Scope and Purpose

This Chapter governs the collection, processing, storage, retention, and dissemination of all documentary information obtained, collected, and/or created by the Department, except for information and records related to juvenile operations and offenders. Juvenile records and files are maintained and controlled by the Youth Division.

The purpose of this Chapter is to ensure all records within the Department are collected, stored, and disseminated in a manner that ensures the completeness, integrity, accuracy, and security of such information in a manner that protects individual privacy.

In instances where employees of this Department are faced with a situation regarding the disclosure of information, and a question is not specifically address in this Chapter, every reasonable attempt will be made to balance the legitimate competing interests of the public's right to know versus a person's right to privacy.

Records Definitions

The following definitions will be observed in this Chapter:

A. Criminal History Records Information (CHRI) – Records and related data contained in either a manual or an automated criminal justice information system, which is compiled by criminal justice agencies for the purposes of identifying criminal offenders and maintaining, as to such persons, notations of arrest, the nature and disposition of criminal charges, sentencing, confinement, rehabilitation, and release. CHRI is a general term, which includes within its scope conviction and non-conviction data. The term does not include identification information to the extent that such information does not indicate involvement of the individual in the criminal justice system.
B. Dissemination – The release, either verbal or printed (hard copy), of CHRI by an agency to another agency or individual, or the transfer of CHRI from one computer to another.

Dissemination of Information

Except as hereinafter provided, the records collected, stored, or retained by this Department shall not be disseminated unless the party(s) seeking such information is authorized to receive that information. If an individual requests any police record, they are entitled to:

A. "Page 1" of the Public Release Version of any police case report; and
B. Log entry only call sheets in regards to motor vehicle crashes, subject to any mandatory redactions made by the Records Division personnel. No other call sheets may be released to the public.

Police records involving juveniles, including "Page 1" of the Public Release version, shall not be released without review and approval from the City Attorney, Records Division Manager, and/or Open Records Clerk.

Any additional requests for police records shall be reviewed by the City Attorney's Office via the Open Records Clerk and/or Records Division Manager, and may require a ruling from the Attorney General's Office.

All open records requests must be made using the following methods:

A. Through the Next Request open records portal, available on the Department's website or the City's website;
B. Via email through the publicinfo@abilenetx.gov email address; or
C. In person at City Hall or Police Department.

Requests sent via fax or an email address other than publicinfo@abilenetx.gov shall not be accepted. All requests for information shall be referred to the Records Division Manager or Open Records Clerk before dissemination is allowed.

Security and Retention of Records (TBP 5.01, 5.02)

The Department operates and maintains a fully integrated, computerized records management system (RMS). The Department maintains a Records Division, in which paper copies are stored in lockable filing cabinets or in locked room(s). Only the Records Division Manager and Records Division Supervisor have a key to the filing cabinets and room(s). Police records shall be accessible to authorized police personnel to perform their official law enforcement duties. Paper copies of any record shall be scanned into the RMS by a Records Division employee, where the records will be stored electronically prior to being provided to any police personnel.

Records shall be retained in compliance with applicable state laws and in compliance with the City of Abilene Records Retention Scheduled.

Juvenile records shall be disposed of in accordance with the Texas Family Code and will be maintained separately from adult records.

Personal Use of Police Records

All records collected or stored in police files are confidential to the extent that no Department employee shall make use of such information for personal purposes.

Release of Police Records (TBP 5.03)

Department employees will not confirm or deny the existence of any CHRI in Department files to any individual or agency that would not be authorized to receive the information directly.

Warning: Pursuant to the Texas Public Information Act, written or electronic requests for information must be addressed within ten (10) business days of receipt. Failure to respond to the requestor within the ten (10) business day period may cause the information requested to become public record.

The employee making the dissemination shall promptly and completely leg each dissemination of CHRI taken from a criminal file folder in the RMS' dissemination module.

Information shall only be released in accordance with the Texas Public Information Act.

The Department shall provide appropriate training to designated employees who are authorized to release public information.

Other than the routine release of police records, employees should consult with the City Attorney prior to releasing information. A request for disclosure of information may require an Attorney General's Opinion, in compliance with the Texas Public Information Act.

CHRI File Maintenance

All CHRI files maintained by the Department (excluding juvenile records) shall be maintained by the Records section, or any other secure area designated by the Chief of Police. No CHRI file or contents of any CHRI file shall be removed by any employee of the Department, except by authority of the Chief of Police, the Records Division Manager, or the Records Division Supervisor.

Electronic Communications Policy

Purpose - The Department provides electronic communications to employees for use in performing police duties.

