ADMINISTRATIVE DIRECTIVE – 101.026
USE OF DEPARTMENT COMPUTER SYSTEMS

EFFECTIVE DATE: June 20, 2000 **REVISION DATE: September 20, 2011**
REVIEW DATE:
AFFECTS: All Personnel

NOTE: ALSO REFER TO ADMINISTRATIVE DIRECTIVE 113.004
ELECTRONIC TRANSMISSIONS – EMPLOYEE RIGHT TO PRIVACY

I. PURPOSE

This directive addresses the access, use, and controls of Plano Police Department computer systems. The procedure provides specific guidelines and rules governing the use of MDCs, computers, laptops, and other computer hardware and software, including Internet browsing, e-mail, and file transfer/download.

II. POLICY

The continuing success of the Plano Police Department depends largely on public trust and confidence. The organization's reputation and integrity necessitates adhering to the highest standards of business conduct. The Department requires computer systems to perform tasks essential to its operation and the safety and welfare of employees and the residents of the City. The use of these computerized systems must be in compliance with the following procedures.

III. PROCEDURES

A. MDCs, E-Mail, laptops or wireless and other computer systems and resources are expected to be used for official city business; however, from time to time employees are permitted occasional personal use of assigned computer equipment (provided the personal use does not result in cost being incurred by the City).

B. Allowable uses of computer systems and information include the following:

1. Facilitate performance of job functions
2. Communication of information in a timely manner
3. Coordinate meetings for departmental business
4. Communicate with other city departments
5. Communicate with outside organizations as required to perform an employee's job function

C. Prohibited uses of systems and information include but are not limited to the following:

1. Illegal activities
2. Slander
3. Defamation
4. Political endorsements
5. Commercial activities
6. Using non-business software including games or entertainment software
7. Using any city software or hardware to conduct non-city business or for personal purposes, except as outlined in III.A above.
8. To violate any other city policy (See HR Policies 223.000 Internet and E-Mail and 224.000 PC Use)

D. Employee Responsibilities

1. Encouraged practices:

a. Regular deletion of unneeded files, as permitted by Records Retention Schedules,

especially those stored on shared computer resources.

b. Electronic viewing of documents rather than printing

c. Keeping disk space use to a minimum

d. Maintaining E-mail boxes by deleting old messages and sent files

e. Routine backup of important files

f. Signing on to the city's network to obtain the latest virus update

g. Supervisors must notify the system administrator of any departmental transfer, employee separation, or change in access requirements. Notification should be made in memorandum form through the chain of command via the Police Information Services Coordinator as soon as the supervisor becomes aware of the change.

h. Unless otherwise directed by Information Services, PC's should be logged on to the network daily in order to get the latest virus protection updates.

2. Discouraged Practices

a. Do not send e-mail to "all PPD users" unless it is absolutely necessary

b. Users will not bypass or attempt to bypass security mechanisms or data protection schemes.

c. Screen savers, other than those provided by the Department, are not permitted. Screen savers consume memory resources and are often problematic even after removal.

d. Refrain from the use of computer generated sounds or visuals that might be disruptive to coworkers.

E. User IDs and Passwords

1. User IDs and passwords establish accountability for activity performed on Plano Police Department computer systems, and all actions performed are the responsibility of the person who has been assigned that user ID. Employees should not share their personal user ID or password, or use their ID or password to log onto PPD computer systems for another person. Passwords must remain confidential and should not include information that can be easily guessed. This includes changing the initial assigned password as soon as possible.

2. The Police Information Services Coordinator must be immediately notified if any unauthorized use of User Ids or passwords is detected, or if unauthorized use is suspected.

F. Software

1. Copying of City owned/licensed software for unauthorized purposes is prohibited.

2. Privately owned software may be loaded on departmental computers if it is necessary for business and is properly licensed. Personal software will be removed if it conflicts with departmental hardware or software, interferes with the ability of other employees to access or utilize the computer or occupies excessive storage space needed by the department.

