CITY OF LYONS POLICE DEPARTMENT

POLICE OPERATIONS MANUAL

CHAPTER: 14 - Records/Information Management

EFFECTIVE DATE: February 1, 2012 **NUMBER OF PAGES: 62**

REVISED DATE: October 21, 2026 **DISTRIBUTION: All**

SPECIAL INSTRUCTIONS: None

INDEX

I. PURPOSE

II. DEFINITIONS

III. RULES AND REGULATIONS

S.O.P. 14-1 COMMUNICATIONS/FIELD INCIDENT REPORTING

S.O.P. 14-2 RELEASE OF INFORMATION TO THE NEWS MEDIA

S.O.P. 14-3 DISSEMINATION OF PROTECTED INFORMATION

S.O.P. 14-4 INDIVIDUAL INSPECTION OF CRIMINAL HISTORY

S.O.P. 14-5 RELEASING CRIMINAL HISTORY INFORMATION TO NON-CRIMINAL JUSTICE AGENCIES AND INDIVIDUALS

S.O.P. 14-6 GCIC/NCIC ENTRY

S.O.P. 14-7 PROTECTION OF RECORDS SYSTEM INFORMATION AND THE CRIMINAL ANALYST

S.O.P. 14-8 RECORDS SAFETY DURING NATURAL OR MAN MADE DISASTER

S.O.P. 14-9 RECORDS RETENTION POLICY

S.O.P. 14-10 FLOCK SAFETY ALPR

I. PURPOSE

A. To establish and prescribe guidelines for processing and filing reports.

B. To establish individual position responsibilities as part of the overall records management system.

C. To establish guidelines concerning the release of public information and public cooperation.

D. To establish a standard operating procedure regulating the release of information to the news media.

E. To establish a standard operating procedure regulating the dissemination of protected information.

F. To establish a standard operating procedure for the processing of civil process served on the Department or its employees.

II. DEFINITIONS

CRIMINAL JUSTICE HISTORY INFORMATION - Information collected by criminal justice agencies on individuals including identifiable descriptions and notations of arrests, detentions, indictments, accusations, information or other criminal charges, and any dispositions arising there from, including sentences, correctional supervision, and releases.

RESTRICTED INFORMATION - Information involving data gathering techniques, CJIS network operational procedures, manuals and forms.

SECRET - Information involving elements of the operation, programming, and security constraints of the GCIC/CJIS and satellite computer system.

III. RULES AND REGULATIONS

Overview of Records Management - The records management system of this Department is designed to reflect the system recommended by the Georgia Crime Information Center (GCIC) in the Georgia Law Enforcement Records Management Manual. A copy is maintained for reference in the Administrative Services Division.

A. The Department shall provide training for the appropriate employees to ensure the effective performance of job-specific tasks relating to:

1. The use of the Georgia CJIS System;

2. The use of the National Crime Information Center (NCIC);

3. The use of the National Law Enforcement Telecommunications System;

4. The security and dissemination of criminal history record information;

5. State and national Uniform Crime Reporting (UCR) programs;

6. Fingerprinting of arrested persons and the initiation of Offender Based Tracking System (OBTS) forms; and

7. The preparation and submission of reports of final dispositions of charges.

B. Records System for Civil and Criminal Process - Records will be maintained for each item of civil and criminal process. The records will include information on the following:

1. Date and time received;

2. Type of process;

3. Nature of document;

4. Source of document;

5. Name of plaintiff/complainant or name of defendant/respondent;

6. Officer assigned for service;

7. Date of assignment;

8. Court docket number; and

9 Date service is due and court date,

C. Records will be maintained on the service or execution of civil/criminal process. The records will include the following information:

1. Date and time served;

2. Name of officer making service;

3. To whom process was served or to whom executed;

4. Method of service;

5. Location of service.

STANDARD OPERATING PROCEDURE

EFFECTIVE: February 1, 2012

S.O.P. 14-1 COMMUNICATIONS/FIELD INCIDENT REPORTING

I. INTRODUCTION

The Communications/Field Incident Reporting system describes the personnel and various duties that shall be performed to collect information, process and file reports for the Department's records system.

II. DUTIES

A. Dispatch Center Officers' Duties:

The Dispatch Center is the point in the system at which most report processing originates. The dispatchers are responsible for:

1. Receiving complaints from all sources and relaying this information to officers to respond to those complaints;

2. Providing communications support to officers in the field;

3. Recording all activity of officers in the field and being continuously aware of their status and pending emergency conditions;

4. Recording law enforcement activities with the following documents:

   a. Complaint Card: Used to record the receipt of a complaint or other notification of impending activity including traffic stops. After the complaint is answered, the time and nature of police action taken is recorded. All incidents and traffic stops which result in formal documentation by the responding officer are assigned a case number. **NOTE: The Complaint Card can either be a physical piece of paper or a computer record.**

   b. Before completion of each tour of duty, the dispatcher will prepare an incident report log showing all actions documented by the shift. The format is as follows:

      OFFICER # / TYPE OF CALL / LOCATION / DISPOSITION
      (Shown by patrol area)

      NOTE: The incident report log can either be a physical piece of paper or a computer record.

B. Patrol Officers' Duties:

When providing normal law enforcement services, patrol officers perform four primary duties including patrol and surveillance, investigation of offenses, arrest of offenders, and public service and assistance. In performance of these duties, the following records shall be completed by law enforcement officers:

1. Incident Report: Used in describing the incident which has occurred and those actions taken by the officer; reporting names and other related information on persons involved in incidents; recording serialized and non-serialized articles, events, suspects and witnesses, statements and investigative leads, recording the details and events that led the officer to believe that a crime was committed, recording the details and events wherein a person or persons was arrested and brought to a detention center; incident reports are not to be used to report damage to police property that is not criminal in nature;

2. Miscellaneous Incident Report: Used in reporting those incidents that are non-traffic and non-criminal in nature;

3. Supplemental Incident Report: Used in recording follow-up investigations and all overflow information from the Incident Report;

4. Arrest/Booking Report: Used in recording details of an arrest and booking;

5. Officer Activity Log: Used primarily by officers to record their daily activities;

6. Uniform Traffic Citation: Used in recording a traffic violation

    a. All citations will be written uniformly; all blanks to be filled in on citation.

    b. When writing a citation, write plain and clearly.

    c. The location is where the offense took place; not where the vehicle stops.

    d. Use the City Street Names on all citations (First Street, McIntosh Street,)

    e. Upon issuing citations, officers will be required to turn in completed citations with an arrest booking to his/her shift supervisor prior to ending his/her tour of duty.

f. All officers are to write citations in order from the ticket book they are assigned to and complete it before going to another. Upon completion of a citation book the officer will turn the completed citation book into the records clerk at which time a thorough accounting will be performed before a new citation book is issued.

g. Remember, when writing a citation that the subject is being arrested for, the jail gets the issuing department copy. The only exception is when a citation is going with a criminal warrant, then the issuing department copy is turned into Captain of UPD and the rest of the citation goes with the warrant.

7. Courtesy Warning Citation: Used in recording a traffic stop where a UTC is not issued;

8. Uniform Accident Report: Used in recording a vehicle accident;

9. Wrecker Pull/Vehicle Impound/Inventory Report: Used in recording a vehicle which is impounded/inventoried/pulled;

10. City of Lyons Summons (Citation); Used in recording city ordinance violations **(Note: The procedures for City Citation Books is the same as the procedures used for Uniform Traffic Citation)**.

11. Officer will enter their reports into the department's computer system.

C. Shift Supervisors' Duties:

Shift supervisors are responsible for the immediate supervision, control and administration of personnel on their shift, and for activities or incidents which occur during their shift. Duties include reviewing and approving all reports generated during the shift, in order to ensure that each is clear, accurate, legible, and completed according to established procedures and policies.

Shift supervisors shall account for each complaint number issued and the corresponding complaint cards with required reports, using the Incident Report Log as the final check.

D. Records Personnel's Duties:

The records personnel are responsible for the distribution, indexing, filing, and retrieval of information resulting from investigations and other activities conducted by the Department. Records personnel perform the following functions:

1. Receiving and verifying all reports entered into the Department's computer system;

2. Distributing copies of forms and reports to the courts and prosecutor when required;

3. Indexing and filing Departmental copies of all reports. To include copying arrest file data to the department's archive system. Arrest file data will include the following items at a minimum:

    a. Completed fingerprint cards

    b. Copy of criminal history transcript

    c. Booking photograph

    d Copy of arrest report;

4. Receiving, entering, and updating all arrest and booking reports in the Department's computer system. Records personnel will ensure that each person arrested has only one jail management ID number;

5. Forwarding fingerprint cards to GCIC;

6. Forwarding criminal dispositions requested;

7. Entering, updating and canceling GCIC/NCIC entries (in coordination with the Dispatch Center);

8. Entering, updating, and canceling warrants in the department's computer system.

9. Extracting data which are needed for the UCR and existing internal reports, and generating these reports;

10. Records processing - All forms used in the Incident Reporting and Records Management System will be processed by the records personnel. These forms and duties are outlined below:

    a. Complaint Card, Incident Report, Miscellaneous Incident Report, Supplemental Report, Uniform Traffic Ticket, Courtesy Warning Citation, Accident Report. Received for all pertinent agency activities. Used for:

        1). Extracting data needed to complete UCR and departmental reports;

        2). Storing documents in the appropriate files.

b. Arrest/Booking Report - Provides details of the arrest, booking and court disposition. Used for input into UCR and filed in Arrest File and Case File;

c. GCIC/LEDS Worksheets - Used to enter, add, cancel, delete information to the GCIC/NCIC System.

STANDARD OPERATING PROCEDURE

EFFECTIVE: February 1, 2012

S.O.P. 14-2 RELEASE OF INFORMATION TO THE NEWS MEDIA

I. PURPOSE

It is the purpose of this policy to establish guidelines for release and dissemination of public information to print and broadcast news media.

II. POLICY

It is the policy of this law enforcement agency to cooperate fully and impartially with authorized news media representatives in their efforts to gather factual, public information pertaining to activities of the department, as long as these activities do not unduly interfere with departmental operation, infringe upon individual rights or violate the law.

