written request, or on-line. On-line reports include:

- eCrash
- Daily case reports
- Daily arrest reports
- Drug Arrest report
- Daily calls for service
- RAIDS online crime map

All reports of incidents involving juveniles as either the victim or suspect, or incidents involving sex crimes shall have the names of the juvenile or the sex crime victim removed.

North Carolina General Statute 132-1.4 stipulates that records of criminal investigations or records of criminal intelligence information are not public records with the following exceptions:

- The time, date, location, and nature of a violation or apparent violation of the law reported to a public law enforcement agency
- The name, sex, age, address, employment, and alleged violation of law of a person arrested, charged, or indicted
- The circumstances surrounding an arrest, including the time and place of the arrest, whether the arrest involved resistance, possession or use of weapons, or pursuit, and a description of any items seized in connection with the arrest
- The name, sex, age, and address of a complaining witness

Greenville Police Department personnel may temporarily withhold the name or address of a complaining witness pursuant to North Carolina General Statute 132-1.4, if release of the information is reasonably likely to pose a threat to the mental or physical health or personal safety of the complaining witness or materially compromise a continuing or future criminal investigation or criminal intelligence operation. Release of the information is governed by North Carolina General Statute 132-6.

The Greenville Police Department may release other records not categorized as confidential to the public upon request.

82.3.1 RECORDS INDEX

CALEA Standard: 82.3.1, 82.3.2

Master Name Index (Global Jacket)

An alphabetical master name index is maintained through the LERMS computer system. The master name index includes names of persons identified in incident reports, supplemental reports, arrest reports, NC DMV-349 crash reports traffic citations, tow/impound reports and mug shots. The following types of people meet the criteria for inclusion into the master name index:

- Victim
- Reporting Party
- Suspect/Offender
- Arrestee
- Witness
- Injured (crash report related)
- Other/Mentioned

- Persons of Interest

Calls for Service Records
The Greenville Police Department maintains a computerized database containing records that include service calls, crimes by type, and crimes by location. This information is available to all Department personnel via computerized query of the RMS Computer Aided Dispatch (CAD).

Stolen, Found, Recovered, and Evidentiary Property Index
The Property & Evidence Unit maintains a record of all found/recovered property, evidentiary property, property retained for safekeeping, and property to be destroyed. All property received by the Property & Evidence Unit is recorded in the LERMS property module by the Property and Evidence Unit. All property is recorded as part of the case report and filed in the Property and Evidence Unit as outlined in Chapter 84 of the Greenville Police Department Policy and Procedures Manual.

Prior to submitting the property or evidence to the Property & Evidence Unit, police officers shall request a query of the DCI/NCIC files for any property that has a unique identifying number to determine if the property has been reported stolen. Stolen property will be cleared/located from the DCI/NCIC files in accordance with DCI regulations.

82.3.2 TRAFFIC RECORDS SYSTEM

CALEA Standard: 82.3.3, 82.3.4

The Greenville Police Department utilizes various systems to maintain or have access to traffic information to include:

- Crash data, (reports, investigations, and locations)
- Traffic enforcement data, (citations, arrests, dispositions, and locations)
- Report of roadway hazards and hazardous conditions

The Traffic Safety Unit utilizes TEAAS – Traffic Engineering Accident Analysis System to collect statistical information. Additionally, the LERMS provides accurate information including locations of crashes and citations to field personnel and provides data upon which management decisions can be based.

Greenville Police Department Policy and Procedures Manual, Chapter 61, *Traffic*, identifies data to be collected, analyzed, and disseminated relative to traffic records.

Traffic Citations
The Administrative Office of the Courts manages the automated program eCITATION used by NC law enforcement agencies. eCITATION allows officers to issue a state citation for traffic offenses without having to handwrite data. The forms are completed electronically and the offenders copy is printed from the vehicle. Once an officer has submitted the information, it is uploaded almost immediately to the local Clerk of Superior Court's office.

