


# TEXARKANA POLICE DEPARTMENT

## GENERAL ORDERS MANUAL

<b>SUBJECT</b>	<b>Use of Computer Equipment, Email and Internet Access</b>		
<b>NUMBER</b>	<b>1109.01</b>	<b>EFFECTIVE DATE</b>	<b>February 15, 2011</b>
<b>Scheduled Review Date</b>	<b>March 01, 2017</b>	<b>ISSUE DATE</b>	<b>February 15, 2011</b>
<b>Date Reviewed</b>		<b>REVISION DATE</b>	<b>March 12, 2015</b>
<b>APPROVED BY</b>		<b>(Reserved for Expansion)</b>	

### I. Scope and Purpose

- A. The purpose of this policy is to establish the policies and procedures for employee use of Texarkana Police Department computer systems to include all computer hardware, software, email systems, and Internet access systems. The provisions of this policy shall apply to all members of the Texarkana Police Department.

### II. Policy

- A. The Texarkana Police Department encourages and supports the use of computer systems as a means of improving productivity and efficiency. To ensure certain standards are managed, appropriate security of vital data is maintained and improper and inappropriate uses of computer equipment are avoided, certain restrictions and guidelines governing the use of computer equipment are necessary. All Texarkana Police Department computer systems and software must be used for official Texarkana Police Department use only. Personal use and correspondence using Texarkana Police Department computer systems during and outside business hours is not permitted. All members of the Agency shall recognize and adhere to the guidelines and procedures set forth by this policy.

### III. Definitions

#### A. For the purposes of this policy, the following terminology shall apply:

1. **Data File**—Collection of data accumulated for a definite use. Examples include word processing files, spreadsheet files, databases, etc.
2. **Hardware**—The electric, electronic and mechanical equipment used to process data. Examples of hardware include the central processing unit, display screen, keyboard, printers, etc.
3. **Software**—A set of programs that direct the computer to perform a function or series of functions. The "office suite" on each computer are examples of software. Programs are generally referred to as a set of unique instructions, created by a "programmer", for specific functions.
4. **Server**—The hardware and associated pieces of equipment that act as a "host" for all of the computers on the network in the police facility. The server also houses the email software, as well as stores the majority of the software used by the Texarkana Police Department.

Page 1 of 5	Number: 1109.01	Effective Date: February 15, 2011
Subject: Use of Computer Equipment, Email and Internet Access		<b>Revision Date: March 12, 2015</b>

5. **Internet**—A worldwide network of computers containing millions of pages of information and many diverse points of view.

#### IV. Procedures

##### A. The following governs computer equipment and its use:

1. The installation of any hardware or related equipment on the Texarkana Police Department's computer network without prior authorization by the Chief of Police or his designee is prohibited.
2. All computer equipment is the property of the Texarkana Police Department. Like all other Departmental equipment, employees shall exercise due care when using computer equipment. Abuse or unauthorized tampering with computer equipment will not be tolerated.
3. Employees shall report incidents of malfunctioning equipment to their supervisor who will in turn notify the Services Division Commander or his designee. Unless authorized, employees shall not attempt to make any repairs to any computer equipment owned by Texarkana Police Department.
4. Once an employee has established or been assigned passwords and usernames that facilitate access to the Texarkana Police Department's network and related computer systems on that network, the respective employee shall be solely responsible for all actions taken while using that password.
5. Sharing or disseminating individual usernames and/or passwords with any other person is prohibited. Employees of the Agency will be held responsible for the actions of another individual who utilizes a username and password assigned to him/her when such information has been disclosed to that individual.
6. Deletion, examination, copying or modification of any computer files or data belonging to the Texarkana Police Department or another user without their prior consent is prohibited.
7. Forgery or attempted forgery of electronic mail messages is prohibited.
9. Electronic messages are considered official correspondence. As such, they may be subject to both internal and external review. Transmission of electronic messages and information on communications media provided for employees of the Agency shall be treated with the same degree of propriety, professionalism and confidentiality as other official written correspondence.
10. Confidential, proprietary or sensitive information may be disseminated and/or made available through shared directories or network systems only to those individuals with a need and a right to know and when there is sufficient assurance the appropriate security of such information will be maintained. Although not inclusive, confidential, proprietary or sensitive information includes the following:
  - a. The transmission of personal information, such as salaries, performance reviews, complaints, grievances, misconduct, disciplinary information, medical records, or related employee information.
  - b. Criminal history information and confidential informant master files, identification files or related information.
  - c. Intelligence files and information containing sensitive, tactical or undercover information.
11. All Department computers are designed and intended to conduct the Agency's official business and is restricted to that purpose. Installation of software or access to software solely intended for

