DUBLIN POLICE DEPARTMENT

**STANDARD OPERATING PROCEDURE**

**SECTION: C-002 CRIMINAL JUSTICE INFORMATION SYSTEM / GEORGIA CRIME**

 **INFORMATION CENTER**

**EFFECTIVE DATE: 31 JUL 2000 NUMBER OF PAGES: 17**

**REVISED DATE: 16 JUN 2021 DISTRIBUTION AUTHORIZATION:**

#### STANDARD COVERED *CHIEF KEITH MOON*

**N/A**

1. **PURPOSE**

This policy provides an overview of regulations and policies that govern and regulate the use of the Georgia Criminal Justice Information System network. The purpose of these procedures is to establish guidelines to ensure the security, privacy, accuracy, and completeness of access to and dissemination of adult and juvenile record information, driver license information, and tag/vehicle registration information; proper entry, maintenance, and removal of all wanted/missing person and property records; and to ensure the accuracy, timeliness, and completeness of all related records maintained by the department and its employees.

1. **POLICY**

The Criminal Justice Information System is an integral part of law enforcement. The Dublin Police Department participates in and has access to the state and federal criminal justice information system network. Recognizing this, the department and all employees will follow all CJIS, GCIC, and NCIC policies, procedures, rules, and regulations. These include, but are not limited to, the CJIS Network Policy Manual, GCIC Operations Manual, GCIC Rules of Council, and the NCIC Code Manual and related federal rules/policies.

1. **SCOPE**

This policy applies to all sworn and non-sworn personnel of the department, volunteers, visitors, vendors, contractors, and any others who have access to Criminal Justice Information Systems or areas that contain such information.

1. **SANCTIONS**

Agencies are subject to GCIC administrative sanctions for violation of the laws governing the operations of the CJIS network, of the GCIC Council Rules, GCIC CJIS Security Policy, or of CJIS network policies published by GCIC.

Sanctions for CJIS network terminal agencies may include, but are not limited to: purging of Hot File records entered into GCIC/NCIC files, restricting CJIS network access, and suspension/revocation of the agencies’ terminal access to the CJIS network.

Administrative sanctions may be imposed on individual violators. Such sanctions may include but are not limited to, mandatory retraining and/or recertification of TACs, terminal operators, or practitioners.

Individual violators are also subject to criminal prosecution when their actions constitute violations of applicable state or federal law.

1. **DEFINITIONS**

**Criminal Justice Information System (CJIS) Network**: network comprised of four major components, including (1) devices and associated equipment operated by Georgia criminal justice agencies; (2) records and files accessed through those devices; (3) computers and associated equipment used by GCIC and local or regional computer centers that are connected to the Georgia CJIS network; and (4) federal, state, local criminal justice and other authorized agency employees who operate, support, use and benefit from the CJIS network.

**Georgia Crime Information Center (GCIC)**: a division of the Georgia Bureau of Investigation that manages the Georgia CJIS network under the provisions of Georgia law and various state and federal entities. The GCIC operates the network on a continuous basis and provides procedures, standards, and training necessary for the uniform operation of the network. The GCIC also establishes complete control over the network, restricts its use to criminal justice and other authorized agencies, and restricts the use of criminal justice information obtained through the network for purposes authorized by law.

**National Crime Information Center (NCIC)**: United States’ central database for tracking crime-related information, maintained by the Federal Bureau of Investigation’s Criminal Justice Information Services Division. NCIC is interlinked with GCIC (and other state systems).

**Terminal Operator**: department employee whose primary job function includes accessing the CJIS network. Includes any employee who accesses CJIS. This employee is also identified as a CJIS operator in this policy.

**Terminal Agency Coordinator (TAC)aka Secondary TAC**: a terminal operator who is certified by the state in CJIS matters and is assigned by the department to oversee terminal operators and serve as a liaison between the department and the GCIC for CJIS network-related matters.

**Primary Terminal Agency Coordinator**: individual assigned by the Chief of Police to manage and oversee all CJIS operations, and serve as a primary liaison between the department and the GCIC for CJIS network-related matters.

# AUTHORIZED PERSONNEL

A. Only authorized personnel are allowed access to the CJIS – GCIC/NCIC databases through specified department terminals that access GCIC and NCIC files and records. CJIS information is protected by law and shall be accessed by or disseminated to those who are authorized to access or receive said information in accordance with department policy, state law, and/or by rules, regulations, and policies of the GCIC/NCIC.

B. Authorized employees must successfully complete CJIS training as specified by current GCIC rules prior to accessing the CJIS system; they must also be recertified in accordance with GCIC rules and regulations as specified by GCIC rules.

C. All employees must receive a minimum of four hours of training on the Security and Integrity of Criminal History Record Information (CHRI) and GCIC Rules and Regulations prior to having access to a CJIS system; this training and recertification will be conducted in accordance with GCIC rules.

D. No employee of the department shall access GCIC information when not on duty. Access to GCIC when working off-duty employment shall be addressed on a per-case basis and shall only be allowed after receiving written permission from the chief of police or his designee.

1. **RESPONSIBILITIES AND PROCEDURES**

A. All supervisors will ensure that security measures are followed to provide maximum security for CHRI and CJIS databases, records, and files. Unauthorized personnel and/or individuals will not be allowed to frequent areas where such information is maintained, stored, collected, or processed. When an authorized employee accesses a CJIS terminal, the employee must log on and off the CJIS system using their assigned ID and password. If an employee must leave his/her computer unattended while accessing the CJIS system, the employee must log off the CJIS system prior to leaving the computer terminal. Leaving the system includes, but is not limited to, work breaks and shift changes. If a computer is accessible by multiple users, each user must follow the above procedure.

