Policy #	113E	**Effective Date**	10/04/2023
Policy Name	Public Safety Technology and Information	**Approved Date**	10/04/2023
Approved by	*Wendell Franklin, Chief of Police*	**Previous Date**	NEW

PURPOSE OF CHANGE:

New policy.

POLICY:

Public safety technology is a powerful tool that can assist first responders with situational awareness, public safety investigations, and threat prevention. However, the use of such technology also raises ethical and privacy considerations. The Department's policy is to use public safety technology and public safety information in a manner that safeguards the privacy and civil liberties of all individuals.

The Tulsa Police Department will not use public safety technology or its information as a general or indiscriminate tool. The use of public safety technology will be legal, necessary, and proportionate to the objectives, and users are expected to understand and adhere to these standards. Operational procedures for public safety technology will include steps that minimize the collection of irrelevant or unnecessary information and only retain what is directly relevant. Public safety information collected will adhere to retention and disposal schedules, be stored securely, and be protected from unauthorized access, theft, or destruction.

The Tulsa Police Department will be transparent about its use of public safety technology and provide mechanisms to ensure that the technology is being used appropriately. The Department will not use public safety technology to collect information on individuals based on their race, ethnicity, religion, political beliefs, or other protected categories.

SUMMARY: Procedures utilizing public safety technology.

APPLIES TO: All personnel.

DEFINITIONS:

AUTHORIZATION - documented approval granted by the highest-ranking member of the Police Department or their designee, indicating that the use of public safety technology and information is necessary for legitimate public safety purposes.

CIVIL LIBERTIES - fundamental rights and freedoms that are guaranteed to individuals by the Constitution and laws of the United States, including but not limited to the right to privacy, freedom of speech, and freedom from unreasonable search and seizure.

CRIMINAL INTELLIGENCE PRODUCTS – documents, electronic communications, and law enforcement bulletins related to suspected criminal behavior or suspicious activity. Also includes criminal investigation updates created by the Tulsa Police Department or any other Law Enforcement Agency disseminated for the purposes of updating personnel regarding criminal investigations and crime trends, as well as suspected criminal activity and suspicious behavior.

CRIMINAL JUSTICE INFORMATION (CJI) – all FBI CJIS provided data necessary for law enforcement and civil agencies to perform their mission including, but not limited to identity history, biographic, property, and case/incident history data.

CRIMINAL JUSTICE INFORMATION SYSTEMS (CJIS) - mandatory procedures for accessing criminal justice information required by the FBI.

LEGITIMATE PUBLIC SAFETY PURPOSE - any purpose related to a public safety investigation, threat prevention, or threat minimization.

PRIVACY RIGHTS - rights of individuals to control the collection, use, and dissemination of their personal information, including but not limited to information related to their location, communications, and online activity.

PUBLIC SAFETY - protection of the general public from events or actions that could endanger their physical welfare, such as crimes or disasters.

PUBLIC SAFETY INFORMATION - any electronic information collected, captured, recorded, retained, processed, intercepted, analyzed, or shared with public safety technology, including but not limited to video footage, photographs, location information, and social media posts.

PUBLIC SAFETY TECHNOLOGY - any electronic intelligence device, hardware, or software that is capable of collecting, capturing, recording, retaining, processing, intercepting, analyzing, monitoring or sharing audio, visual, digital, location, thermal, biometric, behavioral, or similar information or communications specifically associated with or capable of being associated with, any specific individual or group; or any system, device, or vehicle that is equipped with an electronic intelligence device, hardware, or software.

PUBLIC SAFETY TECHNOLOGY AND/OR INFORMATION - technology and its information deployed for the purposes of enhancing public safety.

PUBLIC SAFETY TECHNOLOGY TYPE - technology and its' information deployed for the purposes of enhancing public safety.

PROCEDURE:

A. AUTHORIZATION

1. Prior to use, all public safety technology or public safety information is recommended by the TPD Technology Committee and approved by the Chief of Police or their designee.

B. SCOPE

1. Public safety technology and information is used for legitimate law enforcement and/or public safety purposes only.

2. The use of public safety technology to gather information on individuals based on their race, ethnicity, religion, political beliefs, or other protected categories is not tolerated and is in direct violation of 136B Prohibition Against Bias-Based Policing.

C. PUBLIC SAFETY INFORMATION MANAGEMENT

1. Access: Access to public safety information is restricted to authorized personnel who have a legitimate public safety purpose and reasonable steps taken to ensure the accuracy of the information.

a. Users accessing public safety technology and information managed by the City of Tulsa have individual login access that is tracked.

2. Collection: Public safety technology and information is used in a manner that respects the rights of all individuals and deployed in a manner that minimizes the collection of information on individuals who are not threats to public safety.

3. Storage: All information obtained by public safety technology is stored in a secure manner.

   a. Information classified as digital evidence is stored in accordance with 113A Digital Evidence Management.

4. Sharing: Requests for public safety information are subject to scrutiny and granted only in accordance with applicable laws and regulations.

   a. Criminal justice information is shared in compliance with 28 CFR Part 23 and 318B Criminal Justice Information Services. Criminal intelligence products are shared in accordance with 105A News Media/Release of Information and marked with a warning indicator such as, but not limited to, "Law Enforcement Sensitive" or "Not for Public Dissemination".

   b. Non-criminal justice information may only be shared with those that need to know (i.e., city officials, fire, EMS) and for legitimate public safety purposes only.

   c. No public safety information shall be sold to any third parties, including private companies or other government agencies.

5. Retention: The retention of information collected through public safety technology is limited to what is necessary to achieve the legitimate public safety purpose. The retention period should be determined based on the type of information collected, the purpose for which it was collected, and any applicable legal requirements.

6. Disposal: Public safety information acquired by TPD owned resources is disposed of in a manner that protects individuals' privacy and civil liberties.

D. TRAINING

1. Personnel working with public safety technology and information are instructed on their proper use in compliance with applicable TPD policy, federal and state laws, the Fourth Amendment to the United States Constitution, and how to report any abuse or illegal access.

REGULATIONS:

1. Gathering public safety information on individuals based on their race, ethnicity, religion, political beliefs, or other protected categories will not be tolerated and is in direct violation of 136B Prohibition Against Bias-Based Policing.

2. Criminal justice information shall be shared in compliance with 28 CFR Part 23 and 318B Criminal Justice Information Services. Non-criminal justice information may only be shared with those that need to know (i.e., city officials, fire, EMS) and for legitimate public safety purposes only.

REFERENCES:

105A, *News Media/Release of Information*
113A, *Digital Evidence Management*
136B, *Prohibition Against Bias-Based Policing*
318B, *Criminal Justice Information Services*
Federal Regulation 28 CFR Part 23, *Criminal Intelligence Systems Operating Policies*