This policy statement and the procedures thereunder are intended for Police Department use only. The policies, procedures, and regulations are for internal Police Department administrative purposes and are not intended to create any higher legal standard of care or liability in an evidentiary sense than is created by law. Violations of internal Police Department policies, procedures, regulations, or rules form the basis for disciplinary action by the Police Department. Violations of law form the basis for civil and/or criminal sanctions to be determined in a proper judicial setting, not through the administrative procedures of the Police Department.

Policy #	318A	**Effective Date**	01/21/2016
Policy Name	Use of Departmental Computer Systems	**Approved Date**	01/21/2016
Approved by	*Wendell Franklin, Chief of Police*	**Previous Date**	01/30/2008

PURPOSE OF CHANGE:

To update policy format.

POLICY:

All computer systems that are installed or used in the Tulsa Police Department are under the administrative control of the Chief of Police or his designee. No changes will be made to Tulsa Police Department hardware, software, or peripherals without obtaining approval outlined in this policy. The Tulsa Police Department will partner with the City of Tulsa IT Department to determine which technology platforms meet the needs of TPD and comply with City of Tulsa technology and security requirements in addition to ensuring Tulsa Police Department policy is compliant with City of Tulsa policy and security standards. IT Department personnel or City of Tulsa Security shall not view files or data stored on Tulsa Police Department computers or on the City of Tulsa network unless such access is necessary for routine maintenance, to repair a technology malfunction, to maintain network security, or as directed to do so by the Chief of Police or his designee.

The Tulsa Police Departments prohibits the installation, duplication, or copying of software on any Tulsa Police Department computer if the installation would violate copyright or licensing laws.

Internet access is vital to conducting the official business of the Tulsa Police Department. Tulsa Police officers shall use the internet to assist in the investigation of criminal cases, conduct work-related research, and perform other official TPD business. Officers may connect personal devices to Tulsa Police Department wireless internet access within TPD facilities or to TPD issued broadband devices. While using City of Tulsa internet access, Officers are obligated to use personal devices within the constraints set forth within this policy.

Information or data transmitted in any form using City of Tulsa technology including email, internet connections, CADS messaging, text messages, or any other communication media must follow Tulsa Police Department policy regulating conduct of police personnel. Communication conducted on any TPD equipment including but not limited to the following: text, facsimile, graphical, visual, or voice, is the property of the Tulsa Police Department and as such is subject to inspection by any City of Tulsa personnel or outside agency authorized by the Chief of Police. In addition, communication on any City of Tulsa technology may be subject to the Open Records Act or other public scrutiny. Any transmission of actual or inferred sexual or racial text, graphics, or audio using the City's technology is forbidden. Violation of this policy will result in disciplinary action being taken upon the party or parties initiating or actively participating in such a transmission.

This policy provides specific procedural guidelines for the operation of computing and technology devices that are necessary to safeguard the integrity of the system and to ensure compliance. Police personnel are expected to adhere to measures to safeguard the security of the City of Tulsa computer network and report any issue which indicates a security breach has occurred.

SUMMARY: Procedures for using departmental computer systems and for operating any Tulsa Police Department Computing device.

APPLIES TO: All police personnel

DEFINITIONS: See 31-318 Attachment

PROCEDURES:

A. CITY OF TULSA NETWORK

1. The IT Department (IT) will assign a network username/login name and initial login password to all police personnel granted access to the Department's computers. All users will be required to change their password upon their first login and on a regular basis thereafter.

2. All police personnel will have access to the email system. The email system can be accessed from any City of Tulsa computer or any other computer with internet access. The email system is operated by IT and users will follow IT's practices and policies.

3. If a PC malfunctions or a problem with the system occurs, employees shall notify the Service Desk at extension 7070.

4. If an employee terminates employment or transfers to another City Department, the IT shall be notified by the Police Budget Section as soon as practical to remove the user's access to City and Police information systems.

B. AUDITS AND SECURITY

1. IT will periodically monitor and audit. If any unauthorized software, hardware, and/or any passwords are discovered, IT personnel will notify the Chief of Police, or designee.

