
ADMINISTRATIVE DIRECTIVE – 101.005
UNAUTHORIZED DISCLOSURE OF DEPARTMENT INFORMATION

EFFECTIVE DATE: January 3, 1977
AFFECTS: All Personnel

REVISION DATE: March 25, 2020

I. PURPOSE

The nature of police work requires specific information to remain confidential because of laws protecting individual rights and the need to protect certain operating procedures of the agency. This directive provides general guidelines regarding employee responsibilities in maintaining confidentiality of information.

II. POLICY

The disclosure of recorded information or any information concerning departmental operations is prohibited unless there is a determined "need to know"; the information is needed by another criminal justice agency; or it is required by law to be disclosed. Personnel are expressly prohibited from the disclosure or discussion of departmental information of a confidential nature, information that might jeopardize the success of a tactical operation, investigative information, or information that might violate the right to privacy of an individual. Unless specifically authorized, no information will be released without a request in writing from the person/agency seeking the information.

III. DEFINITIONS

- A. CJIS Security Policy – Provides criminal and non-criminal justice agencies with a minimum set of security requirements for access to criminal justice information.
- B. Criminal Justice Agency User Agreement - A written agreement with the Department of Public Safety to receive access to criminal justice information, signed by the Plano Police Department.
- C. Criminal Justice Information - Refers to all Federal Bureau of Investigation provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data.
- D. Department of Public Safety Information Systems - Information systems sponsored by the State of Texas that require a Criminal Justice Agency User Agreement.
- E. Restricted Criminal Justice Information - Specific files within the Department of Public Safety Information Systems that require additional protection while the information is "in transit" to another person or location.
- F. Secure Location - A facility, area, room, or group of rooms within a facility, or any enclosed mobile vehicle used for the purposes of criminal justice activities with both the physical and personnel security controls complying with the CJIS Security Policy and referencing the protection of criminal justice information and its associated information systems.

IV. PROCEDURES

- A. Disclosure of information to other members of the department will be on a need-to-know basis only. Work papers and documents within an office, on or in a desk, or computer files and disks are not for general viewing and all members are prohibited from attempting to observe or read such papers.
- B. Personnel shall not photograph or record, by any means, any official police action or activity including but not limited to, vehicle or foot pursuits, use of force, or crime scenes except as is necessary in the official performance of their duties. Personnel shall not make any such recordings with their personally owned equipment for their personal use. All recordings of such activities made by personnel during the official performance of their duties shall be the property of the Plano Police Department and the dissemination shall be in accordance with the department's established procedures.
- C. Emailing Criminal Justice Information

ADMINISTRATIVE DIRECTIVE – 101.005
UNAUTHORIZED DISCLOSURE OF DEPARTMENT INFORMATION

EFFECTIVE DATE: January 3, 1977
AFFECTS: All Personnel

REVISION DATE: March 25, 2020

1. Criminal Justice Information can be emailed with the intention of sharing information to other authorized personnel.
2. Personal email addresses are strictly prohibited to send from, sent to, or receive Criminal Justice Information. The City of Plano assigned email address will be used.
3. Following the CJIS Security Policy, when emailing restricted criminal justice information (listed below) outside of the City of Plano, ENCRYPTMAIL will be added to the subject line.
 - a. Gang Files
 - b. Historical Protection Order Files specifically listed in NCIC
 - c. Identify Theft Files
 - d. Known or Appropriately Suspected Terrorist Files
 - e. National Sex Offender Registry Files
 - f. NICS Denied Transaction File
 - g. Person With Information data in the Missing Persons Files
 - h. Protective Interest Files
 - i. Supervised Release Files
 - j. Violent Person File
- D. This directive is not intended to restrict the flow of information within the department, but is necessary to preserve the confidentiality of information.
- E. Disclosure of Information Received Through any Department of Public Safety Information System
Information obtained from any Department of Public Safety Information System that is controlled through a user agreement will not be disclosed to any non-authorized personnel, any person not directly associated with law enforcement and who does not have a need to know.
- F. Disclosure of Specific Crimes Information
 1. Employees should refer to directives regarding the following for specific limitations:
 - a. Juvenile Operations
 - b. Release of File Information
 - c. Sexual Assault Investigations
 - d. Sexual Offender Registration
 2. Questions regarding Open Records requests should be referred to the departmental Legal Advisor or Open Records Unit.
- G. Accessing Information Outside a Secure Location
 1. The CJIS Security Policy must be adhered to when accessing criminal justice information outside of an approved secure location.
 2. Remote access to criminal justice information must be on city issued equipment allowing access to be controlled.
 3. All personnel will ensure that any displays of criminal justice information will be positioned in a way to prevent unauthorized individuals from accessing and viewing the information.

ADMINISTRATIVE DIRECTIVE – 101.005
UNAUTHORIZED DISCLOSURE OF DEPARTMENT INFORMATION

EFFECTIVE DATE: January 3, 1977
AFFECTS: All Personnel

REVISION DATE: March 25, 2020

4. When away from the computer, personnel will lock and close the screen to protect the criminal justice information.
 5. Personally owned devices are not authorized to access, process, store, or transmit criminal justice information.
 6. All digital and physical media will be stored within an approved secure location.
- H. Violation of Requirements and Procedures

The violation of requirements and procedures established by this administrative directive and as determined by the CJIS Security Policy and the Department of Public Safety Crime Records Service may result in disciplinary action up to and including dismissal.