B. The Chief of Police is responsible for the department’s compliance with laws, policies, and operational procedures regulating access to the CJIS network. The Chief has the overall responsibility to ensure that:

1. A TAC is appointed and certified within 90 days of appointment.
2. Replacement TACs *must* be appointed immediately **and certified within 90 days**.
3. Agreements required by GCIC are current and signed.
4. All department employees *must* sign current Awareness Statements.
5. All department employees adhere to all GCIC/NCIC policies.
6. Establishment of department CJIS/GCIC policy based on all applicable laws/regulations.
7. All department employees who utilize any component of the Georgia CJIS network are
8. appropriately trained and that appropriate training documentation is maintained by the agency.
9. A Local Agency Security Officer (LASO) is appointed to serve as the department’s point of
10. contact for computer security responsibilities.

C. Primary TACs are to work on day shifts from 0800am to 1700pm. Secondary TAC is to work on night shifts from 1600pm to 0000am unless Primary TAC is out on leave and/or vacation.

D. Secondary TAC *must* successfully complete the Terminal Agency Coordinator Certification course, administered by the Georgia Crime Information Center, within **90 days** of their appointment. The Secondary TAC will assist the Primary TAC and Chief in managing CJIS network-related operations to ensure compliance with relevant laws, regulations, and policies. In the absence of the Primary TAC or the direction of, the Secondary TAC is required to:

1. At a minimum, successfully complete the Inquiry level of the GCIC Computerized Based Training (CBT) Terminal Operator Training Program before they are accepted into the TAC Certification course.
2. Administer the GCIC Terminal Operator Training Program within the department, and provide appropriate GCIC/NCIC-related training for all other agency employees. Maintains documentation verifying all CJIS-related training for the agency.
3. Assist the Chief in developing policies and procedures for all CJIS network operations.
4. Ensure those terminal operators responsible for *HIT confirmations* have immediate access to documentation supporting the agency's active hot-file records.
5. Maintain access to CJIS network-related documents such as:
	1. GCIC Council Rules, GCIC CJIS Security Policy, GCIC Policy Manual, GCIC Operating Manual, NCIC Operating Manual, NCIC Code Manual, Operations Bulletins, updates and revisions, and broadcast messages related to the operation of the CJIS network.
	2. Copies of current agreements (as required).
6. Other responsibilities as designated by GCIC Council and GCIC CJIS Security Policy.

E. The Secondary TAC *must* successfully complete the Terminal Agency Coordinator Certification course, administered by the Georgia Crime Information Center, within **90 days** of their appointment. In the absence of Primary TAC or the direction of, the Secondary TAC will assist the Chief in managing CJIS network-related operations to ensure compliance with relevant laws, regulations, and policies. In the absence of the Primary TAC or the direction of, the Secondary TAC is required to:

1. At a minimum, successfully complete the Inquiry level of the GCIC Computerized Based Training (CBT) Terminal Operator Training Program before they are accepted into the TAC
	1. Certification course.
2. Administer the GCIC Terminal Operator Training Program within the department, and provide appropriate GCIC/NCIC-related training for all other agency employees. Maintains documentation verifying all CJIS-related training for the agency.
3. Assist the Chief in developing policies and procedures for all CJIS network operations.
4. Ensure those terminal operators responsible for *HIT confirmations* have immediate access to documentation supporting the agency's active hot-file records.
5. Notify the GCIC Assistant Deputy Director for Security Operations when a new Chief of Police is appointed and arrange for the signing of new agreements.
6. Serve as the point of contact for validations and all other GCIC/NCIC network-related matters.
7. Maintain access to CJIS network-related documents such as:
	1. GCIC Council Rules, GCIC CJIS Security Policy, GCIC Policy Manual, GCIC Operating Manual, NCIC Operating Manual, NCIC Code Manual, Operations Bulletins, updates and revisions, and broadcast messages related to the operation of the CJIS network.
	2. Copies of current agreements (as required).
8. Maintain User IDs and passwords for department personnel who access the CJIS network.
9. Monthly completeness of GCIC/NCIC record validations to ensure that records are valid, complete, accurate, current, and active. Validation reports are to be completed accurately and in a timely manner.
10. Ensure that CHRI logs are properly maintained by department personnel.
11. Ensure that all department personnel review and sign a current awareness statement and that these forms are maintained in the employee's personnel file.
12. Ensure that volunteers, community service workers, and other non-employee individuals who frequent areas where CHRI is processed and/or maintained are given instructions regarding the confidentiality of department records. Such individuals are to review and sign a current awareness statement and forms shall be maintained on file by the Primary TAC.
13. Receive training, testing, and certification as mandated by GCIC.
14. The administration of terminal operator training, certification/recertification testing, and the reporting to GCIC the certification/re-certification status of all terminal operators employed by the Dublin Police Department.
15. Other responsibilities as designated by GCIC Council and GCIC CJIS Security Policy.

F. Terminal Operators must successfully complete CJIS training, are responsible for accessing the CJIS network, and are responsible for the security of CJIS information.

G. Mobile Data Terminal (MDT) Operators are considered Terminal Operators; they must successfully complete CJIS training, are responsible for accessing the CJIS network, and are responsible for the security of CJIS information.