2. Audits to ensure hardware, software applications, and peripherals are compliant with City of Tulsa policy will be conducted at the direction of the Chief of Police. IT personnel may access Tulsa Police Department computers for routine maintenance and to ensure security from external threats. IT personnel shall not view files which may contain investigative details or criminal intelligence unless directed by the Chief of Police.

3. TPD personnel may connect external storage devices to City of Tulsa computers to back up files and move files between City of Tulsa computers. However, due to security concerns external storage devices attached to City of Tulsa computers may never be attached to any non-City of Tulsa owned device.

4. Electronic files concerning criminal investigations or criminal intelligence to be shared with an outside law enforcement agency may only be sent to a government email address. In rare circumstances where a law enforcement agency does not possess a government email account, TPD personnel may send electronic files to the agency via a non-governmental email address (such as gmail, yahoo, or hotmail) with approval of a TPD supervisor. TPD personnel shall not create email groups which contain non-governmental email addresses for the purposes of forwarding periodic crime bulletins or criminal intelligence bulletins to outside law enforcement agencies. Communication not involving criminal investigations or criminal intelligence may be sent to a non-governmental email address.

5. IT will have an automated system in place for verifying TPD passwords and security access. The IT will conduct at a minimum, annual password audits of the Department's information systems.

C. INTERNET

1. Employees are provided internet access to perform official duties for the Tulsa Police Department. Personnel are to give full attention to their duties and are forbidden from engaging in any offensive behavior using City of Tulsa internet access. Any electronic transmission that contains sexual or racial content is prohibited. In addition, any electronic transmission that is political or ideological that could be perceived as offensive by the reader is also

prohibited.

2. Internet access is provided to personnel through the COT network, Wifi, and Broadband devices (such as Mifi Units). As a convenience, police personnel may connect personal devices such as smart phones or tablets to Wifi in TPD facilities and to TPD Mifi units to check personal email accounts or to conduct other personal business. Connection to TPD internet should be brief and must not interfere with duties or TPD business as personnel are expected to give their attention to public safety issues for the City of Tulsa. When connected to any COT internet access, officers may not engage in any offensive communication as outlined in this policy even if using a personal device.

3. Officers may not allow non TPD personnel to use a department issued broadband device (MiFi) to access the internet. Officers are prohibited from using Mifi units to provide internet service to an officer's household or for an officer's personally owned business.

4. Officers are prohibited from using Mifi units to "stream" large amounts of data for entertainment purposes such as movies or gaming.

5. High data usage using Mifi's by the Tulsa Police Department may impact the cost of broadband service. The Headquarters Division will monitor TPD data usage and periodically forward a data usage report to Division commanders. The purpose of the report will be to assist with the management of Mifi data usage to promote efficiency and to control costs.

D. COMPUTERS

1. All transmissions of data and/or queries via computers should be limited to official Department business pertinent to a legitimate and lawful law enforcement function. Inappropriate use of the computer is prohibited. Random audits of computer messages may be conducted by the Department to ensure compliance. Violations could result in termination of the user's National Crime Information Center (NCIC) privileges, OLETS/NLETS service, or access to other law enforcement telecommunications networks.

2. The content of all transmissions via computers shall comply with the same requirements as with voice radio transmissions, which are governed by the FCC and Department policy and procedures. Obscene, derogatory, racial, demeaning, or sexual remarks shall not be transmitted. Computer messages are recorded and may be retained as official records of the Department.

3. Operational instructions regarding mobile computer s (i.e., how to log on, how to run inquiries or commands for operating the mobile computer) must not be broadcast over the radio. This will prevent unauthorized persons who monitor radio frequencies from gaining a working knowledge of the digital system. This does not prohibit giving voice instructions on the appropriate use of the mobile computer to communicate with dispatch or supervisors in a particular situation. Security of the mobile computer is of extreme importance.

4. Any actions which may compromise the security of the system will not be tolerated. This includes visual access by unauthorized personnel or the general public to confidential files (i.e., criminal histories, etc.). Officers will exit or hide all screens which contain confidential information or close their laptops so that unauthorized personnel do not have access. Security of the mobile computer is the responsibility of the officer who is logged on.

