FAYETTEVILLE POLICE DEPARTMENT
FAYETTEVILLE, ARKANSAS 72701

GENERAL ORDER # 42

SUBJECT: ***Electronic Communication Policy***

CROSS-REFERENCE: CJIS Security Policy 5.8, Arkansas Code Annotated 14-2-204, IT-03 Electronic and Phone Communications and HR-04 Non-discrimination, Anti-Harassment, and Bullying.

DATE APPROVED BY COP:

PURPOSE: The purpose of this general order is to ensure the proper use of all police computer technology systems. These systems are for the official use of Fayetteville Police Department (FPD) employees and are intended to improve the efficiency and quality of departmental operations. Access to the system permits employees to connect to information resources on a global basis. Each employee has a responsibility to use all types of electronic communication including: The Internet, Mobile Computer Terminal (MCT) and email in a productive manner consistent with a good public image. This general order outlines the minimum requirements for use of email within the FPD network. This general order covers appropriate use of any email sent from a FPD email address and applies to all employees, vendors, and agents operating on behalf of the FPD.

ORDER: Employees of the FPD will follow the procedures outlined below.

DEFINITIONS: Criminal Justice Information (CJI) refers to all data provided to law enforcement agencies via FBI Criminal Justice Information Systems (CJIS) (i.e. ACIC, NCIC, Justice Xchange, etc.) provided during an investigation. This information includes but is not limited to biometric, identity history, biographic, property and case/incident history data.

***PROCEDURES*:**

A. All use of email must be consistent with FPD policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.
    1. FPD email accounts should be used primarily for FPD business-related purposes. Personal communication is permitted on a limited basis, but non FPD related commercial uses are prohibited.
    2. The FPD email system shall not be used for the creation or distribution of any disruptive or offensive messages, including derogatory comments about any person or group of people, either directly or indirectly, based on race, color, sex, religion, age, disability, political beliefs, national origin, or sexual

orientation. Employees who receive any emails with this content from any FPD employee should report the matter to their supervisor immediately.

3. Users are prohibited from forwarding FPD emails that contain criminal justice information (CJI) to a personal third-party email system.
4. Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail, etc. to conduct FPD business, to create or document any binding transactions, to store or retain email on behalf of FPD. Such communications and transactions should be conducted through proper channels using FPD approved documentation.
5. FPD employees shall have no expectation of privacy in anything they store, send or receive on the FPD email system.
6. FPD may monitor messages without prior notice, but the department is not obligated to monitor email messages.
7. FPD employees shall not email criminal justice information (CJI) to anyone outside of the FPD network or to anyone inside of the network that is not Criminal Justice Information System (CJIS) Online certified with a finger-print based background check.
8. When sending CJI via email, users must place the word ENCRYPT in the subject line of the email.
9. All messages created, sent or retrieved by employees over the Internet are the property of the City of Fayetteville, and may be subject to the Arkansas Freedom of Information Act (FOIA), even messages created, sent or retrieved by employees that are thought to be personal.
    a. The FPD reserves the right to access and monitor any or all messages and files on the computer system as deemed necessary and appropriate. Internet messages are public communication and are not private.
    b. An employee should not have any expectation of privacy as to his or her Internet usage while using FPD information technology systems.
    c. Software and systems are in place that can monitor and record all Internet and email usage.
    d. All communications including text images can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver.
10. Multi-factor authentication is required for all devices that connect to the department's email outside the FPD's network.
    a. Employees shall contact the IT Division to upload the required software.

B. Security for Computer System

1. Each employee shall use their own unique User-ID and password when logging onto FPD information technology systems. Employees shall log off all information technology systems when they are no longer in use or lock the computer's screen to prevent unauthorized use.
    a. No employee shall attempt to modify any record or file which would be illegal, or which tends to impair the operation of this department in its administration of justice. No employee shall attempt to delete any file or record contained unless authorized to do so. Attempts to modify or delete

any file or record, which tends to impair the operations of this department, may result in disciplinary action being initiated against the offender.

b. Unauthorized copying or transferring of files from FPD information technology systems to a system outside the police department is strictly prohibited.
   (1) Those employees who have Arkansas Crime Information Center (ACIC) and National Crime Information Center (NCIC) computer system certification shall access those files and records in accordance with specific training.
   (2) Information retrieved from ACIC and NCIC is intended for official police use only and the dissemination of the information to non-criminal justice individuals is strictly prohibited and could subject the offender to criminal penalties.
   (3) Each employee who has ACIC and NCIC computer access must recertify every two years to maintain security authorization. Failure to recertify will result in the employee being required to attend a basic course to obtain re-certification.
   (4) Each employee who has access to Criminal Justice Information shall have CJIS basic security awareness training within six months of initial hire and biennially thereafter.

c. All requests for new programs or applications or the modification of current programs, applications or advanced information searches shall be forwarded through the employee's chain of command to the IT Division.

d. All requests for assistance and/or equipment repair shall be sent to the IT help desk at (479) 575-8367 or email at pditservice@fayetteville-ar.gov.

e. Any supervisor who needs additional training for their employees or any employee who desires computer technology systems training should contact the IT Division to schedule the requested training.