III. DEFINITIONS

A. Public Information: Information that may be of interest to the general public regarding policy, procedures or events involving the department or other newsworthy information that is not legally protected, does not unduly interfere with the mission of the department, infringe upon the rights of a defendant or compromise the legitimate safety and privacy interests of officers, victims, witnesses or others.

B. News Media Representatives: Those individuals who are directly employed by agencies of the electronic or print media such as radio, television and newspapers. Freelance workers in this field are to be regarded as other members of the general public unless otherwise designated by the departmental chief executive.

C. Public Information Officer (PIO): The department's PIO serves as a central source of information for release by the department and responds to requests for information by the news media and the community.

IV. PROCEDURES

A. Duties of the PIO

The department's PIO is available to

1. Assist news personnel in covering routine news stories, and at the scenes of incidents;

2. Assist the news media on an on-call basis;

3. Prepare and distribute news releases;

4. Arrange for, and assist at, news conferences;

5. Coordinate and authorize the release of information about victims, witnesses and suspects;

6. Assist in crisis situations within the agency; and

7. Coordinate the release of authorized information concerning confidential agency investigations and operations.

B. Cooperation with the Media

1. Authorized news media representatives shall have reasonable access to the PIO, the agency's chief executive or his designee and operations of the government as governed by this policy. When information must be denied to a media representative, the basis for that denial shall be fully and courteously explained.

2. This department recognizes authorized identification from all local, national and international news organizations. Failure of media personnel to present authorized identification may provide grounds for restricting access to requested information or to incident scenes.

3. Public information shall be released to the media as promptly as circumstances allow, without partiality and in as objective a manner as possible.

4. Public information may be provided to media representatives by telephone if the identity of the representative is known or can be authenticated.

5. Ranking officers at crime or incident scenes may release information of a factual nature to the media as governed by this policy or refer the inquiry to the PIO. Where the officer is unsure of the facts or the propriety of releasing information, he shall refer the inquiry to the PIO.

6. Written press statements shall be released only following approval of the department's chief executive or his designee.

7. The dispatch center shall inform the watch commander as soon as possible upon receipt of information about events or activities that may have media interest.

8. The watch commander shall be responsible for ensuring that the agency's PIO or chief executive is informed of events that may have media interest.

C. Investigative Information

From the initial stage of a criminal investigation until the completion of trial or disposition without trial, police personnel shall refer all requests for information to the department chief executive or his designee.

1. Information that may be released in connection with an investigation of an event or crime includes:

   a. the type or nature of an event or crime;

   b. the location, date and time, injuries sustained, damages and a general description of how the incident occurred;

   c. type and quantity of property taken;

   d. the identity and approximate address of a victim with the exception of sex crime victims, and in other cases where reprisals or intimidation may be employed;

   e. requests for aid in locating evidence, a complainant or a suspect;

   f. numbers of officers or people involved in an event or investigation, and the length of the investigation; and

   g. name of the officer in charge of a case, his supervisor and division or unit assignment (exception: the name of any undercover officer will not be released).

2. Information that may not be released in connection with an investigation of an event or crime, unless authorized by the department chief executive or his designee, include

   a. The identity of a suspect prior to arrest unless such information would aid in apprehending the suspect or serve to warn the public of potential danger;

   b, The identify of any victim of a sex crime or any related information which, if divulged, could lead to the victim's identify;

   c. The identity of victims or witnesses if such disclosure would prejudice an investigation to any significant degree, or if it would place the victim in personal danger;

   d. The identity of any juvenile who is a suspect or defendant in a case subject to the jurisdiction of the juvenile court;

e. The identity of any critically injured or deceased person prior to notification of next of kin;

f. The results of any investigative procedure such as lineups, polygraph tests, fingerprint comparison, ballistics test or other procedures (the fact that these tests have been performed may be revealed without further comment);

g. Information which, if prematurely released, may interfere with the investigation or apprehension such as the nature of leads, specifics of an "MO", details of the crime known only to the perpetrator and the police, or information that may cause the suspect to flee or more effectively avoid apprehension;

h. Information that may be of evidentiary value in criminal proceedings;

i. Specific cause of death unless officially determined by the medical examiner; and

j. The home address or telephone number of any member of the department.

D. Arrest Information

1. Following arrest, issuance of an arrest warrant or filing of an information or indictment, it is permissible to release

a. The accused’s name, age, residence, occupation and family status;

b. The time and place of arrest whether pursuit or resistance was encountered, whether weapons were used, charges placed against the suspect and description of contraband seized;

c. The identity of the arresting officers and the duration of the investigation unless the officers are engaged in undercover operations; and

d. The amount of bond, scheduled court dates and place of the suspect's detention.

2. Following arrest and formal charging of a suspect, but prior to adjudication, the following types of information should not be released without express permission of the department's chief executive:

   a. Prior criminal conviction record, character or reputation of a defendant

   b. Existence or contents of any confession, admission or statement of a defendant, or his failure or unwillingness to make a statement

   c. Performance or results of any tests, or a defendant's refusal or failure to submit to tests such as a polygraph

   d. Identity, statement or expected testimony of any witness or victim

   e. Any opinion about the guilt or innocence of a defendant or the merits of the case

   f. Any opinion or knowledge of the potential for a plea bargain or other pretrial action

E. Special Considerations - Criminal Matters

1. Departmental personnel shall extend every reasonable courtesy to news media representatives at crime scenes. This may include closer access of personnel and equipment than available to the general public to the degree that it does not interfere with the police mission or the movement of traffic.

2. The news media shall not be allowed access to any area or scene of an incident or crime where there is a possibility that evidence may be damaged, altered, destroyed or otherwise prejudiced by its existence being published or portrayed. Once evidence has been processed, removed and secured by the department, the media may be allowed to enter by permission of the commanding officer at the scene.

   a. On private property, photography, film or videotape recording requires the permission of the owner or the owner's representative.

   b. Suspects or accused persons in custody shall not be posed or arrangements made for photographs, telecasts or interviews, nor shall departmental personnel pose with suspects or accused persons in custody.

c. When an individual is charged with a criminal offense and is sought by law enforcement authorities, photographs or mug shots may be released to the media to help locate the individual. No departmental photographs, mug shots, videotape, film or composites of subjects in custody shall otherwise be released to the media unless authorized by the department chief executive or authorized designee.

3. At the scene of major crimes, such as hostage and barricade situations, the officer in charge shall designate a preliminary press area as early as possible and as close to the scene as safety and operational requirements allow.

4. The fact that a suicide or suspected suicide has occurred may be reported to the media, along with factual information describing how it happened. The name, age, address, sex and occupation of the victim may also be released following notification of next of kin. The fact that a suicide note exists may also be acknowledged without further comment. The content of such notes is personal and confidential and shall not be released except as provided by law.

F. Special Considerations – Non-criminal Matters

1. At the scene of significant accidents, man-made or natural catastrophes, the principles of media cooperation shall be maintained to the degree that they do not interfere with the mission of the police, fire, medical or other emergency relief workers.

2. Media access to and movement within fire lines shall be controlled by the fire officer in charge. In consultation with the fire officer in charge, the ranking police officer at the scene shall establish an observation point from which the media may observe and photograph the incident.

a. At the discretion of the officer in charge, an inner perimeter may be established for the media from which to record the event.

3. News media representatives should not be prevented from access to any area solely because of the possibility of their injury or death. If this is the only consideration, the media representative should be advised of the danger and allowed to make the decision to enter on his/her own volition.

4. Sensitive information relating to internal investigation of police officers shall not be released without the express permission of the department chief executive.

5. Daily administrative reports of criminal activity will be made available on a routine basis to media representatives. Statistical reports of criminal activity will also be made available to the media.

6. Media representatives shall be denied access to the contents of investigative or incident reports and records where release of the information would;

   a. Interfere with law enforcement proceedings, including pending investigations;

   b. Deprive a person of the right to a fair trial or an impartial adjudication, or give one party to a controversy an undue advantage by exclusive access to such information;

   c. Constitute an unwarranted invasion of the personal privacy rights of another person;

   d. Reveal the identity of an individual who has furnished information to the department under confidential circumstances;

   e. Disclose investigative techniques and procedures, thereby impairing future effectiveness of the department; or

   f. Endanger the life or physical safety of any person.

The press serves the public by supplying information, stimulating thought, and providing a medium for expression. The news media exercises a genuine interest in the public good and greatly influences public opinion. Crime, its results, and the efforts to combat it are matters of continuing public concern. The Department is regularly involved in events at which members of the news media are present and gathering information.

B. Role of the Department

The Department actively seeks to establish a cooperative environment in which the news media may obtain information on matters of public interest without hampering departmental operations. However, certain information will be withheld from the news media to protect the constitutional rights of an accused, to avoid interfering with a Department investigation, or because it is legally privileged (see S.O.P. 14-2 Dissemination of Protected Information).

C. Responsibility for the Release of Information

1. When an event being investigated is of a spectacular or unusual nature and stimulates general community interest, the news media will be notified at the discretion of the Chief of Police or his designee.

2. When an incident involving departmental policy or the interpretation of policy occurs, or statements are requested which may adversely reflect on the Department's reputation, the release of information will be made at the discretion of the Chief of Police or his designee.

3. A release of information in an on-going investigation shall be made at the discretion of the Chief of Police or his designee.

4. In other cases, the type of information listed in Section 3 below may be released by the ranking officer present, upon approval of the Chief of Police or his designee.

D. Scope of Content for News Releases

In cases other than on-going criminal investigations, only the following information shall be made available to the news media:

1. Accused's name (if adult), age, residence, sex, race, employment, and marital status. If juvenile, arrest status only;

2. Originating source of information for the action, either citizen complaint, officer initiated, warrant or indictment;

3. The length of the investigation and present status, either active or concluded;

4. The immediate circumstances surrounding the arrest including time, place, any acts of resistance on the part of the arrestee, and a description of any items seized;

5. Information on the victim shall be limited to the following:

   a. If a victim is killed or seriously injured as a result of the action, his/her name or address cannot be released pending notification of next of kin;

   b. If it involves a crime against a person:

      1). physical status (e.g., hospitalized with a gunshot wound);

      2). relationship to suspect;

      3). sex; age; race.

   c. If it involves a property crime other than a business, identification of the victim, no address. An address can be included on businesses.