H. In the absence of or the direction of Primary TAC, the Secondary TAC shall ensure that:

1. All inquiries of the CJIS files are processed in accordance with department policy and procedures, state and federal laws, and GCIC/NCIC rules and regulations.
2. Adult and juvenile arrest records will be collected, retained, disseminated, and disposed of in accordance with department policy and state law.
3. When a report is taken by an officer that contains information with identifiable descriptors and said information is required by policy to be reported to NCIC, a copy of the officer's incident report containing said information, and other required documentation, will be forwarded to the CJIS operator, 7 days a week, 0800 to 2400 hours.
4. All reports with identifiable descriptors and said information is required by policy to be reported to NCIC are forwarded to the E911 Center when the CJIS operator is absent (2400 to 0800, seven days a week). Missing juveniles and missing persons under 21 years of age will be forwarded immediately for entry when all required information has been collected. All other records must be forwarded for entry as soon as practical but within 12 hours or prior to leaving their tour of duty.
5. All reports, and other required documentation, shall be reviewed for accuracy and completeness by the supervisor prior to being forwarded to the CJIS operator or E911 personnel.
6. All reports entered into the computer that require removal shall be removed in accordance with state law and GCIC/NCIC rules and regulations. They shall be removed in a timely manner as outlined in the CJIS Network Operations Manual by the CJIS operator or E911 personnel.
7. When an existing record is to be cleared, canceled, or modified, all information needed (incident report, supplemental report, etc.) will be forwarded to the CJIS operator or E911 personnel in a timely manner. Supervisors will ensure that all information is complete and accurate.
8. Officers who receive and process criminal history, driver history, tag, and VIN information will destroy said information in accordance with department policy, state law, and rules of GCIC/NCIC.
9. Supervisors and officers will not provide criminal history, driver history, tag, or VIN information to any individual, citizen, business, or other non-law enforcement party. Individuals, businesses, and other non-law enforcement personnel requesting such information shall be referred to the CJIS operator for inquiry, processing, and dissemination of criminal history, tag, and VIN information. All driver history inquiries shall be referred to the Department of Driver Services.
10. Personnel under their supervision are aware of the laws, rules, and regulations governing criminal history information, and those personnel under their supervision are aware of penalties for illegally disseminating criminal history information.
11. Personnel under their supervision are aware of the Georgia Computer Systems Protection Act and the penalties that apply to violations of this law.
12. Personnel under their supervision have reviewed, understood, and signed a current GCIC awareness statement form. All signed forms shall be forwarded to and maintained in the employee’s personnel file.
13. Personnel under their supervision have successfully completed a Terminal Operator workbook and Security and Integrity training prior to being allowed to access CJIS systems.

G. Terminal/CJIS Operators shall ensure that:

1. Ensure that inquiries of GCIC/NCIC files are processed and maintained in accordance with state and federal laws, GCIC/NCIC rules, regulations, and policy and department policy.
2. Ensure that only authorized personnel utilize their assigned CJIS terminal during working hours.
3. Ensure that terminal usage and messages are transferred to the E911 Center by Integrated CJIS Data Center (ICDC) operations at 2400 hours.
4. Will log off the system when being relieved by another employee, at which time the relieving

employee will log into the system using their Operator ID and Password.

1. Ensure that all wanted/missing person files, property files, and other files are maintained and stored in accordance with state and federal laws, GCIC/NCIC rules and regulations, and department policy.
2. Enter, modify, clear, and cancel all wanted and missing person files and property files 7 days a week, 0800 – 2400 hours. Personnel from the E911 Center shall be responsible for making the appropriate entries, modifications, clearances, and cancellations when the CJIS operator is absent. Missing juvenile records will be entered immediately. All other records must be entered within 12 hours.
3. Missing Juvenile: Based on the National Center for Missing and Exploited Children (NCMEC) and the Federal Amber Alert Law missing persons who are 21 years of age or less are required by federal, state, and local law to be entered into NCIC immediately upon receipt of a report.
4. Within 24 hours, excluding weekends and holidays, after original entry, the GCIC Technician will verify the record and secure additional information if necessary and if available. If additional information is required during a weekend or holiday period, the on-call detective will be called in to perform this function and forward the additional information to 911 Center personnel for modification of the record. Within 60 days of entry of a missing juvenile, the lead investigator on the case must attempt to update the record with any available additional information, specifically medical and dental records for identification purposes.
5. Maintain a log of all transactions for driver and criminal histories and III files. Logs shall include but not be limited to the date of the request; type of request; name, date of birth, race, sex, and social security number of person being inquired upon; agency and person making the request; the operator accessing the computer for the information; purpose for the request; departmental case number, traffic citation number or other number related to the request, Agency Reference Number (ARN), SID or FBI number if one is assigned and any other miscellaneous number associated with the request. If there is no identifiable number available, the CJIS operator will assign an Agency Reference Number (ARN) to the requested inquiry. The CJIS operator shall maintain a log of all ARN numbers used. The ARN is a sequential list of numbers that are maintained in a separate database and used when no other reference number is available.
6. Ensure that all criminal and driver history logs are maintained and stored in accordance with department policy, state and federal laws, and GCIC/NCIC rules and regulations.
7. Requests for driver histories shall be made in person by on-duty personnel only. No requests shall be made via phone except by an on-duty officer in the field who must have the information immediately for work-related purposes. The employee receiving the request for an inquiry will verify the identity of the caller prior to processing the request. All requests will be logged and maintained in accordance with department policy.
8. Requests for a tag, VIN, and driver's license information will be made in person and by on-duty personnel only. Requests shall be made only when an officer/employee cannot access the information through their computer system. All requested information will be logged by the Operator processing the request. Requests by off-duty personnel will not be honored.
9. Ensure that only authorized personnel are allowed to review files containing criminal, driver history, tag/VIN, and driver license information.
10. Ensure that all computer printouts containing criminal history information, driver's license or history information, tag/VIN information, or other law enforcement-related information are destroyed by shredding when no longer needed. Only department employees are authorized to destroy said files. At no time shall community service personnel, trustees, volunteers, or any other non-employed person destroy said files.
11. Prior to making any GCIC/NCIC file entry, the CJIS operator will first transmit a wanted inquiry on the person or item. For wanted or missing person entries, the CJIS operator will run a driver's license and a criminal history inquiry. They will check with investigators to determine if the information is accurate or needs updating, check the original warrant to ensure it is still valid, contact the district attorney's office to ensure extradition if a warrant is served, and check other sources of information known to provide possible additional information; such as utility companies, county tag office, city directory, county jail, etc. For property files, the CJIS operator will check case files to determine if the information is accurate, complete, and current and contact the investigator (and owner if possible) to verify the item is still missing and secure additional information if available.
12. Ensure that all entries are reviewed for completeness and accuracy by another CJIS operator.
13. Report unresolved problems to the Primary TAC**,** GCIC, or NCIC.
14. Ensure that all warrants issued by municipal/magistrate court are completed in a timely manner with current and accurate information; and that all warrants are processed, maintained, and stored in accordance with state and federal laws, NCIC rules and regulations, and department policies.
15. Prior to making an NCIC file entry, the CJIS operator shall transmit and inquire on the wanted person’s, driver’s license/history and criminal history files.
16. The CJIS operator will check with investigators and/or other sources**;** such as utility companies, county tag office, city directory, county jail, etc. to determine if additional information is available.
17. Entering, modifying, clearing, and canceling all wanted/warrant files 7 days a week, 0800-2000 hours daily. Personnel from the E911 center shall be responsible for making the appropriate clearances and cancellations during non-business hours.
18. Ensure that another CJIS operator reviews all entries for completeness and accuracy.
19. Reporting unresolved problems to the Primary TAC, GCIC, or NCIC.