Page 2 of 5	Number: 1109.01	Effective Date: February 15, 2011
Subject: Use of Computer Equipment, Email and Internet Access		<b>Revision Date: March 12, 2015</b>

entertainment or recreational purposes is prohibited. Although not inclusive, the following is a list of those exceptions to the official business requirement:

- a. Infrequent personal use of Department computers may be permissible if limited in scope and frequency and as long as such use remains within the mandates, requirements, guidelines and other elements contained within this policy. Authorized use must not be connected with a profit-making business enterprise or the promotion of any product, service or cause that has not received prior approval from the Chief of Police or his/her designee. Examples of this include brief computer use prior to and after normal duty hours and/or during an employee's lunch break.
  - b. Members of the Agency may make off-duty personal use of Department computers for the purposes associated with professional and career development activity. All such authorized use must remain within the mandates, requirements, guidelines and other elements contained within this policy.
12. To avoid breaches of security, members of the Department shall lock his/her Departmental computer that has access to the Agency's network, electronic mail system, the World Wide Web or sensitive information when the member leaves his/her work station. Department members who are accessing a shared workstation shall ensure they log-off the system before departing from their session at the workstation.

**B. The following governs software and its use:**

1. The integrity, security and safety of the data on the Texarkana Police Department's network is of the highest priority.
2. No employee shall introduce, remove, alter nor cause to be introduced any software or other program on any piece of computer equipment owned by the Texarkana Police Department unless authorized by the Chief of Police or his designee.
3. Employees are prohibited from displaying screen savers on Departmental computer equipment that contain inappropriate, offensive, degrading or otherwise impermissible content.
4. All software purchased by the Texarkana Police Department remains the property of the Texarkana Police Department. Copying or transferring of Departmental software in a manner contrary to the software manufacturer's licensing agreements is not only prohibited by this policy but is illegal. Software owned by the Texarkana Police Department shall not be loaned or distributed to others.
5. All computer software use must follow appropriate copyright and licensing laws to avoid any potential liability to the Texarkana Police Department. Only software purchased by and licensed to the Texarkana Police Department will be permitted to be installed on any Departmental computer, and then only with the authorization of the Chief of Police or his designee.
6. Members of the Agency shall not download or install on any Department computer or network terminal any file, software or other materials from the World Wide Web or other external sources without taking the prescribed steps to preclude infection by computer viruses.
  - a. All material should be downloaded to discs or other outside media storage methods and scanned for viruses prior to being entered into any Department computer or network terminal.
  - b. In no case shall external materials or other applications be downloaded directly to any Department computer or network terminal.

Page 3 of 5	Number: 1109.01	Effective Date: February 15, 2011
Subject: Use of Computer Equipment, Email and Internet Access		<b>Revision Date: March 12, 2015</b>