6. Officers and employees of the Department shall not make statements at public gatherings concerning the plans, policies, or affairs of the administration of the Department unless directed by the Chief of Police;

7. Responsibility for publicity for the Department shall be delegated by the Chief of Police.

D. Releasing Photographs to the Media

Employees of the Department will neither encourage nor discourage the media from photographing or televising defendants when they are in public places. Employees of the Department shall not position or pose the accused for the benefit of the media.

E. Allowing News Media to Enter Area of a Serious Incident or Crime Scene

Police lines may be established to prevent persons from entering the area of a serious incident or crime scene. Dependent upon the tactical situation and the likelihood of jeopardizing police operations, members of the news media may be allowed in these areas. Authorization for entry is normally dependent upon the judgment of the supervisor present. While the news media may be permitted in the area of a crime scene or a serious incident, he/she does not have the author-ity to be within an area which has been secured to preserve evidence, or at any location where his/her presence jeopardizes police operations.

F. News Media Not Exempt from Laws

A newsperson's primary responsibility is to report the news by obtaining information and photographs of newsworthy incidents. His/her opportunity to do so is frequently at an emergency scene. An officer sharing these circumstances with a newsperson should not obstruct him in the performance of his/her duty. However, members of the news media are neither implicitly nor expressly exempt from the requirements of any municipal, state, or federal statute.

G. Requesting Withholding of Publication

Newspersons may photograph or report anything they observe when legally present at any emergency scene. When publication of this coverage would interfere with an official investigation or place a victim, suspect, or others in jeopardy, the withholding of publication is based on decisions of a cooperative press, not censorship by the Department. Under these circumstances, officers should advise newspersons or their superior officers of the possible consequence of publication. However, officers may not interfere with newsperson's activities as long as the newsperson's performance remains within the confines of the law.

STANDARD OPERATING PROCEDURE

EFFECTIVE: February 1, 2012

S.O.P. 14-3 DISSEMINATION OF PROTECTED INFORMATION

I. INTRODUCTION

The Department shall disseminate accurate and factual accounts of occurrences of public interest not protected by law. This dissemination is to be made with consideration of an individual's legal rights and the confidentiality of Department records.

II RULES AND REGULATIONS

A. Records maintained or originated by the Department which are and are not covered by Federal and State Privacy Laws:

Covered	**Not Covered**
Arrest Fingerprints	Uniform Crime Reporting Form
Final Disposition	Incident Report
Misdemeanor "Rap Sheets"	Supplemental Report
	Felony "Rap Sheets"
	Arrest Booking Report
	Uniform Traffic Ticket
	Radio Log
	Jail Docket
	Complaint/Dispatch Cards
	Miscellaneous Incident Reports

B. Release of all criminal history information to individuals shall be done in accordance with the Rules of the Georgia Crime Information Center Council.

C. The release of any photograph made by the Department shall be as follows:

1. Crime Scene - Any photograph made at the crime scene, or for any official on-going investigation, shall be processed and made available only to the investigating officer, investigating agency, or to the District Attorney. No photographs shall be disseminated to, or viewed by, anyone else without the written approval of the Chief of Police, the District Attorney, or without a Court Order.

2. Traffic Scene - Provided no death or serious injury resulted, traffic accident photographs may be reproduced and released to the victim's insurance company, or its agent, or to the victim's attorney, for civil action. Disseminations are subject to a fee to cover the associated costs. When death or serious injury occurs in an accident, no photograph shall be released to anyone, other than the investigating officer/agency, or the District Attorney, unless approved in writing by the Chief of Police, the District Attorney, or without a Court Order.

3. Uniform Crime Reporting - Each law enforcement agency is required by law to participate in the Uniform Crime Reporting (UCR) program. UCR reports include:

    a. Reports of criminal offenses reported to or investigated by law enforcement agencies;

    b. Reports of persons arrested (Arrest/Booking Report and Incident Report);

    c. Reports of offenses cleared by arrest or exceptionally cleared;

    d. Special reports on juveniles arrested for DUI (Juvenile DUI Arrest Reports);

    e. Special reports on all homicides;

    f. Special reports on law enforcement officers killed or assaulted in the line of duty;

    g. Special reports on known or suspected arson;

    h. Special reports on juvenile arrests or administrative dispositions of juvenile offenders;

    i. Special reports on the number and type of law enforcement agency employees.

4. Applicability of State and Federal Laws and Regulations: All State and Federal Statutes not referenced in this procedure shall be adhered to by the employees of this Department and shall supersede this procedure if some conflict should exist between it, the law, or GCIC Rules and Regulations.

STANDARD OPERATING PROCEDURE

EFFECTIVE: February 1, 2012

S.O.P. 14-4 INDIVIDUAL INSPECTION OF CRIMINAL HISTORY

I. INTRODUCTION

The Lyons Police Department will assist citizens who request to inspect their local or Georgia criminal history records. This assistance will only be provided upon the establishment of the persons identity, as prescribed in the implementing procedures of this standard operating procedure.

II. PROCEDURES

A.Local Records Check:

1. Records Clerk: When a citizen requests to inspect his/her criminal history record, the clerk will determine if the person wishes to inspect his/her local record or Georgia criminal history record.

   a. If the person wishes to inspect his/her local record, the clerk will positively identify the person. Positive identification for a local records check **SHALL** include the presentation of a Georgia Drivers License or an Identification Card issued by the Georgia Department of Public Safety or a Military Identification Card **AND** the vouching for the person's identity by a member of the department or a citizen known to a member of the department.

   b. If the person has been identified and requests a local records check:

      1). Complete the Request to Inspect Local Record Form. This form must be signed and notarized.

      2). Inform the person that the charge for a local records check is $15.00. The fee may be paid in cash, by cashiers or certified check or by money order.

      3). Give the person the Records Inspection Form and direct them to the Senior Records Clerk.

2. Senior Records Clerk: Check the Records Inspection Form, if it is complete, then check the local files:

   a. If the person does not have a record in our files, enter "NO RECORD, LOCAL FILE CHECK ONLY," sign the form and return a copy to the person and file the original in the Record Check Folder.

b. If the person has a record in the local files, show, BUT DO NOT GIVE THEM, a copy of the record. If they verify that the record is/are correct; have the person sign and date Part II, Verification of Record, of the Record Inspection Form. File the signed and dated form in the Verified Record Folder.

c. Log the dissemination in the CHRI in the dissemination log in the Records Room. The purpose of the dissemination is "Record Inspection."

d. If the person challenges the accuracy of the record, have them complete Part III, Challenge of Record, of the Record Inspection Form. Inform the subject that the Captain of the Administrative Services Division will investigate their claim and contact them within FIVE days to resolve their claim.

e. Log the dissemination to the person requesting to inspect his/her record and the dissemination to the Captain of the Administrative Services Division in the CHRI log.

3. Captain, Administrative Services Division:

a. Upon receipt of Record Inspection form take the appropriate action to investigate the matter and contact the person within FIVE days to settle the claim. If unable to settle refer the matter to the City Attorney through the Office of the Chief.

b. If assistance is needed contact the GCIC Security Officer at 404-244-2603.

B. Georgia Records Check

1. Records Clerk: If the person wishes to inspect his/her Georgia record the person **SHALL BE FINGERPRINTED ON AN APPLICANT (BLUE) FINGERPRINT CARD** as proof of the persons identity.

a. Inform the person that a Georgia Records Check will cost $25.00 payable by Certified Check or Money Order made payable to the Georgia Bureau of Investigation.

b. Have the person complete all the Blocks on the Applicant (Blue) Fingerprint Card using a BLACK ballpoint pen except the Reason Fingerprinted Block. This Block is to be completed by the Desk Clerk. The Desk Clerk will enter the following in the Reason Block: "RECORD INSPECTION."

c. Enter the subjects home address in the ORI BLOCK on the Applicant Fingerprint Card.

d. Inform the person to obtain the certified check or money order payable to the Georgia Bureau of Investigation and return to be fingerprinted. Explain that after they are fingerprinted, the Certified Check or Money Order will be sent with their fingerprints to GCIC. GCIC will check their record and their record will be returned to them.

e. Direct the person to the Criminal Investigations Division or the Detention Center to be fingerprinted when they return with the certified check or money order.

2. Fingerprinting Officer: Check the Information Blocks and the Applicant (Blue) fingerprint cards, if they are complete, fingerprint the person and place the Certified Check or Money Order and the completed fingerprint card in an envelope, seal the envelope and return the envelope to the Records Clerk for mailing to GCIC.

3. Records Clerk: When the Fingerprinting Officer returns the sealed envelope, place a mailing label on the envelope and mail to GCIC.

INSPECTION & CHALLENGE OF LOCAL RECORDS

PART I - Subject Identification and Verification:
Identification:
NAME:_____
SEX:_____, RACE:_____, DATE OF BIRTH__/__/__
SOCIAL SECURITY NUMBER___-__-____.

I request to inspect any criminal history record maintained in the local files of the Lyons Police Department.

Signature of Applicant:_____
Notarized:

Verification by: _____
(Initials)
Drivers License Number:_____ (Y) or (N)
State ID Card Number:_____ (Y) or (N)
Military ID Card Number:_____ (Y) or (N)
Name of person verifying Identification:_____

PART II - Verification of Accuracy of Local Record:

I have checked my records in the local files of the Lyons Police Department. These records are correct.

Signature:_____ Date:__/__/__

PART III - Challenge to Local Records:

I challenge the accuracy of the local records maintain by the Lyons Police Department. Specifically I challenge the following records:
_____
_____
_____
_____
_____
_____
_____
(If more space is needed use the back of this form)

Signature:_____
Date of Record Challenge__/__/__

Form turned over to Captain, Administrative Services Division:__/__/__.

STANDARD OPERATING PROCEDURE

EFFECTIVE: February 1, 2012

S.O.P. 14-5 RELEASING CRIMINAL HISTORY INFORMATION TO NON-CRIMINAL JUSTICE AGENCIES AND INDIVIDUALS

I. INTRODUCTION

The Lyons Police Department will provide criminal history information to a non-criminal agencies and individuals upon receipt of a signed, notarized, Consent Form and the payment of a fee.