H. Records Supervisors shall ensure that:

1. Access to the department's designated records holding areas where criminal history record information is collected, stored, processed, and disseminated shall be limited to authorized persons only. Authorized personnel are determined by the Chief of Police.
2. All arrest records shall be collected, stored, processed, and disseminated with accuracy and completeness. All arrest information will be retained for the specified length of time as designated by state law.
3. All department reports, criminal and driver history, driver's license, and tag/VIN information that is to be destroyed is destroyed by shredding. Only department employees are authorized to destroy said files. At no time shall community service personnel, trustees, volunteers or any other non-employed person destroy said files.
4. All employees who access the CJIS database files have received training in Security and Integrity (S&I), have successfully completed CJIS training, and receive S&I training every 2 years.
5. All employees have read, understood, and signed a current GCIC awareness statement form. Completed forms shall be maintained in the employee’s personnel file.
6. Ensure that only authorized personnel utilize the CJIS terminal during working hours.
7. Ensure that all computer printouts containing criminal history information, driver's license or history information, tag/VIN information, or other law enforcement-related information is destroyed when no longer needed by shredding. Only department employees are authorized to destroy said files. At no time shall community service personnel, trustees, volunteers or any other non-employed person destroy said files.
8. **NATURAL AND/OR MAN-MADE DISASTERS**

A. In the event of a natural or man-made disaster, the Senior Shift Supervisor or Incident Commander shall have the responsibility of ensuring that areas, where records are maintained by the department, are secure and that department records are not in danger of being damaged or destroyed.

B. In the event that an area has been identified as being unsecured and department records may be or have been damaged and/or destroyed, the Senior Shift Supervisor or Incident Commander shall make immediate notification to the affected department/section supervisor and advise them of the situation. A police officer(s) shall be stationed in the area(s) to secure the unsecured areas and/or records until the appropriate supervisor responds and assumes control of the affected area and records. Affected areas include record-holding areas, municipal court, property/evidence, CID, ACE, Operations, and the offices of the Chief and Assistant Chief.

C. The affected supervisor shall be responsible for taking immediate necessary steps to ensure that the affected area(s) and all records are secured on site. If the affected area is unsecurable, the records and files affected shall be removed to another location where they can be secured until such time that the records and files can be returned and secured within the department.

# DISSEMINATION OF CRIMINAL / DRIVER HISTORY INFORMATION, DRIVER

#  LICENSE, AND TAG / VEHICLE REGISTRATION INFORMATION

1. All criminal history, driver history, and tag/vehicle registration information shall be disseminated in accordance with department policy, state law, and GCIC/NCIC rules and regulations. Terminals that access CJIS files shall be located in a secure area, out of view of unauthorized personnel or the public, and in an area restricted to authorized personnel only. Files shall be stored in locked file cabinets when not in use.
2. Only authorized personnel shall access the CJIS system and make inquiries. Officers not certified as CJIS operators will not directly access criminal history information from a CJIS system but will request the information through the CJIS operator on duty when it is necessary to access CCH files for work-related purposes. All records accessed shall be documented in accordance with department policy. **All documentation must be placed in a case file or destroyed in accordance with agency policy, and shall not be left out in plain view nor thrown into the trash can.**