3. Software that is not properly licensed to the City of Plano or the Plano Police Department shall not be utilized on Department owned computer hardware without prior approval of the Police Information Services Coordinator or his designee.

4. All outside disks or software (not owned by the City of Plano) must be inspected for virus infection prior to introduction in to the departmental system, stand-alone systems, or

departmental owned laptops.

5. Users may not modify software except when software is intended to be user customized.

G. Internet

1. System users must use extreme caution when transmitting information over the Internet.
2. All use of the Internet, including the use of e-mail, is subject to review and monitoring at any time.
3. Plano Police Department personnel should be aware that certain information about the police department as it relates to crime information or case investigations must never be discussed on the Internet. Extreme care must be taken at all times not to compromise this information.
4. Only business-related Web sites or bulletin boards should be "browsed." Browse access must be approved by the Administrative Manager or the Assistant Chief.
5. Only business related e-mails and file transfers/downloads are permitted. Use of Web-based e-mail services (such as Hotmail, Yahoo E-mail, Juno etc.) is not permitted through the department's resources.
6. E-mail use must be professional and courteous. E-mail communications must never jeopardize or impinge the reputation or integrity of the police department.
7. Users must recognize that the Internet is a worldwide network of interconnected computers and that internet technology makes it easy to replicate or edit a message and distribute it to many people without the knowledge or consent of the author.
8. Do not communicate department sensitive or confidential information unless you are explicitly approved to do so. Sensitive information includes but is not limited to, the following:
   a. Case Information
   b. Investigative notes
   c. Individuals under investigation
   d. Personnel information
9. The Police Information Services Coordinator is responsible for providing information, when requested, regarding computer use to the area's chain of command about users, access levels, usage, Web sites visited, and e-mails (including e-mail attachments) sent.

H. Investigative Databases

1. The Department has various commercial/free on-line databases and query systems available for investigative purposes. Most of these resources are not available to the general public, and personnel access to these resources is contingent upon employment with the Department. These systems are to be utilized for official Law Enforcement purposes only. Any use other than for legitimate Law Enforcement Investigative purposes is strictly prohibited and may constitute a violation of the law. Personal use of these resources is prohibited.

   Note: List of the available resources used can be found at:
   http://planonet/sites/pd/CID/Technology/default.aspx

I. Records Management System

1. All passwords and codes for personnel authorized to access the Records Management System are assigned by the Police Program Analyst.

    a. New employees will be assigned passwords and/or codes during their initial training, at the request of their immediate supervisor.

    b. In the event an employee who has been assigned an individual password or access code transfers or resigns, the Police Program Analyst will immediately deactivate the password or code. The Professional Standards Unit is responsible for notifying the Police Program Analyst of employee transfers or resignations through a copy of the employee Personnel Action Form.

    c. The Police Program Analyst may elect to assign a new employee password or access code at any time he believes the integrity of the Records Management System may be compromised or threatened.

2. The Police Program Analyst is responsible for overseeing the Central Records Computer System to ensure passwords and codes are valid as well as ensuring no system access violations occur. The computer systems will continuously check the validity of attempts to log into the system and an audit trail will be created which can be reviewed by the Police Program Analyst.

3. Employee Responsibilities

    a. Employees authorized to access the Records Management System must take special care to log off the System when leaving their workstation for any extended length of time; and should shut down their computer at the end of their shift.

    b. Do not allow others to sign on to the System using your password or access code, unless they are specifically authorized to do so by the Police Program Analyst.

    c. Notify your supervisor and/or the Police Program Analyst immediately if you believe the integrity of the Records Management System has been compromised or is susceptible to compromise. The Police Program Analyst is responsible for determining what appropriate action should be taken to regain security of the Records Management System.

IV. Special Considerations

A. Departmental

Each unit is responsible for policy compliance and may implement more restrictive policies as necessary for the performance of unit tasks.

B. Use of a home computer for the conducting of PPD business, while permitted, is subject to all the same practices, controls, and penalties described in this procedure regarding information confidentiality and security. No sensitive case information is allowed to be stored on home computers or any computer or electronic device that is not under the control of the PPD and PPD personnel.