II. PROCEDURES

A. Records Clerk: Consent forms (UPD Form CHRI-001) are available from this department. They will be issued upon request. Instruct the person to whom the form is issued to fill out the form and have it notarized in duplicate. When a request using a consent form is received from a non-criminal justice agency or individual it will be delivered to the Captain of the Administrative Services Division or his/her designee prior to any action being taken.

B. Captain, Administrative Services Division: Review all requests for criminal history information by non-criminal justice agencies and individuals to ensure all necessary information is provided and the request is signed by the subject of record and properly notarized. Once the information has been verified, the Captain will authorize the Senior Records Clerk to request the information by initialing the form, annotating the form "USE PURPOSE CODE E ONLY" on the face and delivering the form to the Senior Records Clerk.

C. Senior Records Clerk: Log each request prior to requesting the information over the terminal. All requests for CHRI for non-criminal justice agencies/individuals will "USE PURPOSE CODE E ONLY". If "NO RECORD" is received, the remarks section of the CHRI log shall contain the words "NO RECORD." If a positive response is received from the NAME, SEX, RACE, DOB, SSN inquiry, the terminal operator shall transmit a FQ message requesting the full rap sheet. The STATE and FBI numbers from the positive response shall be entered on the log. When the rap sheet is received from the terminal, it shall be attached to the request for criminal history records and placed in an envelope with the name of the person designated to receive the record written on the envelope. The original copy of the consent form shall be filed with the CHRI log.

D. Delivery of the Information: The information will only be delivered to the person whose name appears on the envelope containing the duplicate copy of the signed notarized consent form and the NO RECORD or rap-sheet. Positive identification is required.

E. All employees are reminded that any violation of these procedures can result in criminal prosecution or other administrative action to include termination, suspension, or other form of disciplinary action authorized by the personnel policies.

CONSENT FORM

I,_____
(LAST NAME) (FIRST NAME)(MIDDLE NAME)

RACE_____ HEIGHT_____

SEX_____ WEIGHT_____

DOB_____ EYE COLOR_____

SSN_____ HAIR COLOR_____

Authorize:

_____
(Name of Agency/Individual)

_____
(Name of Person Authorized to pick-up Record)

_____
(Street Address)

_____ _____ _____
(City) (State) (ZIP)

To receive my record from the Vidalia Police Department.

_____
(Signature of Subject)

UNLESS ALL BLANKS ON THIS FORM ARE COMPLETED AND THE FORM IS NOTARIZED, NO INFORMATION WILL BE RELEASED.

STANDARD OPERATING PROCEDURE

EFFECTIVE: February 1, 2012

S.O.P. 14-6 POLICIES AND PROCEDURES FOR GCIC/NCIC RECORD ENTRY

I. POLICY

It is the Policy of the Lyons Police Department to follow GCIC/NCIC guidelines for entry procedures of all records of the GCIC/NCIC Computer Network.

II. INTRODUCTION

All law enforcement agencies shall enter (or cause entry of) information in GCIC and/or NCIC computerized files pertaining to wanted and missing persons, unidentified dead bodies, and serial-numbered property reported as stolen when the required data elements become available.

Each GCIC/NCIC computerized file entry must contain the valid identifier (ORI) of the criminal justice agency responsible for the entry. Responsibilities for the record include entering and updating the record, confirming a hit on the record, and removing the record when it is no longer active or valid.

Record entries shall be made within 12 hours after a determination by the investigating agency that a wanted person should be arrested or that a vehicle or other property identifiable by serial number or owner-applied number was stolen. When agencies receive reports of missing minors, including runaways, records must be entered immediately.

All record entries must be supported by official documents which reflect initial and continuing efforts to apprehend wanted persons or to recover identifiable, serial-numbered stolen property. Originals of arrest warrants must be on hand to support wanted persons record entries.

Agencies with terminals on the Georgia CJIS Network shall maintain these supporting documents in their files until such time as wanted/missing persons are located, stolen property is recovered, or the record entries are removed from the computerized files. When the reasons for record entries are no longer valid, the entries must be removed from GCIC and NCIC computerized files immediately.

III. PROCEDURES

Vehicle Entry - It will be the responsibility of the officer taking the incident report to give a copy of the report to the Records Clerk for entry on the GCIC/NCIC computer.

The Records Clerk must perform an inquiry on the license plate information and/or vehicle identification number prior to entering the record. This inquiry must be done to ensure that the information contained in the report is accurate. If the inquiry produces a "not on file" response, the record will be entered based on the information contained in the report. If the information received from the inquiry does not match the information contained in the report, a supervisor must be contacted to have the information verified. If the information is changed to correspond with the information obtained from the computer, all copies of the report must be corrected.

A LEDS worksheet is to be filled out with the vehicle information prior to entry. A copy of the incident report is to be attached to the original LEDS worksheet along with the computer printout showing tag/vehicle identification number information, the computer printout showing SRN number and NIC number. The operator is then to do an inquiry based on the SRN number. The completed LEDS worksheet (with attachments) and the inquiry are to be placed in the appropriate box for review by a second person. After review by second person, any and all corrections are to be made and the file then placed in the TAC's box for review. After review by TAC, the file will then be ready to be filed. The copy of the LEDS worksheet is to be forwarded to the Investigative Services Division to be placed in the case file.

When a vehicle is cleared or canceled, the computer printout will be attached to the original LEDS worksheet and forwarded to the Investigative Services Division to be placed in the case file. The original report is to be stamped (with the GCIC/NCIC entry stamp) with the appropriate information filled in prior to the original report being forwarded to the Administrative Services Division. Recovered/Abandoned Vehicles - Georgia law requires law enforcement agencies to enter records on vehicles which have been abandoned and impounded by law enforcement agencies or reported as impounded by operators of wrecker services or vehicle storage facilities in the vehicle file.

FOLLOW THE SAME PROCEDURE AS LISTED FOR VEHICLE ENTRY. (Except: do not send the copy of LEDS worksheet to the Investigative Services Division).

Property Entry (i.e. Guns, Articles, Boats, Securities) - It will be the responsibility of the Records Clerk to review all reports to ensure that stolen/missing property is entered on the computer. The Records personnel will review the reports that are forwarded from the precincts and made copies of the ones that have property reported as stolen/missing and contain the necessary information to make the computer entry. Those reports that do not contain the necessary information need not be copies; it will be the responsibility of the investigator handling the case to submit the report for entry after obtaining the required information.

An inquiry is to be performed on the reported stolen/missing item prior to entry to determine if the item is already on computer. A LEDS worksheet is to be filled out prior to entry. A copy of the incident report is to be attached to the original LEDS worksheet along with the computer printout showing SRN and NIC numbers. An inquiry by SRN number will then be performed. The computed LEDS worksheet (with attachments) is to be placed in the appropriate box for review by a second person. After review by second person the file is to be placed in the TAC's box for review. After review by the TAC, the file will be returned for filing. The copy of the LEDS worksheet is to be forwarded to Criminal Investigations Division to be placed in the case file. The original report is to be stamped (with GCIC/NCIC entry stamp) with the appropriate information filled in prior to being forwarded to the Administrative Services Division.

When property is cleared or canceled from the computer, the computer printout will be attached to the original LEDS worksheet and forwarded to the Criminal Investigations Division to be placed in the case file.

Runaway Juveniles - It will be the responsibility of the officer taking the incident report to give a copy of the report to the Records Clerk for entry on the GCIC/NCIC computer (all runaway/missing juveniles must be entered immediately).

A drivers license inquiry should be performed either by name, DOB, race, sex or by OLN number. A LEDS worksheet is to be filled out with the required information prior to entry. A copy of the incident report is to be attached to the original LEDS worksheet along with the computer printout showing SRN and NIC numbers. An inquiry by SRN number should then be performed. The completed LEDS worksheet (with attachments) is to be placed in the appropriate box to be checked by a second person. After being checked by a second person the file is then placed in the TAC's box for review. After being reviewed by the TAC it will be returned for filing. The copy of the LEDS worksheet is to be forwarded to the Investigative Services Division to be placed in the case file. The original report is to be stamped with the (GCIC/NCIC stamp) and the appropriate information filled out prior to the original report being forwarded to the Administrative Services Division.

When the juvenile has been picked up, the record is to be cleared from the computer. If the juvenile returns home and the agency is notified by the parents/guardian, the record is to be canceled from the computer. The computer printout is to be attached to the original LEDS worksheet and forwarded to the Criminal Investigations Division to be placed in the case file.

Warrant Entry - Officers obtaining warrant will submit those warrants to the Records personnel for entry on the GCIC/NCIC computer. If the person is to be available for pick-up nation wide, a copy of the signed extradition paper must be attached to the warrant when it is submitted for entry.

The Records personnel must perform the following inquiries prior to completing the warrant LEDS worksheet:

1. Wanted Person Inquiry

2. Drivers License Inquiry (by name, DOB, race, sex or OLN)

3. Criminal History Inquiry

This is to ensure that all information is available (i.e. alias names, additional DOBs, social security numbers, etc).

If you perform a drivers license inquiry either by name or OLN and it comes back not on file and you obtain other names and social security numbers and dates of birth from your criminal history inquiry, make sure that you run drivers license inquiries on these additional names and social security numbers and dates of birth to see if they are on file. A LEDS worksheet is to be filled out prior to entry. A copy of the warrant, signed extraditions paper (if pick-up is nation wide) and all the computer printouts including the printouts showing SRN and NIC numbers are to be attached to the original LEDS worksheet. An inquiry by SRN number should then be performed. The completed LEDS worksheet (with attachments) is to be placed in the appropriate box to be checked by a second person. After review by second person, the file is to be placed in the TAC's box for review. After being reviewed by the TAC, will be returned for filing. The copy of the LEDS worksheet will be attached to the original warrant and returned to the Investigator's Office (the original warrant must be stamped with the GCIC/NCIC stamp) with the appropriate information filled out prior to being returned to the Investigator's office.

If the subject is arrested, the copy of the LEDS worksheet is to be attached to the original LEDS worksheet and the person is to be cleared from the computer. The computer printout will be attached to the LEDS worksheet and then filed in the proper file (cleared/canceled file).

If the warrant is recalled or dismissed, the copy of the LEDS worksheet is to be attached to the original LEDS worksheet and the person is to be canceled from the computer. The computer printout will be attached to the LEDS worksheet and then filed in the proper file (cleared/canceled file).