C. Criminal History and Driver History Access and Dissemination:

* 1. Only authorized personnel shall make inquiries and receive Criminal or Driver History Record Information and only when it is job-related and in accordance with department policy, GCIC/NCIC rules and regulations, and state and federal laws.
	2. Authorized persons who make inquiries into driver and/or criminal history files will log the inquiry in the GCIC CHRI logbook located at each CJIS terminal.
	3. All logs shall include but not be limited to the date of the inquiry; type of request; name, date of birth, race, sex, and social security number of the person being inquired upon; the agency and person making the request; the operator accessing the information and the purpose of the request (C, J, P, E**,** W, N, M**,** Z or F) when inquiring in criminal history files; the department case number, ticket number**,** Agency Reference Number (ARN) or other number related to the request; and the SID or FBI number if one is assigned.
	4. All logs shall be maintained for a period of four years. These logs shall be maintained in a locked file cabinet in the office where the CJIS files are located.
1. Logs shall be inspected periodically by a TAC or the Primary TAC.
2. Driver history and/or criminal history information received but not maintained or disseminated shall be shredded. Only department employees are authorized to destroy criminal history and driver history records.
3. When a request is made for the criminal history of an individual and a signed consent form is received, a copy of the consent form shall be kept on file for a period of one year. Consent forms shall be destroyed by shredding.
4. When officers, supervisors, detectives, or other personnel receive driver history or criminal history information, the information shall be placed in a file maintained by the employee or in a case file. Employees will destroy all information not used by shredding said information.
5. At no time shall criminal or driver history information be left lying around on tables or other objects, left in department vehicles, thrown in the trash can, or given to unauthorized persons or businesses.
6. Violations of said policy and/or state law may result in disciplinary action and/or criminal prosecution.

D. Information may be disseminated to individuals as designated by state law as follows:

1. To other criminal justice agencies for the administration of criminal justice, disseminate all CHRI including first offender complete information to the requester, Purpose Code C, no requirement of consent form or fingerprints.
2. To the Federal Bureau of Investigation, Defense Investigative Service, U.S. State Department, Central Intelligence Agency, and Office of Personnel Management for national security purposes only, without a signed notarized consent form or fingerprints of the person being checked for security clearance and persons being considered for employment in sensitive national security jobs, disseminate all CHRI using Purpose Code E**.**
3. For all inquiries for the purposes of issuance of a pistol permit; refer all requests to the county probate office.
4. This agency prohibits the commercial dissemination of HOT file information.

E. Requests by Firefighter Applicants:

1. All requests shall be made by submitting a signed consent form for a Criminal History and a Driver History.
2. All CHRI except first offender complete information shall be forwarded to the Personnel Director. The CJIS operator shall make local and state CHRI inquiries for the Personnel Office using Purpose Code E.
3. Single requests shall be completed within 24 hours. Multiple requests shall take the appropriate amount of time per the number of applicants.
4. No fees shall be assessed for the completion, processing, and obtaining of CHRI information from local and/or state files.

Driver history requests shall be processed using Purpose Code J and forwarded to the Human Resources Director as stated in number 3 above.

F. Requests for Educational Purposes:

1. All requests for fingerprinting of persons applying for teacher or other positions with the Dublin City School System shall be referred to the local Georgia Applicant Processing Services (GAPS) office.
2. Local and state CHRI computer inquiries shall be made by the CJIS operator when the school system forwards a request via a signed consent form from the individual being inquired upon. Purpose Code W shall be used when making these inquiries. All CHRI information shall be forwarded to the school system personnel office.
3. Single requests shall be processed within 48 hours. Multiple requests shall take the appropriate amount of time per the number of requests received.
4. If an adverse employment decision is made due to the criminal history inquiry, the contents of the record received and the effect the record had on the employment decision must be made known to the applicant/employee by school system personnel.

G. Requests by Prospective Employers:

1. All requests for CHRI by prospective employers shall be in accordance with department policy, state law, and GCIC/NCIC rules and regulations. Record inquiries may be made for local and/or state records. All requests shall be made to the CJIS operator.
2. The prospective employer must furnish the CJIS operator with a signed consent form by the individual whose record is being checked. If needed, blank forms shall be provided by records personnel. Purpose Code M shall be used for individuals working with the mentally disabled. For all other employment reasons not covered in this policy, Purpose Code E shall be used.
3. Single requests shall be processed within 48 hours. Multiple requests shall take the appropriate amount of time per the number of requests. Information disseminated from local or state (GCIC) files shall only be information that matches the individual being inquired upon.
4. Each local or state record check will require a $20 fee to cover processing costs. All fees shall be paid at the time the inquiry is made. Payments shall be made in cash, money order, or by check to the City of Dublin.
5. If an adverse employment decision is made due to the criminal history inquiry, the contents of the record received and the effect the record had on the employment decision must be made known to the applicant/employee by the employer, organization, or agency.
6. Personnel shall be referred to the local Georgia Applicant Processing Services (GAPS) office for processing applicant fingerprints.

H. Nursing Homes, Licensing, Background, International and other Requests:

1. All requests for CHRI shall be in accordance with state law, GCIC rules and regulations, and department policy, and made through the CJIS operator. Record inquiries may be made for local and/or state records. All requests shall be made to the CJIS operator.
2. The requester must furnish the CJIS operator with a signed consent form from the individual whose record is to be checked. Blank consent forms shall be provided by the CJISoperator or records personnel if needed.
3. Single requests shall be processed within 48 hours. Multiple requests shall take the appropriate amount of time per the number of requests. Information disseminated from local or state (GCIC) files shall be only that information which matches the individual being inquired upon.

Requests for Nursing Home Employment shall be processed within a reasonable time not to exceed three days using Purpose Code N.

Each record check will require a $20 fee to cover processing costs. All fees shall be paid at the time of the requested inquiry. Fees are payable in cash or by check to the City of Dublin.

1. If an adverse employment decision is made due to the criminal history inquiry, the contents of the record received and the effect the record had on the employment decision must be made known to the applicant/employee by the employer, organization, or agency.
2. Personnel shall be referred to the local Georgia Applicant Processing Services (GAPS) office for processing applicant fingerprints.

I. Housing Authority Requests:

1. All requests for CHRI by the Dublin Housing Authority shall be in accordance with department policy, state law, and GCIC/NCIC rules and regulations. Record inquiries may be made for local and/or state records. All requests shall be made to the CJIS operator.
2. Authorized Housing Authority personnel must receive and maintain a signed consent form completed by the prospective tenant whose record is to be checked prior to the request being made to the police department. The CJIS operator shall have access to all completed individual tenant consent forms when necessary. If needed, blank consent forms shall be provided by records personnel or the CJIS operator.