5. Officers will be instructed in proper use of the computer before they are authorized to operate the equipment. This training will include log on and log off procedures. Operation manuals will be made available for reference material.

6. All personnel operating a mobile computer will be issued a laptop unit number assigned to a particular officer, police unit number, and VRM. Operators will also be issued a user I.D. number and password for Frontline, OLETS/NCIC, and CADS by the System Administrator. Patrol Officers are required to log on to these systems at

the beginning of each shift. Personnel are responsible for maintaining security of their passwords. Sharing of passwords with another user is expressly prohibited.

7. Dispatchers will continue to advise officers of the call type, nature of the call, and address via the radio. Officers will continue to acknowledge their status via the radio for the benefit of officers/backers without mobile computer accessibility.

8. Officers should report computer system malfunctions immediately to their supervisor and contact the appropriate maintenance personnel. Problems with the VRM or docking station can be addressed by the Radio Shop or the IT. Database problems will be addressed by IT. Report problems to the Service Desk at extension 7070 or email at servicedesk@cityoftulsa.

REGULATIONS:

1. TPD computer hardware shall not be removed from, or added to, the assigned workstation without assistance or prior approval from the IT Department or from an officer with Administrative Access.

2. Employees shall not copy software from a TPD device for use on their personally owned computers.

3. The unauthorized introduction of software programs or other files is strictly prohibited. The manipulation or alteration of current software running on agency-owned mobile, desktop, or handheld computers is strictly prohibited. Software shall only be installed by, or with approval the IT Department or an officer with Administrative Access.

4. All work products that are created on a TPD owned computer or device are considered the property of the Tulsa Police Department.

5. Officers shall not put any information on a TPD computer or device or use any TPD provided internet access that violates Policy 136A, *Performance of Duty - Nondiscrimination* or any materials that are considered obscene or profane.

6. Employees shall not put application passwords or power-on passwords on any Department PC.

7. Email messages are not considered confidential and may be examined upon the authorization of the Chief of Police, or designee and may be subject to Open Records Act.

8. The COT provided internet shall not be used for any illegal, improper, unprofessional, or illicit purposes even if connecting with a personally owned device. The transmission of any material in violation of any city, state, or federal law or regulation is prohibited. This includes, but is not limited to, copyrighted, threatening, or obscene materials, etc., as defined in City policy.

9. Personnel may connect personal devices to TPD internet access via Wifi or Mifi units provided that such connection does not interfere with officer's duties, violate the terms of this policy, or violates any city, state, or federal law.

10. Employees shall not share or give their personal login password to another employee.

11. The CADS and mobile computer messaging system shall be used for business purposes only.

12. The mobile computer shall remain operational during an officer's shift and shall be properly shut down at the conclusion.

13. Mobile computer hardware shall not be removed from the assigned laptop or modified without assistance from the IT Department or an officer with Administrative Rights or prior approval from the officer's Division Commander.

14. Communications and other information accessible by the mobile computer shall not be distributed to the general public.

15. If entering data into the mobile computer compromises safe driving, the task should be delayed until the vehicle is stationary.

16. To ensure confidentiality, officers will exit or hide all screens that contain confidential information so that unauthorized personnel do not have access. Officers will also close their laptop or hide all screens when exiting their vehicle.

17. All police personnel will access their e-mail at least one time daily while on duty, to check for updates and other important information.

18. Before adding hardware or software to a TPD owned computer or device officers with Administrative Access will determine if the hardware or software is authorized.

19. Unauthorized hardware or software will not be installed.

20. After adding or removing hardware/software from or to a TPD owned computer or device, officers with Administrative Access will notify the service desk of the addition or subtraction.

REFERENCES:

106A, *Arrest Warrants*
136A, *Performance of Duty – Nondiscrimination*
318 Attachment, *Use of Departmental Computer Systems – Attachment*
TOG 2017, *Law Enforcement Driving*