3-01/005.05 - Artificial Intelligence (AI)

Definition of Terms Related to Artificial Intelligence (AI)

This policy adopts the definitions below, which are defined by California law.

Artificial Intelligence (AI) – California Government Code Section 11546.45.5 defines AI as an engineered or machine-based system that varies in its level of autonomy and that can, for explicit or implicit objectives, infer from the input it receives how to generate outputs that can influence physical or virtual environments. There is also a more specific definition of AI in Penal Code Section 13663 that applies in relation to the use of artificial intelligence in report writing as noted in more detail below.

Generative Artificial Intelligence (GenAI) – California Government Code Section 11549.64 defines GenAI as an artificial intelligence system that can generate derived synthetic content, including text, images, video, and audio that emulates the structure and characteristics of the system's training data.

Automated decision system – California Government Code Section 11546.45.5 defines an automated decision system as a computational process derived from machine learning, statistical modeling, data analytics, or artificial intelligence that issues simplified output, including a score, classification, or recommendation, that is used to assist or replace human discretionary decision making and materially impacts natural persons. "Automated decision system" does not include a spam email filter, firewall, antivirus software, identity and access management tools, calculator, database, dataset, or other compilation of data.

Large Language Models (LLM) – LLMs are a subset of GenAI. They are advanced natural language processing models powered by AI. They are designed to generate human-like text responses, based on the input they receive.

Speech-to-text (STT) – STT is a type of AI technology that converts spoken language into written text by recognizing and transcribing audio into text format.

Text-to-Speech systems (TTS) – TTS is a type of AI technology designed to transform written text into spoken language.

Voice cloning or voice synthesis systems – Programs that learn the characteristics of an individual's voice by processing audio data collected from audio samples and produce new speech that sounds exactly like the original speaker.

Purpose

The policy promotes the authorized and responsible use of artificial intelligence to strengthen public safety, protect officer safety, improve investigations, increase efficiency, and expand accessibility.

Accountability of Artificial Intelligence

The Department's acquisition, deployment, implementation, and use of AI technologies must comply with Departmental ethical standards and must be used in a manner that upholds constitutional rights, protects privacy, avoids bias, ensures accuracy, and follows legal guidelines and requirements. All users have a legal

duty to safeguard personal information of the public and their privacy.

AI may assist with workload, information processing, drafting of documents, data analysis, and recommendations but human authority, independent judgment, verification, and accountability do not transfer to an AI system.

The guiding principles for Department use of AI systems include the following:

- Legal and Civil Rights: All Department use will comply with the United States Constitution, California state law, federal law, and California Department of Justice guidelines.
- Fairness and non-discrimination: All systems implemented by the Department will be reviewed for potential disparate impact on race, ethnicity, gender, and other protected classes.
- Human Oversight: A human shall oversee and be responsible for all outputs. AI use will not include fully automated decision-making regarding arrests, use of force, or liberty restrictions.
- Transparency: AI use will be publicly disclosed when required by law. If not legally required, AI use will be disclosed when feasible without compromising investigations or privacy rights.
    - To ensure the Department maintains transparency with the public, both planned and random audits will be conducted to monitor the use of these technologies.

Prohibited Use

Department members are prohibited from inputting non-public, confidential, sensitive, personally identifiable, investigative, or otherwise protected information into public AI platforms. Public AI platforms present significant risks related to unauthorized disclosure of information, infringement of privacy rights, and data loss. Information entered into a public AI platform may be retained, disclosed, or otherwise become accessible outside of Department control.

> **Note**: For purposes of this policy a public AI platform is defined as any AI tool or service without a Department approved Data Processing Agreement (DPA) that guarantees tenant-isolated storage, prohibits the use of inputs for model training, and maintains full compliance with CJIS and California law enforcement data standards.

The input of sensitive, confidential, or private information to a public AI platform is strictly prohibited, regardless of device used. Non-public, sensitive, confidential, or private information may include, but is not limited to:

- Department member personal information, including personnel records as defined by Penal Code Section 832.7.
- Protected Health Information (PHI)
    - Medical records
    - Mental health information
    - Substance abuse treatment data
- Non-public Personal Identifying Information (PII)
    - Social Security Numbers (SSNs)
    - Biometric data (e.g., fingerprints, facial recognition, etc.)

- CA Law Enforcement Telecommunication System (CLETS) derived information
    - Criminal history record information (CHRI)
    - Criminal Justice Information (CJI)
    - Arrest, booking, and incident reports
    - Surveillance data
    - Case file content
    - Investigative notes
- Department or County financial information that is not already publicly available or published.
- Passwords
- Confidential information including, but not limited to, incident reports, witness statements, probable cause affidavits, as this confidential information includes:
    - Names or aliases of informants
        - Contact information
        - Payment or support details
        - Notes on informant credibility
        - Witness statements or identities
    - Operational or strategic data
        - Details of ongoing investigations
        - Warrant service or arrest planning
        - Undercover officer identities
        - Surveillance targets or tactics
        - Sensitive law enforcement procedures
    - Classified or sensitive government Information
        - Intelligence briefings or inter-agency communications
        - Federal or national security data
        - Any Law Enforcement Sensitive (LES) content
    - Juvenile justice information
        - Names or identifiers of juveniles
        - Juvenile detention or probation records
    - Court-sealed or protected content
        - Sealed records or court restricted evidence
        - Witness protection program details
        - Testimonies under protective order
- Attorney-client privileged communications
    - Legal advice between agency legal counsel and staff
    - Internal legal memoranda
    - Notes or summaries of legal strategy or litigation plans
    - Emails exchanged with legal counsel

  - Deposition transcripts.
  - Documents prepared in anticipation of litigation
- Departmental forms or templates
  - Unreleased or draft SOPs (standard operating procedures)
  - Confidential personnel forms (e.g., disciplinary records, evaluations)
  - Internal use-only documentation (e.g., field interview cards, incident worksheets)
  - Specialized or restricted-use checklists

In addition, the creation of any Application Programming Interface (API) with a public AI platform requires prior Data Systems Bureau approval.