Information furnished shall be the full name of the prospective tenant, their date of birth, race, sex and social security number. Purpose Code E shall be used for all inquiries.

1. Single requests shall be processed within 48 hours. Multiple requests shall take the appropriate amount of time per the number of requests. Information disseminated from local or state (GCIC) files shall be only that information which matches the individual being inquired upon.
2. Each record check will require no fee to cover processing costs.
3. If an adverse housing decision is made due to the criminal history inquiry, the contents of the record received and the effect the record had on the housing decision must be made known to the applicant by the Housing Authority.
4. Personnel shall be referred to the local Georgia Applicant Processing Services (GAPS) office for processing applicant fingerprints.

J. Requests by Private Attorney or Defense Attorney:

1. Requests for criminal history record information by a defense attorney for use in pending criminal cases shall be referred to GCIC.
2. Requests for criminal history record information by a defense attorney in a civil case shall be referred to the District Attorney's Office.

K. Requests for Open Records Felony Conviction Records:

1. All requests for inquiries regarding an individual's felony conviction record shall be processed by the CJIS operator. Purpose Code P shall be used when making inquiries. Single requests shall be completed within 48 hours. Multiple requests shall take the appropriate amount of time per number of requests.
2. Individuals requesting such records shall complete a felony conviction request form for each request. Completed forms shall be maintained on file in the CJIS operator’s office for a period of one year at which time they shall be destroyed by shredding.

Each record check will require a $20 fee to cover processing costs. All fees shall be paid at the time of the requested inquiry. Fees are payable in cash or by check to the City of Dublin.

# L. Individual Inspection of One's File:

1. An individual may, upon proper photo identification, review any criminal history record maintained on the individual by this department. Proper photo identification shall include a valid driver’s license, a State-issued identification card, or a military identification card. Such requests shall be handled by the records section or the CJIS operator.
2. An individual requesting to inspect his or her criminal history record file shall first show photo identification of which he or she is to records personnel or the CJIS operator, complete and sign a consent form, and pay a $20 processing fee. Requests shall be processed 7 days a week, 0800-2400 hours.
3. An individual requesting to inspect his or her driver history record file shall be instructed to make application with the Department of Driver Services.

M. Fees for Criminal History Record Information Inquiries:

1. When individuals request CHRI inquiries of departmental files, a fee of $20 will be assessed for each request.
2. When individuals request CHRI inquiries of GCIC files, a fee of $20 will be assessed for each request.
3. Fees shall not be assessed when inquiries are made using Purpose Code C or J. Fees are not assessed when requests are made by other City departments, government agencies, or law enforcement-related agencies when the request is for that agency’s employment purposes.
4. Fees shall not be assessed when requests are made by the Laurens County Juvenile Court, Dublin Housing Authority, and WINGS.

N. Transmission of Criminal History Record Information:

1. Criminal history record information (CHRI) shall be disseminated to non-criminal justice individuals by the following methods:
2. person-to-person
3. in writing
4. Criminal history record information (CHRI) shall be disseminated to criminal justice individuals by the following methods:

1. person-to-person
2. in writing
3. over the telephone if the requester is known
4. by fax machine if the requester is at the fax machinewhere the information is to be faxed
5. Police radios MAY BE used for the transmission of CHRI if the information is necessary to effect an immediate identification or to ensure adequate safety of police officers or the general public.

O. Record Restrictions:

1. Individuals seeking to have a record restricted from their local file must first request from the original arresting agency in writing their request that the record be restricted using the form prescribed by GCIC Individuals may secure a blank restriction form from records personnel.
2. Record personnel will process restriction requests from individuals making the request of their own file. An attorney may make the request on behalf of a client.
3. The requester shall complete the restriction request form and return it to records personnel for processing. A $25 fee shall be assessed for each arrest date by the GBI.
4. Record personnel shall receive and process all requests for record restriction. Record personnel shall complete a GCIC inquiry regarding the described arrest record. Upon completion, records personnel or the individual requesting the restriction can forward the request to the District Attorney's Office who will then determine if the record meets the criteria set forth in state law.
5. Once the District Attorney's Office has processed the request, they shall notify records personnel that all criteria have been met or have not been met.
6. If the records restriction is denied by the District Attorney's Office, the requesting individual shall be referred to that office for other inquiries and explanations. If the restriction is approved, the District Attorney’s Office shall make a notification to the individual by forwarding a copy of the completed and approved request forms as well as instructions on the process to forward the completed forms and fee to G.C.I.C. A copy of the completed and approved/disapprove section of the request form will also be forwarded to the records division of the department.
7. If the records restriction is approved, the agency shall restrict the individual record relating to the person's arrest.
8. **DOCUMENTATION OF LEDS FILES**

A. All entries shall be supported by official police reports (incident, supplemental, arrest, etc.).

B. Incident reports shall be prepared and completed by the officer taking the report or assigned the case before the end of his/her shift.

C. When the report cannot be completed by the end of the officer's shift, as much information as possible will be furnished and the report stamped incomplete. The full report will be completed as soon as possible.

D. The incident report shall be checked by the reporting officer's supervisor for accuracy and completeness.

E. Before the end of the shift, the supervisor shall submit a copy of all incident reports and other documents containing information that is to be entered into the GCIC/NCIC LEDS files to the CJIS operator, or after normal hours of operation, fax a copy to the E911Center.

F. The CJIS operator or E911 communications officer shall enter the record into the GCIC/NCIC files. Missing persons under the age of 21 shall be entered immediately. All other records shall be entered as soon as practical but within 12 hours.