Supplemental record entries must be made for all available information (all AKA's must be entered, all additional DOBs must be entered, all social security numbers must be entered).

Missing Persons - It will be the responsibility of the officer taking the incident report to provide a copy of the report to the Records Clerk for entry on the GCIC/NCIC computer. The following inquiries should be made prior to filling out the missing persons LEDS worksheet:

1. Drivers license inquiry

2. Wanted person inquiry

3. Criminal History Inquiry

This is to ensure that all information is available (i.e. alias names, additional DOBs, social security numbers, etc). A LEDS worksheet is to be filled out prior to entry. A copy of the incident report is to be attached to the original LEDS worksheet along with the computer printouts including the computer printout showing the SRN and NIC numbers. An inquiry by SRN number will then be performed. The completed LEDS worksheet (with attachments) is to be placed in the appropriate box for review by a second person. After review by a second person, the file is to be placed in the TAC's box for review. After being reviewed by the TAC, it will be returned for filing. The copy of the LEDS worksheet is to be forwarded to the Investigative Services Division to be placed in the case file.

When the missing person has been located, the record is to be cleared from the computer. The computer printout (showing cleared/canceled) is to be attached to the original LEDS worksheet and forwarded to the Investigative Services Division to be placed in the case file.

If the missing person returns home, the record is to be canceled from the computer. The computer printout (showing clear/canceled) is to be attached to the original LEDS worksheet and forwarded to the Criminal Investigations Division to be placed in the case file.

All entries made on the GCIC/NCIC computer will be checked by a second person and the TAC prior to being filed in the appropriate file. This is to make sure that names are spelled correctly, all information is entered correctly, and that all supplemental information is entered correctly.

The operator checking the entry is to place his/her initials in the upper right hand corner of the LEDS worksheet.

CLEARING/CANCELING RECORDS

Wanted Persons:

If the warrant has been dismissed by the court, the record needs to be canceled. Make sure that the copy of the LEDS worksheet is obtained from the Investigative Services Division. Pull the original LEDS worksheet from the file, cancel the entry from the system. Attach all paperwork together (copy of the LEDS worksheet, computer printout showing clear/cancel, original LEDS worksheet) and file in the appropriate file (clear/canceled file).

If the person is arrested, the record is to be cleared. Obtain the copy of the LEDS worksheet from the Criminal Investigations Division or from the booking officer if arrested by our agency. If arrested by another agency, upon confirming the request for hit confirmation, make sure that a locate message is obtained. Pull the original LEDS worksheet from the file, clear the entry from the system. Attach all paperwork together (copy of LEDS worksheet, computer printout showing clear/cancel, original LEDS worksheet, locate message) and file in the appropriate file (clear/cancel file).

Vehicle - Guns - Articles - Boats - Securities:

If the referenced item is recovered by another agency, upon confirming the request for hit confirmation, make sure that a locate message is obtained. Pull the original LEDS worksheet from the file, clear the record from the system. Attach all paperwork together (locate message, clear/cancel printout, etc) and forward to the Criminal Investigations Division. If the referenced item is recovered by our agency, pull the original entry from the file, clear the record from the system. Attach all paperwork together (copy of incident report showing recovery, computer printout showing clear/cancel, etc.) and forward to the Criminal Investigations Division.

If the record is determined to be invalid, cancel the record from the system. Pull the original LEDS worksheet from the file, attach all paperwork together (copy of incident report, computer printout showing clear/cancel, etc) and forward to the Criminal Investigations Division.

VALIDATION PROCEDURES FOR STOLEN SERIAL NUMBERED PROPERTY RECORDS:

Investigators follow up reports are checked on the in-house computer database for recovery or and other additional information.

An inquiry is made by the TAC, against the record and compared character by character and by ORI against the supporting documentation, additional information is added and incorrect information is corrected, if possible, or the record is canceled and re-entered.

The complainant is contacted by certified letter and asked to respond within 10 days to the TAC to insure that the property has not been recovered or found.

An NAQ file inquiry is made for all stolen cars, trucks, vans, ATV’s, and Motorcycles that were manufactured after 1980 and are entered with a VIN.

STANDARD OPERATING PROCEDURE

EFFECTIVE: February 1, 2012

S.O.P. 14-7 PROTECTION OF RECORDS SYSTEM INFORMATION AND THE CRIMINAL ANALYST

I. INTRODUCTION

The Lyons Police Department will provide protection and back-up for the Computers and the Computerized Criminal Records System maintained by the department. The Computer Systems Manager and Systems Analyst will also be responsible for the documentation of criminal data described within this chapter.

II. PROCEDURES

A. Systems Manager:

1. Back-up the system on a weekly basis ensuring that all records are included. Make two copies of the back-up tape. One shall be stored with the system and the other in a remote location.

2. Perform software and hardware upgrades and repairs as necessary.

3. Devise and install such protective measures as are necessary to ensure that the systems is protected from unauthorized entry.

4. Control and maintain master passwords to all records and Personal Computers.

B. Systems Analyst: Perform the duties of A. above in the absence of the Systems Manager.

C. The back-up tapes shall be stored in a secure location.

D. The Systems Analyst will be responsible for analyzing crime, providing technical assistance to other units within the agency, conducting special studies (as the need arises), developing and suggesting plans to improve the law enforcement service in furthering the goals of the department, reviewing existing plans to determine their suitability, and analyzing all operational activities of the agency. This data will be compiled by completing the following tasks:

1. Stolen Vehicle "Hot" Sheet: This report will be compiled 3 times a week and distributed to CSD, ISD, and the 911 Center.

2. Missing Persons: This report will be compiled twice a week and distributed to UPD, CID, and the 911 Center.

3. Part I Crimes by Zone: This report will be compiled weekly and distributed to UPD and CID.

4. Five (5) Top Crash Areas and Five Top Causes: This report will be compiled on a monthly basis and forwarded to the UPD.

5. Five (5) Top Traffic Citation Areas: This report will be compiled on a monthly basis and forwarded to the UPD.

6. Officer Activity Reports: These reports will be compiled on a monthly basis and forwarded to the UPD.

7. Stolen Vehicle Reports by M.O. (modus operandi): These reports will be compiled on a weekly basis and forwarded to the CID.

8. Stolen Property Type: This report will be compiled on a weekly basis and forwarded to the CID and UPD.

9. Burglaries BY M.O. (modus operandi): These reports will be compiled on a weekly basis and forwarded to the CID.

10. Employee Activity Report: This report will be compiled on a monthly basis and forwarded to the ASD.

11. Citations by Age, Race, and Sex: This report will be compiled on a quarterly basis and forwarded to the Office of the Chief.

12. Crime activity Zone Totals Only (all crimes): This report will be compiled on a quarterly basis and forwarded to the Office of the Chief.

E. System Operators - all system operators will be provided passwords for their use in accessing the system by the System Manager. No password may be changed except with the knowledge and consent of the System Manager; this includes and independently operating Personal Computers.

F. Employee Owned Computers - All employee owned computers that are used on department property are subject to the rules and regulations of the department.

G. Expectation of Privacy - There is no expectation of privacy on department or employee owned computers that are operated on department property.

H. Internet Usage - Use of the Internet will be limited to those computers whose operators have an official need. The decision to grant Internet access will be made by the Chief of Police upon recommendation of the Division Head and the Systems Manager.

STANDARD OPERATING PROCEDURE

EFFECTIVE February 1, 2012

S.O.P. 14-8 RECORDS SAFETY DURING NATURAL OR MAN MADE DISASTER

I. INTRODUCTION

RECORDS SAFETY DURING A NATURAL AND/OR MAN MADE DISASTER

In the event of a natural or man-made disaster, the Watch Commander or Senior Officer on duty shall be responsible for ensuring that records maintained by the department are secured and not in danger of being damaged or destroyed.

II. PROCEDURES

A. In the event that department records are not secured or have been damaged and/or destroyed, the Watch commander or Senior Officer on duty shall make immediate notification to the affected division supervisor and advise them of the situation. If necessary, a police officer(s) shall be stationed in the area to secure said records until the affected supervisor(s) responds. Affected areas include Administrative Services Division, Uniform Patrol Division, Office of the Chief, Crime Prevention and Criminal Investigations Services Division.

B. The affected division supervisor shall be responsible for taking the necessary steps to ensure that all records are secured on site or that said records are removed to another location where they can be secured until such time that they can be returned and secured within the department.

STANDARD OPERATING PROCEDURE

EFFECTIVE February 1, 2012

S.O.P. 14-9 PROCEDURES FOR MAINTAINING AND REVIEWING DIGITAL COMMUNICATIONS RECORDING SYSTEM

A. All radio and telephone communications excluding cellular devices at the Lyons Police Department are recorded. This recording is achieved via a digital format through a secure computerized system. This system is to be maintained is to be maintained by the departmental System Expert/Office of Professional Standards. All calls are archived onto digital media for storage as needed depending on call volumes and durations. Once full, the media will be replaced and the archived data will be labeled and maintained in the Office of Professional Standards in a locked cabinet with restricted access.

B. Review of any archived data will be done through the Office of Professional Standards under the direct written order of the Chief of Police. This order is also known as a “Request for Recording System Data” which will be available on the department’s computer network.

C. In emergency situations, departmental personnel are authorized to retrieve emergency calls in which some part of the call was not clearly understood, but only for the purpose of safely responding to an emergency situation.

1. The emergency playback function is located at the communications console center and has a 30 minute window of function before the call receives archive status and will no longer be available without written approval through the Chief of Police.

2. At no time will an employee utilize the emergency playback feature to access the phone conversation of any other party for mere curiosity or amusement.

STANDARD OPERATING PROCEDURE

EFFECTIVE October 21, 2026

S.O.P. 14-9 **RECORDS RETENTION POLICY**

I. PURPOSE

To establish procedures for the maintenance, preservation, and destruction of Police Department records as required by the Georgia Records Act and state record retention schedules.

II. POLICY

All records created or received in the performance of a public duty or paid for by public funds by a governing body are deemed to be public property and shall constitute a record of public acts.