2. The internet will be accessed on department computers for bona fide work purposes and limited personal use.
   a. Sexually explicit material shall not be displayed, archived, stored, distributed, edited or recorded using the FPD's internet, network or computing resources unless tied directly to an investigation or approved training exercise.
   b. Personal usage should not exceed a normal break time.
   c. Use of the internet must not disrupt the operation of the FPD's networks or the network of other users. Users must not knowingly propagate any virus or malicious software.
   d. Copyrighted materials belonging to other entities may not be transmitted by staff on the Internet. One copy of copyrighted material may be downloaded for personal use in research. Users are not permitted to copy, transfer, rename, add or delete programs belonging to other users unless given express permission to do so by the copyright owner.
   e. The City of Fayetteville has installed internet firewalls and Internet security devices to secure the FPD's network. Any attempt to disable,

defeat or circumvent security features will be deemed a serious violation of policy.

C. Mobile Computer Terminals (MCT)
   1. Mobile computer terminals have been installed in police vehicles to assist officers in execution of efficient police functions and to reduce the amount of radio traffic necessary to conduct police operations.
   2. Officers shall log on with their designated User-ID and password. Officers shall not use another officer's User-ID and password. At the end of each shift, officers shall log off the MCT.
   3. Officers have been trained in the use and care of the MCT and are expected to use this equipment in accordance with instruction provided.
      a. Officers should normally use the MCT to check information on persons, vehicles, and other property and refrain from requesting these types of transactions from the Central Dispatch Center (CDC). Officers should utilize CDC for these transactions when an officer needs a printout of the information for inclusion with other reports; the officer does not have access to an MCT, the MCT is not functioning, the mobile interface is down or when officer safety would be compromised.
      b. If the MCT is not working, officers are expected to notify their chain of command and contact the IT Help desk (479) 575-8367 or email at pditservice@fayetteville-ar.gov.
      c. Officers shall keep all CJI from public view when leaving the vehicle or when a person not privy to CJI is in the vehicle to prevent unauthorized users from obtaining confidential information.
   4. MCT's have been programmed to allow for communication of official police business.
      a. No vulgar, obscene, or derogatory messages, racially and or sexually derogatory remarks shall be transmitted via the MCT, nor shall any private, non-police business conversations be conducted on the MCT.
      b. Officers are discouraged from conducting transmissions on the MCT while driving. This does not pertain to two person units with the passenger entering the transactions.
   5. In an effort to ensure employees are using their MCT's in an appropriate manner, patrol supervisors shall monitor MCT transmissions.
      a. Lieutenants assigned to the Patrol Division and the Special Operations Division shall create a quarterly audit of three random officers' MCT use.
      b. The lieutenants shall report the findings of the audits to their captain.

D. Departmental Computers, Tablets and Laptops
   1. The use of all departmental computers and laptops shall have a limited personal use and shall not be used for personal business endeavors.
   2. Personal software shall not be loaded onto any of the department's computers or laptops without the authorization of the IT Division.
   3. No electronic storage devices (i.e. portable hard drives, thumb drives, CD's, etc.) shall be accessed on a FPD computer without being properly scanned for viruses or malicious software.

4. All departmental computers and laptops are inventoried on an annual basis by authorized employees, and all programs on any departmental computer or laptop must be authorized and have appropriate documentation to verify authenticity.
5. The addition or modification of programs or hardware on any departmental computer or laptop must be coordinated through the IT Division.

E. Compliance Measurement
1. A signed copy of the Fayetteville Police Department Employee Internet and E-mail Authorization and Code of Conduct form (page 6 of this general order) must be submitted to the IT Division prior to activating email or internet access for any employee.
2. Upon being issued authorization to use the FPD's internet and email services, each employee will be responsible for all transmissions that occurred under their User-ID. Therefore, each employee must successfully log off before leaving the computer.
3. All inappropriate email or visits to an unauthorized web site during an official investigation or training exercise must be logged in the Prohibited E-mail or Internet Access Ledger. The lieutenant in charge of the Criminal Investigation Division will maintain this ledger. A sample page is included on page 7 of this general order.

Fayetteville Police Department
Employee Internet and E-mail Authorization and Code of Conduct

The employee's supervisor indicating needed access to Internet and E-mail must sign authorization.

_____ _____

Employee Name/# (please print) Supervisor (please print)

Required Access for Internet and E-mail

_____ _____

Supervisor Signature Date

Employee Internet and E-mail Use Acknowledgement

As an employee of the Fayetteville Police Department (FPD), I _____ recognize and understand that the FPD's Internet and E-mail system access are to be used for department business with limited personal use. Furthermore, I agree not to access, retrieve, or disclose stored communications unless prior authorization has been granted. I understand that the content of any e-mail message and Internet usage even during the limited personal use are deemed public information and may be subject to release under the Arkansas Freedom of Information Act.

I am aware that the FPD reserves and will exercise the right to review, audit, intercept, access, and disclose any and all matters on the FPD's e-mail system and internet searches at any time, with or without employee notice, and that such access may occur during or after work hours. I am aware that use of a FPD provided password does not restrict the FPD's right to access electronic communications.

I am aware that violation(s) of the Internet and E-mail conduct may subject me to disciplinary action, up to and including discharge. I acknowledge I have read and understand this policy.

This document will be placed in your personnel file

_____ _____

Employee Signature Date

Prohibited E-mail or Internet Access Ledger

Officer Name/Badge #	Date	Case Number