Officers are issued Uniform Traffic Citation books as needed. Handwritten citations should be utilized for driving while impaired offenses and city ordinance traffic violations. The Field Operations Bureau Staff Support Specialist shall obtain uniform state citation books from the Clerk of Court as needed. Uniform state citation books shall be stored in a secured area with restricted access. Watch commanders or supervisors shall contact the Field Operations Bureau Staff Support Specialist to obtain state uniform citation books which are then assigned to the requesting supervisor. The Field Operations Bureau Staff Support Specialist shall record the control numbers from each uniform state citation book issued and the date issued. The requesting supervisors shall issue citation books to the police officers and shall maintain a log of citation books assigned to police officers.

Accounting for Citations and Citation Books
Police officers are accountable for the citation books issued to them. Citations are cross-referenced by the issuing police officer's name and date of issuance.

If a citation or citation book is lost or stolen, the police officer shall immediately notify the police officer's on-duty supervisor. The police officer shall write and submit a memorandum that explains the circumstances of the loss. The citation control number(s) should be identified in the memorandum. If either a citation or a citation book is missing, a copy of the memorandum submitted by the police officer should be taken to the Clerk of Court's office.

The police officer shall return used citation books to the on-duty supervisor. The supervisor shall inspect the used citation book to ensure that all necessary copies are accounted for, and record the used citation book as being returned next to the name of the police officer submitting the book. The supervisor shall verify that all of the yellow copies of the citations have been left in the citation book prior to returning the used citation books to the Field Operations Bureau Staff Support Specialist.

Additional policy and procedures relative to the preparation and accountability for Uniform Traffic Citations is presented in the Greenville Police Department Policy and Procedures, Chapter 61, *Traffic.*

82.3.3 OPERATIONAL COMPONENT RECORDS

CALEA Standard: 82.3.5

Operational records are maintained as follows:

- The Greenville Police Department's LERMS shall be the central repository for all offense and incident reports, arrest reports, citations, other field reports, and official records.
- The Greenville Police Department's eCrash server shall be the central repository for all NC DMV-349 crash reports completed in-house. Statistical data for crashes will be imported from the eCrash server into the LERMS.
- The Special Investigations Unit shall maintain a secured file containing Greenville Police Department Intelligence and Informant activities.
- The Special Victims Unit shall maintain only working files of current investigations concerning juveniles.
- The Administrative Services Bureau shall maintain the Department's personnel records and training records.

82.3.4 CRIMINAL IDENTIFICATION AND HISTORY

CALEA Standard: 82.3.6

Criminal History File
The Department database includes a criminal history file maintained on every person arrested by the Department. The file can include:

- Fingerprint card
- Criminal history transcripts (state and federal)
- Photograph (mugshot if available)
- Arrest reports

Arrestee criminal history file information is maintained in at least one of the following locations:

- North Carolina State Bureau of Investigation, Division of Criminal Information (DCI)
- Police Department LERMS
- Clerk of Court's office
- Greenville Police Department Forensic Services Unit

All information subject to inclusion in an arrestee's criminal history file is accessible through the DCI terminal and is cross-referenced according to a number of descriptors including, but not limited to:

- Name
- Case number
- FBI number
- SID (state identification) number

Arrest Identification Number

The Greenville Police Department's records management system automatically assigns a unique global jacket number to each person entered in the system. All arrests and other information concerning that person should be referenced to his or her global jacket number. The Information Services Administrator or designee shall ensure that numbers are not skipped or duplicated.

Access and Dissemination of Criminal History Records

The State Bureau of Investigation (SBI) Division of Criminal Investigative Records (DCI) maintains a computerized criminal history of individuals who have been arrested and/or for which the SBI has a valid criminal fingerprint card.

Access is restricted to DCI authorized law enforcement/criminal justice agencies and personnel.

DCI provides an automated log of criminal/investigative inquiries. The automated log will contain the information supplied by the operator in the inquiry screen. Secondary dissemination to any person outside the initial requesting agency must be indicated in the inquiry screen or in the case file pertaining to that record. All inquiries and disseminations must comply with all DCI rules regarding access and dissemination. Any misuse or possible violations must be reported to DCI. Violations may result in loss of access and/or fines to the agency.

The NC SBI identifies all regulations and requirements for DCI certification, access, and dissemination of criminal histories.