A "record" for purposes of this policy means all documents, papers, letters, maps, books (except books in formally organized libraries), microfilm, magnetic tape, or other material, regardless of physical form or characteristics, made or received pursuant to law or ordinance or in performance of functions by any agency. This definition includes those records created, used and maintained in electronic form, including e-mail, text messages, voicemail and online postings/communications.

It is the policy of the Lyons Police Department to maintain, preserve and dispose of its records in accordance with federal and state law and established records retention schedules. All Department personnel are expected to adhere to the retention requirements set forth herein. Any Police Department employee who fails to preserve Department records in accordance with this policy will be subject to disciplinary action, up to and including termination.

The records subject to this policy are those records that are specific to the Police Department. To the extent the Police Department generates records that are not included in the retention schedule contained in this policy, the Records Management Officer should contact the Georgia Archives for guidance on the appropriate retention period.

III. RECORDS MANAGEMENT

A. The Chief of Police, or his/her designee, will be the Records Management Officer for purposes of this policy.

B. The Records Management Officer will be responsible for creating and implementing a records management system that ensures all Departmental records are maintained in accordance with applicable retention schedules. The Records Management Officer will maintain a list of all Department generated documents and classify each according to the proper retention schedule.

C. Any record for which there is reason to believe litigation may be pending (e.g., complaint, grievance, EEOC Charge, ante-litem notice, lawsuit), shall not be destroyed, regardless of whether the retention period has concluded. Such records shall be placed on hold status until all litigation has concluded.

D. Paper records may be retained in electronic form for record retention purposes. After verifying that the record has been accurately scanned to an electronic format, the original may be destroyed. [NOTE: The destruction of originals can present a problem during litigation if the authenticity of a document cannot be proven. Therefore, if using an electronic storage method, the agency must maintain proper documentation of the record management process so that the agency can testify to the authenticity of the document if necessary (i.e., that the electronic record accurately reflects the original, without alteration). Agencies may wish to consider retaining original records until the matter is resolved.]

E. Records existing solely in electronic form are in danger of becoming inaccessible through media decay and hardware/software obsolescence. Therefore, the Records Management Officer will be responsible for the migration and transfer of electronic records to new hardware and software to ensure that the Department's records can be retrieved and viewed for the duration of the applicable retention period.

F. The Chief, or designee, will make every effort to protect the records against deterioration, mutilation, alteration, theft, loss or destruction and will keep them secure in a designated location. Only specifically authorized employees may remove any record from its assigned location.

G. The Records Management Officer will review applicable retention schedules every two years for any updates or changes to the retention schedules, beginning October 21, 2026, and will update the retention schedule accordingly.

IV. DESTRUCTION PROCEDURE

The following procedures shall govern the destruction of the Department's records:

A. When the specified retention period ends, records meeting the criteria shall be destroyed as soon as practical, except records for which there is reason to believe litigation may be pending which will be placed on hold until all litigation, including any appeals, have been concluded.

B. Before any departmental equipment is sanitized for redistribution or reassignment (e.g., the transfer of a terminated employee's computer to another employee), the Records Management Officer is responsible for ensuring that a forensic image of any hard drive for desktop and laptop computers issued to employee, City issued cell phone, and any other electronic device is made. The Records Management Officer will also be responsible for ensuring that an employee's email account is retained in accordance with applicable retention schedules.

C. The Records Management Officer will review the relevant retention schedule immediately before the destruction of any records to ensure no changes have been made to the retention period before destruction.

D. At the end of the retention period for any records, the records will be destroyed by shredding, controlled burning, or other method approved by the Chief of Police. The destruction of records will be witnessed by the Records Management Officer, and/or other person(s) designated by the Chief of Police.

E. Any records designated as confidential by law shall be so treated by Departmental personnel in the maintenance, storage, and disposition of such confidential records. These records shall be destroyed in such a manner that they cannot be read, interpreted, or reconstructed.

F. The records retention periods in this policy constitute legal authority for retention and disposal of Departmental records. No records shall be destroyed until they meet the minimum retention period listed in the Retention Schedule. In cases where there is no schedule for a particular record series, the Chief of Police must grant permission for the destruction.

G. The Records Management Officer will create and maintain a log of any records destroyed as part of this policy. The log should include the description and quantity of each record series disposed of, manner of destruction, inclusive dates covered, the date on which destruction was accomplished, and who was present to witness the destruction.

V. RECORDS RETENTION SCHEDULE

A. Georgia's record retention periods are determined by the content of the record, not by its format. Whether a record is on paper, in electronic form, or on microfilm, it must be retained for as long as the retention schedule specifies.

B. This schedule does not authorize destruction of records that could be deemed relevant to current or threatened litigation. Those records must be held until the matter is resolved if longer than the applicable retention period.

C. If a record is maintained in more than one location, the Department will retain the record for the longer retention period. For example, drug testing records should be retained for 2 years, but if they are also part of an employee's personnel/medical file, they should be maintained until 7 years after the employee's separation.

D. The department will comply with the following retention schedule.

1. Administration

Agency Publications (newsletters, handouts, brochures, etc.)	Permanent (1 copy)	LG-01-035
Annual Payroll Earnings Reports (summary of employees' payroll earnings/deductions)	50 years	LG-14-001
Annual Reports (reports describing agency functions/activities)	Permanent	LG-01-004
Building Security Surveillance	Retain until settlement of claims (Known Incident) 30 days (No Known Incident)	LG-19-079A, B

Destruction of agency records (documents reflecting the destruction of agency records)	7 years	LG-21-003
Emergency Management/Operations Reports	5 years	LG-19-032
Employee Issued Equipment (records documenting property in use by or in possession of an employee)	5 years or until return of item, whichever is longer	LG-18-034
Facility/Building Security Records (records documenting security measures and procedures)	5 years	LG-18-009
Federal Grant Funding (all related documents)	3 years after grant ends	2 C.F.R. § 200.333
Maintenance Records (Capital Equipment & Technology) (purchase orders, warranties, operating manuals, service contracts, and service logs for maintenance of agency-owned equipment and vehicles)	5 years after disposition of equipment	LG-18-007
Maintenance Schedules (agency-owned equipment and vehicles)	5 years	LG-18-017
Motor Pool Vehicle Records (records documenting reservation and use of motor pool vehicles by departmental personnel, gasoline use, mileage)	5 years	LG-18-019

Open Records Act Requests & Correspondence	3 years	LG-01-027
Policies and Procedures	Permanent (1 copy)	LG-01-032
Proof of Compliance with Georgia Law Enforcement Certification Program (certification standards, standards status reports, written directives, photographs, etc.)	2 years after confirmation of certification/recertification	LG-019-020
Property and Equipment Inventories (list of agency-owned property/equipment)	5 years	LG-18-021
Property Disposition Requests (Surplus Property Records)	5 years	LG-18-020
Property/Equipment Purchased with Federal Funds	3 years after disposition	2 C.F.R. § 200.333
Quarterly and other narrative reports (non-annual) (reports describing agency functions/activities)	3 years	LG-01-037
Restricted Area/Access Authorization Identification Records (records of issuance of security/access badges to employees)	5 years after separation	LG-18-024
Daily/Monthly Activity Reports (shift rosters/reports)	2 years	LG-01-016S
Special Event Records (parades, holiday events, etc.)	5 years after event	LG-01-040

Vehicle and Equipment Maintenance	5 years after sold or replaced	LG-18-029
Visitor Logs and Sign-In Sheets	2 years	LG-01-043

2. Recruitment/Hiring

Applications for Employment	2 years (Not Hired) 3 months (Incomplete/Unsolicited)	LG 16-003, 16-004
Background Investigations (Not Hired)		
• Background packet, polygraph testing materials, reference checks, physicals, etc.	5 years	LG-16-005
• Credit reports, GCIC/NCIC criminal history checks, driving records	Immediately after decision not to hire	0466-01-010
Job Recruitment Material (records documenting efforts to advertise positions and attract qualified personnel for employment opportunities, including internal/external/online vacancy announcements and advertisements)	2 years	LG-16-029
Position Classification Materials (job requirements, job description, salary range)	4 years after position is reclassified	LG-16-034
Pre-employment testing/assessments (Not hired) Includes proficiency, physical, and medical testing	2 years	LG-16-035

3. Personnel

Community Service Forms (documenting terms of work or work provided)	3 years after completion of service/project	LG-01-010
Complaints by and against Employees (all related documents) (internal complaints and grievances, and external complaints (EEOC Charge))	2 years or until case is resolved, whichever is later	LG-16-013
Disability Accommodations under the ADA (requests for accommodation, approvals, denials, documents reflecting accommodation provided)	1 year	29 C.F.R. § 1602.14
Drug Testing – Equipment Calibration	5 years	LG-16-011
Drug Testing Records (Employee)	5 years (Positive/Refusal) 2 years (all other testing related documents)	LG-16-010A, B
Employee Discipline/Adverse Action Logs	10 years	0466-01-004
Employee Identification Card Records	5 years after ID Card is recalled	LG-16-015
Family & Medical Leave (FMLA) (records relating to leave under the FMLA, medical certifications, dates/hours of leave taken, leave notices, benefits, premium payments, etc.)	3 years	29 C.F.R. § 825.500 (FMLA)
Intern/Volunteer Program Records	3 yearsafterseparation (individual files) 3 years (all other records)	LG-16-045A, B

Leave Donation Records	1 year after leave is used	LG-16-030
Leave Records (records of leave earned/taken)	3 years	LG-16-031
Off-Duty Employment Requests/Approval	Until employee separates from Department	0466-01-012
Payroll records (salary, wage, tax records)	4 years	LG-14-011, 14-014
Personnel Files (includes pre-employment documents, background checks, training, performance evaluations, discipline, etc.)	7 years after separation	LG-16-018
Officer Subpoena Logs	3 years after disposition	LG-19-081
Work schedules, time/attendance (records documenting employee's daily and weekly work schedules, including shift rosters)	4 years	LG-14-016