G. When additional information that can be included in the record entries is developed, the case officer will forward copies of all updated or supplemental reports containing such information through the shift supervisor to the CJIS operator or E911 communications officer. The original record will then be updated.

H. Copies of all terminal transaction printouts will be attached to a copy of the incident report and any other necessary documentation. Copies will be maintained in the E911 Center files and the Dublin Police Department files.

1. **PROCEDURES FOR HANDLING "HITS" ON INQUIRIES**

A. When receiving a "HIT" responseon an inquiry of aperson, vehicle, or article that has been inquired uponby an officer, the CJIS operator shall notify the originatingagency thatentered the record and notify the officer and shift supervisor that a "HIT" has been received. If the "HIT" contains a CAUTION INDICATOR, IMMEDIATELY notify the officer and shift supervisor of the reasons for the caution. The CJIS operator shall follow procedures as outlined in the CJIS Policy and Operations Manual.

B. GCIC/NCIC "HIT" is not in itself probable cause to make an arrest, detain a missing person, or seize property. Only after a "HIT" has been confirmed by the originating agency, and after the department officer evaluates the age of the record, the closeness of the match between the subject and property described in the record and a “HIT” confirmation message, can there be probable cause to arrest or detain a subject or seize stolen property. If the officer has any doubts, he should contact his shift supervisor for additional direction.

C. If the "HIT" is on a record entered by the Dublin Police department, the CJIS operator will:

1. Notify the shift supervisor.
2. Indicate the time and date the shift supervisor was notified and process the record in accordance with procedures outlined in the CJIS Policy and Operations Manual.

D. During normal business hours, the CJIS operator or after normal business hours, the shift supervisor will check the case file to verify that the record is current, the subject is still wanted or missing or the property is still stolen.

1. The CJIS operator or shift supervisor will notify the officer of what procedure to follow.
2. The shift supervisor will advise the CJIS operator when a person is arrested or located or when property is recovered.
3. The CJIS operator or shift supervisor shall follow procedures outlined in the CJIS Policy and Operations Manual. The shift supervisor may request assistance from E911 personnel if needed.

E. When the "HIT" is on a record entered by another agency, the CJIS operator shall send a "Request for HIT Confirmation" message IMMEDIATELY and notify the shift supervisor.

1. **PROCEDURES FOR HANDLING "REQUESTS FOR HIT CONFIRMATION"**

A. The CJIS operator will notify the shift supervisor whenever a request for "HIT Confirmation" is received.

B. The CJIS operator will locate the original entry documents and verify the information contained in the request for "HIT Confirmation" against the original documents supporting the entry.

C. The CJIS operator will verify that the information in the LEDS files matches the information in the request for "HIT Confirmation."

D. The CJIS operator will respond to the request for "HIT Confirmation" within 10 minutes or 1 hour depending on the urgency by:

 1. Confirming the "HIT",

 2. Denying the "HIT", or

 3. Requesting more time stating the amount of time needed to confirm/deny the "HIT".

E. If a "HIT" is denied because the record is not valid; the CJIS operator will notify the shift supervisor and "Cancel" the entry immediately.

F. If a "HIT" is confirmed, the CJIS operator will wait for a "Locate" message to be entered by the agency to which the confirmation was sent. Upon receipt of the "Locate" message, the CJIS operator will "Clear" the record.

G. The CJIS operator shall refer to procedures outlined in the CJIS Policy and Operations Manual for additional information and instructions.

1. **VALIDATION PROCEDURES**

A. To ensure that all computer entries, hot files, and wanted/missing person files are accurate, complete, current, and maintained properly and securely, records shall be validated online each month when received from GCIC and in accordance with GCIC/NCIC rules and regulations.

B. In the absence of The Primary TAC or the direction of, the Secondary TAC shall ensure that all records received from NCIC shall be reviewed in a timely manner. Information received shall be compared with investigative case files and all other documents on which the record entries were based.

C. Personnel shall consider all possible alternatives for obtaining additional information to determine the current status of extradition limits, stolen property, and wanted/ missing persons. The following resources should be considered when determining the status of a record or when obtaining additional information about a person or item:

1. Compare all computer printouts to the supporting documentation to ensure that records are complete and accurate. Make corrections when necessary.
2. Check the driver's license, driver's history, criminal history, and vehicle registration files to obtain possible additional information.
3. Consult with investigators to ensure the proper status of the warrant, and to obtain additional information regarding a wanted/missing person or stolen property.
4. Consult with the District Attorney's office to ensure the warrant is prosecutable and has not been dismissed. Ensure extradition is authorized.
5. Check all original warrants; ensure they are complete, current, accurate, and valid.
6. Make phone contact with victims and/or other parties listed to ensure that reported items are still missing and have not been located/recovered and to get additional information if available. To ensure that individuals are still missing.
7. Make phone contact with public utilities and other local resources to identify additional information necessary to ensure proper validation of records.
8. When unable to make phone contact with property owners, send a written notice requesting confirmation of record status and any additional identifiable information.
9. Modify record entries that contain erroneous information or that are incomplete. Add supplemental information when appropriate.
10. Remove incorrect information from the records and re-enter the correct information.
11. Cancel invalid record entries from the NCIC files that cannot be corrected. A file that can be corrected will be immediately updated and re-entered with the correct information.

D. Personnel validating records shall document action taken with each record. Problems concerning any record shall be reported to the Primary TAC or Chief of Police and corrective action taken immediately.

E. The validation process shall be completed when all record entries have been verified as accurate, complete, and current or when records have been modified or canceled. The validation certification shall be completed and returned online to GCIC during the specified time frame.