**C. The following governs the email system—both external and internal—and its use:**

1. Employees of the Texarkana Police Department may be authorized by the Chief of Police or his designee as recipients of an email account administered on the Department's computer network system.
2. Employees are prohibited from causing, receiving, displaying, printing or otherwise disseminating material that is fraudulent, harassing, illegal, embarrassing, sexually explicit, obscene, intimidating or defamatory. Any employee encountering such material shall report it to his or her supervisor immediately. The supervisor shall then report the incident to the appropriate Division Commander through the established chain-of-command.
3. Employees are prohibited from using the Texarkana Police Department's computer equipment and all related programs to transmit or receive commercial or personal advertisements, solicitations for non Departmental businesses, commercial promotions, destructive programs (i.e., computer "viruses"), political or religious material or any other unauthorized use.
4. Email messages which are sent and/or received using Departmental equipment are considered the property of the Texarkana Police Department and should not otherwise be considered private in nature. Casual or improper use of email can create a liability to the Texarkana Police Department from both employees and the public. All information, data and emails shall be considered public information through the Freedom of Information Act. All users are reminded that although the active monitoring of routine email messages is not the practice of the Texarkana Police Department, messages may be monitored from time to time—without notice—as deemed appropriate by the Chief of Police or his designee.
5. All attempts to read, delete, copy, or modify the email of other users without their prior permission is prohibited.
6. Employees should not participate in email chain letters, "mail bombs", "spamming", or other activities that generate large amounts of useless network traffic.
7. Users must ensure that they do not divulge information of a sensitive or confidential nature using the email system. Employees should use reasonable care to ensure that the intended recipient will have access to the message.
8. The Texarkana Police Department has taken every precaution to protect the internal computer systems. Software to detect and remove viruses has been installed on the servers, email systems and workstations. This anti-virus software is updated on a regular basis. However, in order to maintain security of the network, network users should never open email unless they are sure of the identity of the sender.
9. Members of the Agency shall check their Department email account at the beginning of their duty assignment each day.

**D. The following governs World Wide Web browsing and internet usage:**

1. In an effort to provide Department employees with a valuable resource to assist in the performance of their duties, employees may be provided access to the internet.
2. No employee may use Departmental internet resources for commercial or personal advertisements, solicitations, promotions, transmittal of destructive programs (viruses, etc), political or religious purposes, or any other personal or unauthorized use. The downloading of computer software programs or any other type of file is prohibited.

Page 4 of 5	Number: 1109.01	Effective Date: February 15, 2011
Subject: Use of Computer Equipment, Email and Internet Access		<b>Revision Date: March 12, 2015</b>

3. Sending, receiving, displaying, printing or otherwise disseminating material that is fraudulent, harassing, illegal, embarrassing, sexually explicit, obscene, intimidating, or defamatory is strictly prohibited. Employees encountering such material shall report such occurrences to their supervisor immediately.
4. Personnel having access to the internet are reminded they are personally responsible for the material they review and download.
5. Accessing or transmitting material—other than material required for police business—that involves the use of obscene language, images, jokes, sexually explicit materials or messages that disparage any person, group or classification of individuals is prohibited, whether or not a recipient has consented to or requested such material.
6. The Texarkana Police Department retains the right to monitor any and all aspects of its computer system to include monitoring those websites employees visit on the internet, reviewing material downloaded or uploaded by employees, and reviewing email sent and received by its employees. Employees waive any right to privacy in anything they create, store, send, or receive on Departmental computers or the internet.
  - a. The Agency reserves the right to access any information contained and/or stored within any computer and may require a member of the Department to provide passwords to those files which have been either encrypted or password protected.
7. Computerized logs of browser access to the internet are maintained. These logs record when all internet connections were made, from where they were made, by whom they were made, and the web sites visited. **Connecting to the Internet using Departmental computer equipment indicates an employee's knowledge of and consent to monitoring and logging.**
  - a. Inappropriate use of computer equipment is prohibited conduct, and the Chief of Police has developed a system by which the computer activity of a random selection of department employees is examined every quarter.
  - b. The Services Division Commander will generate a random group number once per quarter that corresponds to the random selection system used to monitor compliance with policy. The Services Commander will be responsible to generate an electronic computer history associated with every employee assigned to the chosen group.
  - c. As identified within the paragraph 7 above, the computer history provides a detailed account of all computerized activity that occurred on the employee's profile during the selected time frame. This includes a list and categorization of all sites on the World Wide Web which were visited during the time frame. The report will also provide a detailed history containing the type and amount of data downloaded from each web site.
  - d. The Services Commander or his designee will be responsible to research each report and determine appropriate compliance with policy. All misconduct with respect to the use of computer equipment, email and internet access will be managed in accordance with the Department's disciplinary policy: [1104.03--Disciplinary Process](#).
  - e. Supervisory personnel within the agency may request a computer history report associated with an employee falling within their span-of-control at any time without advanced notice. Consistent with Section G Paragraph 3 above, the Services Commander or his designee will remain responsible to generate all computer history reports requested by supervisory personnel.

Page 5 of 5	Number: 1109.01	Effective Date: February 15, 2011
Subject: Use of Computer Equipment, Email and Internet Access		<b>Revision Date: March 12, 2015</b>