KANSAS CITY MISSOURI POLICE DEPARTMENT **PROCEDURAL INSTRUCTION**	DATE OF ISSUE 03/25/2020	EFFECTIVE DATE 03/25/2020	NO. 20-02
SUBJECT Personally Identifiable Information (PII)		AMENDS	
REFERENCE PI Computerized Police Information Systems; DM Records Destruction; PPBM Code of Ethics and Rules of Conduct		RESCINDS	

I. INTRODUCTION

A. To establish guidelines regarding the appropriate protocols for the acquisition, use, storage and transmission of PII and "sensitive data" by the Kansas City Missouri Police Department (Department).

B. Public access to these guidelines will also provide notice to the public about the procedures for correction of an individual's PII and sensitive data collected by the Department.

II. TERMINOLOGY

A. **Breach of Security** – Unauthorized access to electronic PII that compromises security, confidentiality or the integrity of personal information maintained by the Department. A breach of security does not include the good faith access to or acquisition of PII by a member, contractor, or vendor for business purposes of the Department.

B. **PII** – Information collected or stored in a program, system, online collection, or other technology that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual, regardless of whether the individual is a United States citizen, lawful permanent resident, visitor to the United States, Department member or contractor. PII does not include publicly available information or information that is lawfully obtained from publicly available sources as allowed by law.

C. **Sensitive Data** – Information that when linked together, could adversely affect the interest or privacy of individuals when such information is lost, modified or acquired through unauthorized access. Sensitive Data generally includes but is not limited to, the following:

1. Date of Birth

2. Social Security Number

3. State Identification or Driver License Number

4. Military Identification Number

5. Credit card information or Card Verification System (CVS)

6. Medical information

7. Bank or credit card account information relating to account numbers or other information that can link an account to a specific individual

8. Juvenile information

III. POLICY

A. The Department is committed to protecting PII and sensitive data from inappropriate access or disclosure consistent with, but not limited to our current written directives entitled, “Computerized Police Information Systems” and “Code of Ethics and Rules of Conduct”, which govern Department members access to and use of confidential information and members’ duty to use such information only for the express purpose of addressing work assignments.

B. These guidelines apply to all Department members who use computers, have network access, communications systems and data controlled, owned, operated or supported by the Department and Department members who may have access to PII and sensitive data collected, maintained and/or transmitted by the Department.

C. Access to a copy of this written directive will be posted on the Department’s external website.

IV. GENERAL INFORMATION

A. Collection and Use of PII

1. The Department collects PII from individuals including but not limited to citizens, vendors, license holders, applicants for employment and employees. This information is collected in electronic and conventional paper format during the course of reasonable and necessary business operations and services.

2. The Department collects and uses PII as part of its business operations. Information is reviewed on a case-by-case basis for PII and pursuant to law before being disclosed, transmitted or otherwise provided outside the Department.

3. Members authorized to have access to PII are committed to protect PII in their respective course of duties. PII may be accessed by, used, and released to those individuals or entities who are authorized by law, policy, duty manual, procedure or contract to use or have access to such information as part of their official duties or contractual obligation, subject to the following requirements:

a. That the information is used only for official purposes; and

b. That the PII is not provided to others contrary to the provisions of this or any other written directives of the Department.

B. Sharing PII with Third Parties

The Department shares PII when required by contract, by local, state, or federal law, regulation, or applicable agency requirement, or when the information relates to sharing information for criminal justice purposes, or with the individual's consent.

C. Correcting PII Information

1. Unless otherwise prohibited by state law, federal law or regulation, an individual who desires to inquire as to what PII has been collected by the Department may request records pursuant to Missouri Sunshine Law through the Custodian of Records or the Office of General Counsel to view or obtain a copy of any information or records collected and maintained by the Department concerning that individual for the purpose of ensuring the accuracy of the information. Valid legal identification will be required.

2. If the information is incorrect or incomplete, an individual may request a correction or an amendment to their own PII that is maintained by the Department, which is not directly accessible to them.

a. The individual may be required to provide a written reason and verifiable written documentation that supports the request to amend any such record.

b. The determination of whether or not to amend records containing PII shall, at all times, be controlled and retained by the Department element creating the record.

c. Nothing herein precludes a Department element from making corrections or changes to Department records in accordance with policy or applicable law.

D. Security Breach

Any member that becomes aware of a breach or imminent breach of PII will immediately notify the Information Technology (IT) help desk. The IT help desk will then immediately contact the Local Area Security Officer (LASO). Further protocol has been set out in the appropriate Duty Manuals.

E. Exceptions

Exception to this written directive may only be made upon specific requests approved by the Chief of Police or designee responsible for such information as specified in this written directive. Any changes will be to the degree necessary to achieve the mission and needs of the Department consistent with federal, state and local law.

Richard C. Smith
Chief of Police

Adopted by the Board of Police Commissioners this __day of_____, 2020.

Nathan Garrett
Board President

DISTRIBUTION: All Department Personnel
Public View Master Index - Internet
Department Master Index - Intranet
Policy Acknowledgement SyStem (PASS)