1. **MISSING PERSONS**

A. When persons of any age are reported as involuntarily missing, missing and endangered, missing and disabled, or missing as disaster catastrophe victims, these guidelines will be followed. Before entry, obtain documentation that supports NCIC record entries, such as:

1. Official police report of a missing person
2. Written statements from a physician or other authoritative source verifying the missing person's physical or mental disability.
3. Written statements from a parent, legal guardian, next of kin, or other authoritative source advising that the persons are missing under circumstances indicating that his/her physical safety may be in danger.
4. Written statements from a parent, legal guardian, next of kin, or other authoritative source advising that the missing persons' disappearance was not voluntary.
5. Anyone **under the age of 21** should be entered **within two hours** after enough information is obtained to complete an entry per Federal Law and NCIC Policy.

B. AMBER ALERT (LEVI’S CALL). NCIC has implemented the capability to flag a missing person record associated with an AMBER ALERT (in Georgia, LEVI’s CALL). Once a determination has been made that an AMBER ALERT (LEVI’s CALL) will be issued, agencies may enter the missing person using either message key EMI, EMIC, EME, or EMEC with the Missing Person (MNP) code AA. To place AA in the MNP field, the missing person’s age should be less than 18 years. Use of the AA code will generate a $.8. AMBER ALERT notification to the National Center for Missing and Exploited Children (NCMEC) and the FBI. In addition, hit responses will be preceded by the following:

 \*\*\*\*\*AMBER ALERT\*\*\*\*\*ISSUED FOR NIC/MICXXXXXXXXX\*\*\*\*\*AMBER ALERT

If the missing person is already entered in NCIC when the decision to use an AMBER ALERT OR LEVI’S CALL is made, the record can be modified by changing the MNP to AA.

**\*To initiate an AMBER ALERT (LEVI’S CALL) contact the GBI 24-hour communications center at 404-244-2600.**

C. RUNAWAY JUVENILES (LESS THAN 21 YEARS OF AGE)

*Note: Per Federal Law and NCIC Policy, when agencies receive reports of missing juveniles, including runaways or any person* ***less than 21 years of age****, the records must be entered* ***within two hours*** *after enough information is obtained to complete an entry (42 USCS § 5780).*

1. Juvenile courts have jurisdiction over these persons.
2. Georgia law enforcement agencies that locate these persons may detain them without court orders for involuntary return to parents, guardians, or legal custodians within Georgia (O.C.G.A. § 15-11-17).
3. Georgia law enforcement agencies which locate such persons from other states, reported as runaways in other states, may detain them under provisions of the Interstate Compact on Juveniles (O.C.G.A. § 39-3-2). Upon being detained, any such person is to be brought before the local juvenile court for processing (O.C.G.A. § 39-3-2).
4. Within sixty (60) days of entry of a missing juvenile, the agency must attempt to update the record with any available additional information—specifically medical and dental records for identification purposes (42 USCS 5780).

D. RUNAWAY MINORS (LESS THAN 21 YEARS OF AGE)

*Note: Per Federal Law and NCIC Policy, when agencies receive reports of missing juveniles, including runaways or any person* ***less than 21 years of age****, the records must be entered* ***within two hours*** *after enough information is obtained to complete an entry (42 USCS § 5780).*

Because Georgia law does not provide for the forcible detention and return of 17-year-old Georgia runaways, include in the miscellaneous field of the record entry Locate Only - Do not Detain – Contact Dublin PD via administrative terminal message.

1. Neither the Georgia Missing Children Information Center nor GCIC have been able to determine what Georgia courts, if any, have jurisdiction over 17-year-old Georgia runaways.
2. Georgia law enforcement agencies locating such persons from other states, reported as runaways in other states, may detain them under provisions of the Interstate Compact on Juveniles (O.C.G.A. § 39-3-2). When confirming NCIC hits, determine if appropriate court documents have been obtained for the detention and return of the person. If so, those persons are to be brought before the local juvenile court (O.C.G.A. § 39-3-2). Otherwise, they should not be detained.

1. **PHYSICAL SECURITY**

A. CJIS information is protected by law and shall be maintained in secure areas within the department. CJIS documents/systems shall only be accessed by or disseminated to those who are authorized to access or receive said information in accordance with department policy, state law, or by rules, regulations, and policies of the Georgia Crime Information Center/National Crime Information Center (GCIC/NCIC).

B. Only specifically authorized personnel, as defined and described in this policy, shall have access to any and all CJIS terminals, information, documentation, and/or storage locations.

C. CJIS terminal locations shall be placed in secure areas with adequate physical security to protect at all times against any unauthorized viewing or access to computer terminals, access devices, or printed/stored data/information. These locations are **off-limits** to all department personnel except specifically authorized personnel as defined and described in this policy. The general public and other non-department personnel shall not be allowed in these locations. Volunteers, interns, community service workers, auxiliary personnel, etc. must complete a GCIC awareness statement and be fingerprinted prior to assuming any duties and/or functions that may involve access to CJIS information.

D. MDT terminals in vehicles, if used, will only be utilized by on-duty CJIS operators, and utilized for duty-related purposes only; the operator will ensure that the device is physically secured at all times and any display and/or printout is secure from public view. MDTs may not be used if the CJIS operator is not performing duties directly related to department operations; MDTs will not be used out of town during non-department events; they will not be used for an off-duty or extra-duty event. MDT printouts/documents shall be stored in a secure location and destroyed by shredding when no longer needed. These documents will not be left in vehicles.

E. Any and all CJIS information will be kept out of public view at all times. It will be stored in locking file cabinets in designated CJIS record locations when not needed, and shall be destroyed by shredding or burning when no longer needed. This includes computer displays that are designated as CJIS terminals. Again, CJIS information will not be thrown in a trash can.