Because all communications are subject to disclosure and the Department is committed to professional integrity, certain communications are prohibited. Prohibited uses include:

A. Intercepting, eavesdropping, recording, or altering another person's e-mail messages;
B. Adopting the identity of another person in any e-mail message, attempting to send electronic mail anonymously, or using another person's password without the employee's prior approval;
C. Communicating e-mail that contains racial or sexual slurs or jokes, or other material that could be considered by others to be harassing, intimidating, abusive, or otherwise offensive; and
D. Using e-mail for commercial/promotional purposes, including personal messages offering to buy or sell goods or services. Exceptions are authorized uses of the PDNET and those made by the Managing Director for Administration, City of Abilene.

Mobile Data Computer and CJIS Security

Purpose and policy – the purpose of this policy is to establish guidelines for use and security of the Department-issued Mobile Data Computer (MDC) equipment and related CJIS (Criminal Justice Information System) information. Failure to comply with this policy can result in disciplinary action or termination.

Definitions:

A. MDT/MDC (Mobile Data Terminal/Mobile Data Computer) – this term includes all computers that have access via wireless or hardwired network to TLETS, TCIC, NCIC, or any other law enforcement database.
B. Secure Location – this term includes areas of the Department that are not open to the public that have been properly marked with "Authorized Personnel Only" signs. This term also includes official police vehicles that are locked and/or attended by authorized sworn police personnel.
C. Non-secure Location – this term includes all locations not defined as a secure location above.

Procedure: General Security of Access to CJIS Information:

A. CJIS, TLETS, TCIC, and NCIC data shall be accessed only from secure locations, as defined above.
B. Each person authorized to access MDT data shall receive security awareness training within six (6) months of appointment or employment and thereafter at least every three (3) years in accordance with CJIS policy. The training will be documented.
C. Visitors to secure areas shall be escorted by authorized personnel at all times.
D. Changes in authorized personnel shall be immediately reported to the TCIC Training section.
E. All printouts of CJIS data shall be promptly filed with the corresponding incident records. Otherwise, such printouts should be promptly shredded using a cross-cut shredder.
F. All storage media containing or used for CJIS data that is no longer used shall be securely formatted using methodology that overwrites all data in three iterations and then the disk shall be physically destroyed.
G. The local CJIS network equipment room shall be securely locked when not occupied.
H. All equipment used for processing CJIS data shall have anti-virus software installed and updated on a daily basis. The MDT firewall shall be enabled at all times.
I. It shall be the responsibility of each authorized user to report any violations of this security policy to the Chief of Police.
J. No personal hardware of software shall be allowed on the agency's TLETS network.

Security of Mobile Data Terminals/Computers (MDC)

A. The Department shall keep a list of all wireless device IDs and vendor telephone contact numbers so that devices can be promptly disabled, should the need arise.
B. When transporting non-law enforcement personnel in police vehicles, officers will dim/close the screen of the MDT or position it in a manner that will prevent unauthorized viewing of MDT data.
C. All police vehicles containing MDTs shall be securely locked when not in use.

Mobile Data Computer: Acceptable Use

A. The purpose of the Mobile Data Computer is to enhance the patrol officer's ability to obtain necessary information in a timely manner, reduce radio traffic, provide dispatch information, and increase officer safety. Due to the substantial cost and liability associated with this device, distinct guidelines must be established concerning the operation of the unit.
B. All users of the Mobile Data Computer must attend a training session prior to operating the unit.
C. The use of this device must be in support of law enforcement and associated information exchange in the form of dispatch, case report, internet access, and email. Internet access will be restricted, and any attempted to circumvent this restriction will result in termination of the user account.
D. All communications and information accessible by this device should be considered confidential.
E. While mobile data information is confidential in nature, officers are reminded that mobile data messages between terminals are subject to discovery and request for information filed under the provisions of the Texas Public Information Act. Subversive Acts shall apply to all communications transmitted on the mobile data system. Under no circumstances should messages contain language that is profane or offensive, or that tends to denigrate any particular gender, race, nationality, ethic, or religious group or person.

Due to the sensitive nature of the data that will be available to the user, the following guidelines must be followed:

A. No software of any kind may be loaded into the computer.
B. No information will be obtained for the personal gain of the user or any acquaintance. Any such attempt will result in account removal and potential criminal prosecution.

The cost of deployment of a standard Mobile Data Computer is substantial. It is the user's responsibility to respect and handle the computer as a sensitive electronic device.

A. Any damage or problems should be reported to the appropriate Information Technology team member as soon as possible.
B. No component of the computer may be used for any purpose other than its original intent and configuration.

Disposal of All Medial Procedures

A. When no longer useable, diskettes, tape cartridges, ribbons, hard copies, printouts, and other similar items used to process CJIS data shall be destroyed by shredding (which must occur before disposal), incineration, or degaussing, considering whichever method is available, appropriate, and cost effective. This list is not all inclusive.
B. IT systems, which have processed or stored CHRI, shall not be released from control until the equipment's hard drive has been removed and crushed.