4. Patrol (General)

Accident Reports (government vehicle)	7 years	LG-01-001
Body Cam/Dash Cam/Drone Cam Video	30 months if part of a criminal investigation, shows a vehicle accident, shows arrestor detention of individual, shows use of force 180 days (all other)	LG-19-068A, B
Breath Test Reports	4 years (negative result) 5 years (positive result)	LG-19-016A, B
Criminal Trespass Notifications	Useful Life (as long as needed)	LG-19-028
Dead Animal Disposal	2 years	LG-19-029
Extradition Reports	5 years after closed	LG-19-034
False Alarm Reports	3 years	LG-19-035
Incident Reports (Criminal)	Capital offenses - 50 years Non-capital offenses – 5 years	LG-19-053
Incident Reports (Non-criminal)	1 year	LG-19-051
Juvenile Complaints (accusations of criminal conduct)	5 years or after adjudication, whichever is later	LG-19-063

License Plate Data	No more than 30 months, unless the data is the subject matter of a toll violation or for a law enforcement purpose	O.C.G.A. § 35-1-22
Radar/LIDAR Test Log	7 years	0466-04-005
Ride Along Waiver	2 years	0466-04-006
Roadblock Records	7 years	0466-04-021
Traffic Citation Log (list of parking/traffic citations, court dates, fines)	5 years	LG-19-083
Traffic Violations (citations, warnings, summonses)	2 years	LG-19-084
Vehicle Impound Reports	3 years	LG-19-048

5. Accident Reports

Accident/Injury Reports (workers' compensation claims, employee accidents)	4 years	LG-16-046
Accidents involving agency-owned vehicles	5 years	LG-18-027
Accidents Involving Hazardous Material	50 years	LG-19-002

Accidents on Private Property	1 year	LG-19-004
Toxic/Hazardous Substance Exposure (employee)	30 years after separation	LG-16-016
Traffic accidents or other accidents on public property	5 years	LG-19-003

6. Arrest/Booking

Civil Arrests (records of actions taken on orders for incarceration in civil cases)	3 years	LG-19-021
Executed Arrest Warrants	3 years after court appearance	LG-19-013A
Fingerprint Cards (paper)	Keep until entered into Fingerprint database or investigation file	LG-19-090
Fugitive/Wanted Person Files	5 years after apprehension	LG-19-045
Holding Cell/Booking Area Videos/Recordings	180 days	LG-19-047
Incarceration Log (daily list of inmates)	1 year	LG-19-050
Open Arrest Warrants (capital offense)	50 years	LG-19-103B
Open Arrest Warrants (non-capital offense)	15 years	LG-19-013C

Recalled Arrest Warrants	2 years	LG-19-012

7. Bond Records

Bond Receipts (records documenting the receipt and disbursement of cash bonds)	10 years	LG-19-018
Forfeited (records of remittance of forfeited bond)	3 years	LG-19-019
Records of bonds made on individuals for criminal offenses	5 years	LG-19-017

8. Investigations

Investigation Case Files	Capital offense -50 years after adjudication Non-capital felony – 7 years after adjudication Misdemeanor - 5 years after adjudication/2 years after investigation closes	LG-19-025, 19-026, 19-027
Complaint Log (complaint form, complaint log, receipt of complaint form)	2 years	0466-01-011
Consent to Search Forms	7 years	0466-05-009
Internal Affairs Investigations	50 years (Founded) 1 year after investigation is completed (Unfounded)	0466-05-017 0472-13-032A, B

	[***Recommend keeping unfounded investigations for at least 2 years***]	
Investigation Logs (listing of investigations)	3 years	LG-19-059
NCIC/GCIC Record Book (record of NCIC/GCIC usage)	5 years	0466-04-034
Pawn Tickets	4 years after creation	LG-19-069
Sex Offender Registration	7 years after registrant leaves jurisdiction	LG-19-080
Use of Force Investigations	7 years	0466-05-012

9. Evidence/Property

Asset Forfeitures	6 years	LG-0466-03-005
Condemned Vehicle Account Records (records documenting sale/release of impounded vehicles after condemnation)	3 years after condemnation	LG-19-022
Evidence Log	3 years after disposition	LG-19-033A
LED Sheets (GCIC form used to enter stolen property/vehicles into GCIC)	30 days	LG-19-088
Non-evidentiary Property Logs (found property, property stored for safekeeping)	1 year after disposition	LG-19-033B

10. Special Operations

Aviation records (flight logs, fuel and gas logs, maintenance records, Pilot's Flight Report)	7 years	0466-04-010
K-9 Records (health/training records)	4 years after dog leaves unit	LG-19-030
SWAT (records of SWAT activities, training, etc.)	7 years	0466-04-009

11. Training

Field Training (non-POST)	5 years	LG-19-089
Training Lessons	2 years	LG-19-091

12. 911/Communications Center

911 Emergency Call Recordings	3 years	LG-19-001
Emergency Dispatch Logs (radio calls)	3 years	LG-19-031, 19-074

13. Animal Control

Animal Intake Reports and Logs	2 years	LG-19-007

Animal Sterilization Citations and Records	1 year	LG-19-009
Case History records maintained on all animals received at an animal shelter	1 year	LG0-19-006
Records of Animal Bites	3 years	LG-19-075
Shelter Operation Records	1 year	LG-19-008

9. Weapons Transfer/Sale

Report of sale/disposition of pistols and revolvers (ATF form F3310.4)	1 year	LG-19-077
Weapons Sale/Transfer documents	1 year	LG-19-010

10. Crime Statistics

Annual Report	Permanent	LG-19-024A
Other Periodic Reports	5 years	LG-19-024B

11. Information Technology

Computer Inventory Records (computer assignments, inventory of software licensing, IP address/mailbox assigned to employee)	4 years after removal from service	LG-10-001

Equipment Records	Life of equipment	LG-10-004

S.O.P. 14-6 FLOCK SAFETY LPR

I. PURPOSE

To establish procedures for Lyons Police Department employees for the usage of the Flock Safety ALPR Camera System.

II. POLICY

The Lyons Police Department will use the Flock System for the identification of vehicles of interest, including stolen vehicles and others from the Georgia Crime Information Center (GCIC) and other local law enforcement hotlists. The data collected by the Flock System will also assist officers and investigators to confirm a suspect's alibi or location at a particular date and time during the investigation of a reported crime. All patrol officers will log into the Flock Safety ALPR system upon beginning their tour of duty, ensuring that the alert notification feature is activated for all alerts.

III. DEFINITIONS

A. Flock ALPR – Automated License Plate Recognition System sold and maintained by Flock Safety
B. Flock Operator: A sworn officer with the Lyons Police Department who has been properly authorized and trained to utilize the Flock System.
C. Flock Manager: The Administrative Services Captain is responsible for the management of the Flock program. This includes the programs administration, troubleshooting, and coordinating all aspects of the Flock System
D. Alert: An audible and/or visual signal activated upon the captured picture of a license plate that is associated with a Hotlist alert that has NOT BEEN VISUALLY VERIFIED by the officer against the photo in the Flock system
E. Tentative Hit: An alert by the Flock system that has been visually verified by the officer and photo but has not been validated by the officer or dispatch as a live query transaction or confirmed as valid with the original entering agency.
F. Live Query Transaction: A hit by the Flock system that has been validated as active but has not been confirmed as valid by the entering agency.
G. Confirmation (Confirmed Hit): A hit by the Flock system that has been confirmed as valid and active by the original entering agency through teletype via dispatch.
H. Reads: Are pictures that are captured but which did not produce a match or "hit" from the hotlist
I. Hotlist: Data files extracted from the law enforcement databases which contain a listing of stolen license plates, stolen vehicles, wanted persons, and other vehicles/persons actively being sought by a law enforcement agency such as Amber/Silver Alert vehicles/persons. These data extracts are generally facilitated at numerous times per day to provide current data.

VI. PROCEDURES

A. SYSTEM DESCRIPTION.

1. The Flock system takes a digital photograph of every vehicle's license plate and the immediate area surrounding the license plate, which enters its field of view.

2. This digital image is time stamped, and GPS coded. It then searches a hotlist to see if the license plate is wanted for any reason.

3. The Flock system does not conduct a live query against the source database. The system conducts a check of the hotlist database that is periodically downloaded throughout the day.

4. The system then searches the hotlist for the license plate detected.

5. The system downloads the hotlists on a regularly scheduled basis.

6. Every tentative hit by the Flock system must therefore be visually verified by the officer, and a live query transaction must be conducted when reasonably possible before any contact is initiated.

7. Every license plate picture is stored in the Flock database for 30 days. This data can be used by the agency in investigations, may be accessed only by trained users with a legitimate and permissible law enforcement purpose, and is classified "For Official Use Only" requiring a case number for any query into the historical data.

8. The Flock system can conduct various types of alerts that may include:
   - Warrant alerts
   - Missing person alerts
   - Stolen vehicles alerts
   - Stolen license plates alerts
   - Protection order alerts
   - Gang and terrorist watch list alerts
   - AMBER alerts
   - Sex offender alerts
   - Inmate release program

B. ADDITIONAL FEATURES OF THE SYSTEM

1. Searches: The Flock system allows for searches to be run through the database by full license plate number, partial license plate number, time frame, camera location, and geographical boundary. Personnel within the agency will be trained and authorized to conduct searches of the Flock database for legitimate and permissible law enforcement purposes. These searches require a case number or identifying information for future reference during an audit.

2. Flagged Hotlist Vehicles: Shift supervisors, Sergeants, Lieutenants, and Captains may enter the license plate of a vehicle of interest into the ALPR database for law enforcement purposes only. Along with identifying and contact information of the user, hot list entries will provide license plate information, vehicle description, what action to take if the vehicle license plate is scanned (such as stop and notify a specific officer/detective, do not stop/only monitor, etc.), and any other information related to the crime, investigation, or officer safety concerns.

Hot list entries should use an expiration date of no more than one month. When taking into consideration factors such as the type of crime and officer safety, there may be a need to hot list a vehicle for a longer period. If the determination is made by a supervisor that an entry should have an expiration of longer than a month or no expiration by the system, it is the responsibility of the user making the entry to verify its validity monthly.

If a vehicle on a hot list created by a user of this department is located by an officer and no longer needs to be included on the hot list, it is the responsibility of the locating officer to have the located vehicle removed from the hot list and notify the user that created the entry. The notification should include the Incident number that references the details of the stop. If the locating officer determines the removal of the hot listed vehicle should be further reviewed, that officer will contact the user that created the entry with information regarding that decision. If the user who entered the record is off-duty the on-duty supervisor shall remove the record.

When entering a new hotlist record the following information shall be provided at a minimum.

- Plate #
- Plate state of issue
- Case Number (entry documented in report)
- Reason field
    - Information supporting the alert entry.
    - Any cautions that would assist an officer receiving the alert
    - Contact information for Lyons PD or officer entering the alert.
    - Requested action (such as stop and field interview, notify a specific officer/detective, do not stop/only monitor, etc.).
    - Name of officer making the entry

Types of hotlist entries: The following types of entries, if made manually shall be set to an expiration of 24 hours due to automatic upload via GCIC.

- Stolen Vehicles
- Missing Persons*
- Wanted persons*
- Amber Alert*

Note, the above marked with an asterisk: these alerts shall only be set to expire within 24 hours if the entering officer can verify that the license plate has or will be entered into GCIC with the originating record.

3. Unless the officer has independent probable cause to make a stop, the officer shall not make any contact with the subject vehicle until the alert is verified as active through a live query.

4. If the officer witnesses a violation of law or other action that establishes justification for a stop, the officer may conduct a stop based on the observed justification.

5. Upon receiving a Flock alert, the officer shall perform a visual verification that the license plate image captured by the system exactly matches the license plate characters and issuing state. The officer will also verify that this information exactly matches the alert information provided on screen as retrieved from the current hotlist.

6. The officer shall utilize a GCIC request on this license plate to verify that the information that produced the tentative alert is correct and active. This live query transaction may be accomplished via dispatch or using the live query software on the officer's laptop computer.

7. Upon confirmation that the license plate information is active in a live query transaction the officer may initiate appropriate law enforcement action as determined by the information available from the source database. As soon as practical, the officer shall confirm the teletype entry status with the original entering agency.

8. Be On the Look-Out (BOLO) situation refers to a determination by a law enforcement agency there is a legitimate and specific law enforcement reason to identify or locate a particular vehicle, or, in the case of a post-scan BOLO, there is a legitimate and specific reason to ascertain the past location(s) of a particular vehicle. Examples of legitimate and specific reasons include, but are not limited to, persons who are subject to an outstanding arrest warrant, missing adults and/or juveniles, stolen vehicles, vehicles which are reasonably believed to be involved in the commission of a felony, vehicles with expired or suspended license plate registrations, convicted sex offenders, or persons on any watch list issued by a State of Federal agency responsible for homeland security.

9. When an officer receives an alert, the officer shall take such action in response to the alert as is appropriate in the circumstance. An officer alerted to the fact an observed motor vehicle's license plate is on the BOLO list is required to have reasonable suspicion before the officer would have a lawful basis to stop the vehicle. An officer reacting to an immediate alert shall consult the database to determine the reason why the vehicle has been placed on the BOLO list and whether the alert has been designated as a non-encounter alert. In the event of a non-encounter alert, the officer shall follow any instructions included in the alert for notifying the law enforcement or homeland security agency which entered the BOLO.

10. Officers are strictly prohibited from accessing, logging into, or interacting with the Flock Safety platform using personal mobile phones, personal tablets, or any personal electronic devices. Personal devices may get text messages or emails from Flock concerning alerts. The alerts will only be accessed on department devices.

11. Requests from other law enforcement agencies must include the agency name, a valid case number from that agency, and the requesting officer's name. Requests from other law enforcement agencies will be handled by shift supervisors and above.

3. Use of the Department's Automated License Plate Reader (ALPR) System

1. Personnel shall exercise due care and caution when utilizing the ALPR system and while operating a vehicle.

2. An ALPR may be used in conjunction with any routine patrol operation or criminal investigation. Reasonable suspicion or probable cause is not required prior to using an ALPR or accessing ALPR data.

3. Partial license plates and unique vehicle descriptions reported during major crimes shall be entered into the ALPR system in an attempt to identify suspect vehicles.

4. A valid reason and case number shall always be provided when conducting a search or query within the ALPR system.

5. Automated License Plate Reader (ALPR) Alerts/Hits
Prior to the initiation of a traffic stop based on an ALPR alert or hit, the officer must:

a. Visually verify that the vehicle plate of interest matches the image of the l license plate captured by the ALPR system, including alphanumeric characters, state of issuance, and vehicle descriptors.

b. Verify the current status of the license plate via a Live Query through the E911/ Communications Center dispatcher or the Mobile Communications Terminal (MCT), when circumstances allow.

c. In be on the lookout (BOLO) situations, officers shall make reasonable efforts to verify that the driver and/or occupants physically match the description of any person(s) listed on the hit.

d. If an ALPR alert cannot be confirmed, the alert will be rejected.

6. The provisions shall not prevent an officer from taking immediate action when a verifiable emergency situation exists for the sake of officer safety.

7. All ALPR data used in conjunction with an open, ongoing law enforcement investigation shall be considered evidence and must be properly documented and preserved.

4. Use of Automated License Plate Reader (ALPR) System for Administrative Investigations

1. ALPR data may be accessed and used during internal investigations.

2. Prior approval from the Chief of Police is required before accessing any ALPR data for administrative investigations.

3. All requests to use ALPR data during an internal investigation shall be made in writing and shall contain the following:

a. Identify the employee under investigation.
b. State the specific administrative purpose or allegation.
c. Define the scope and timeframe of the requested data.

5. Disciplinary Action

1. Any Employee who intentionally or negligently misuses the ALPR system in violation of this procedure may be subject to disciplinary action, up to and including termination.

2. Employees who knowingly requests, uses, obtains or attempts to obtain ALPR data for any purpose other than a law enforcement purpose may be subject to criminal action.

C. MAINTENANCE

1. Maintenance and all repairs of the Flock equipment will be coordinated by the Flock manager.
2. It is the responsibility of the Flock operator to notify their immediate supervisor and the Flock Manager of any damage, repairs or issues that arise with the equipment.
3. Flock operators shall not attempt to modify, adjust, or repair the Flock system equipment or software.

D. DATABASE ACCESS

1. The Flock database resides on a secure server that is operated by the private vendor, Flock Safety. The data remains property of the Lyons Police Department and is managed according to the agency's data sharing and retention policies. The data is not used in any way by Flock Safety who provides hosting of the data and access to their software as a service. This database houses the current hotlists as well as the license plate pictures that are uploaded from the camera systems. The images are of the area immediately surrounding the license plate, a close-up view of the license plate, as well as the location and date/time of the picture. These images are sorted by the software as either reads or hits. Hits refer to images that have generated a possible match with one of the active hotlists at the time of the picture. Reads are images that are captured but which did not produce a match or "hit" from the hotlist.

2. The collected Flock data contains no Personally Identifiable Information (PII) that may be used to connect a license plate detection to an individual. It is only with permissible purpose that an investigator/officer may make this connection (using other systems) and this access is governed by the Federal Driver's Privacy Protection Act (DPPA).

3. All investigative queries into collected Flock data are logged by user and case number and are available for auditing and review by the agency. Any perceived policy violation or other misuse of the system will result in appropriate disciplinary action including possible termination and legal action.

4. The database may be accessed for law enforcement purposes only. Users are prohibited from conducting any searches of Flock data for non-law enforcement purposes. Users are prohibited from disseminating the information to anyone outside of law enforcement. User accounts are only for employed Lyons Police Department employees. Department employees are not to give their user account information to anyone. Information gathered, collected, or retained by Flock Safety cameras or any other ALPR system shall not be sold, accessed, or used for any purpose other than legitimate law enforcement or public safety objectives.

5. A valid case number shall always be provided when conducting a search of the Flock database or identifying information to help in future audits.

6.The search feature within the database is only enabled for personnel that have been properly trained on the investigative tool and use for only law enforcement purposes.

E. RECORDS RETENTION- Reads and hits will remain in the system for 30 days.

F. ACCOUNTABILITY

1. Agency user audit reports will be produced and inspected quarterly to ensure compliance with this policy. This audit will be conducted by the CID Captain and the Patrol Captain and submitted to the Administrative Captain for review.

2. CID and Patrol Captains shall also conduct random monthly audits of the Flock use of their subordinates, any misuse shall be immediately reported to the Administrative Captain. Any problems or misuse will be reported to the Chief of Police.

3. Any department member found to be in non-compliance with this policy in their use of the Flock system will immediately have their access suspended to the system (if an authorized user) and be subject to appropriate disciplinary or administrative actions. Misuse of the system may constitute a criminal offense under O.C.G.A. § 35-1-22 or O.C.G.A. 16-9-90, the Georgia Computer Systems Protection Act. The act provides for the protection of public and private sector computer systems, including communications links to such computer systems. The Act establishes four major felonious criminal offenses, for violations of the Act: Computer Theft, Computer Trespass, Computer Invasion of Privacy and Computer Forgery. The criminal penalty for each offense carries maximum sentences of fifteen (15) years in prison and/or fines up to $50,000.00, as well as possible civil ramifications.

4. Any non-Departmental personnel found to have gained unauthorized access will be referred to the appropriate authorities for criminal prosecution, as necessary. External law enforcement personnel will not be allowed access to the Agency’s account.

5. Any employee who becomes aware of any misuse of the Flock software by another employee shall immediately report it to their supervisor, Sergeant, Lieutenant, or Captain.

6. Flock and the data generated by Flock shall only be used for official and legitimate law enforcement purposes.

7. Neither the Flock equipment nor software will be modified without authorization.

G. FLOCK SAFETY AGREEMENT

1. Any modifications to the services included in the agreement with Flock Safety beyond the scope of LPR systems shall first have the approval of the City Council and City Manager.

2. Any modifications to the set 30-day retention policy shall be approved by the City Manager and City Council.

3. At no time will the agency or city agree to the selling or release of city LPR data to the commercial sector in accordance with O.C.G.A. § 35-1-22.

H. TRAINING-

1. All new hires will receive training on the system using Flock Academy. Training will be documented within the respective Daily Observation Report. Officers will take the Law Enforcement User Training Session at the beginning of the FTO program. The Certificate shall be placed in the FTO folder.

2. Officers using the ALPR system for searches or creation of hot lists, shall complete the Flock search tool and Alerts certification courses at the beginning of the FTO program. FTOs will check off verifying the new hire has completed required Flock Academy Training by placing the certificate in the FTO folder.