The unauthorized use of AI to generate fake or misleading images, audio, or video is strictly prohibited. The generation of such content may be authorized pursuant to the terms of this policy only in limited circumstances, including, but not limited to, use in training scenarios or for use in computer-assisted development of demonstrative evidence and age progression programs.

The provisions of this policy apply to all Department devices and to any content created on personal devices (e.g., computers, cell phones, laptops) when personnel are using any form of AI to work on a Department project or prepare Department work product.

If a Department member enters prohibited information into a public AI platform, the member shall provide written notification to a supervisor and via a Helpdesk ticket as soon as practicable. If a supervisor is notified of any entry of prohibited information to a public platform, that supervisor shall report the incident to Data Systems Bureau (DSB) in writing.

Authorized Use of Artificial Intelligence Technology – Generally

Department members shall only use Department authorized AI products or tools for Department business that includes confidential, sensitive, or private information. A list of authorized AI products will be posted on the Department's intranet and updated by Technology Support Division when any new tool, software, or system is procured and approved for Department use.

Before procuring or deploying any new AI tool or system, written approval must be obtained from the Assistant Sheriff/Chief Financial & Administrative Officer or their designees. The evaluation conducted will, at minimum, consider the legal, security, operational, and civil rights issues involved in the acquisition and use of that vendor, tool, or system. A pre-deployment risk assessment shall be required for all AI systems.

Further, to ensure compliance with Penal Code Section 13662, the Assistant Sheriff will ensure that all contracts for these services prohibit the resale of Department data and prohibit the transfer of data to the federal government unless permitted by law, limit vendor access to the minimum amount necessary for the proper functioning of the product, and ensure the data is not utilized for model training.

Whether using a public AI platform or a Department authorized AI product, members must review and verify AI outputs. AI tools may generate information that is inaccurate or use offensive or derogatory language. Department members must review any output generated for accuracy and for bias including but not limited to any derogatory references based on race, ethnicity, age, or background.

When using any AI-based technology, Department members shall comply with all Departmental ethical standards and expectations for behavior, just as they are required to follow in other areas or activities under control of the Department. All applicable Department policies that provide direction for member behavior and responsibilities shall be applicable when using AI technology.

This policy does not prohibit Technology & Support Division from implementing authorized AI-enabled data security systems designed to protect Department systems, infrastructure, and data.

Use of Artificial Intelligence Technology – Report Writing

Penal Code Section 13663 significantly impacts the manner in which Department employees are permitted to write reports with the assistance of AI. Department members are reminded that they are responsible for the contents of any official report they generate. (See also MPP 3-01/005.10 – Responsibility for Documentation.)

Definition:

Penal Code Section 13663 defines AI as follows:

> "Artificial intelligence" as used in this section applies to artificial intelligence systems that automatically draft police report narratives based upon an analysis of in-car or dash-mounted cameras, or body-worn camera audio or video, and artificial intelligence systems that analyze a law enforcement officer's dictated report to generate a police report narrative automatically enhanced by generative artificial intelligence.
>
> **Note:** This definition is narrower than Government Code Section 11546.45.5 as it is specific to this statute and to the use of artificial intelligence technology in the generation of police report narratives.

If AI is used - fully or partially - to generate an official report by any member of the Department, that Department member shall:

- Clearly identify every AI program used in the official report.
- Prominently state on each page of the report: "This report was written either fully or in part using artificial intelligence."
- Include the author's physical or electronic signature attesting that they have reviewed and verified the contents and accuracy of the report.
- Retain the first AI-generated draft of the report for the same duration as the official report.
- Recognize that any AI-generated draft (other than the final signed report) cannot be considered an officer's statement.

The Department will maintain an audit trail identifying:

- The person who used AI to create the draft or report.
- Any audio/video footage used by the AI (e.g., BWC, dash cam).

Department members who are procuring or managing AI products shall ensure compliance with the mandates of California Penal Code section 13663:

- AI vendors cannot share, sell, or use agency-provided information for any purpose other than the agency's needs or pursuant to a court order.
- Vendors may access data only for technical reasons (e.g., troubleshooting, bias mitigation, accuracy improvements).

CJIS Compliance Requirements for AI Systems

Any AI system used by Department members that processes, stores, transmits, or has access to Criminal Justice Information (CJI) as defined by the FBI CJIS Security Policy must comply with all applicable CJIS Security Policy requirements.

Training and Awareness Requirements

Prior to the use of any Department-authorized AI system, all Department members will familiarize themselves with this policy and shall complete any Department required training on its use. Members assigned to procure, manage, or evaluate AI systems shall complete supplemental training on AI risk assessment methodology as directed.

Disclosure and Transparency

To further promote public trust and transparency the Department shall annually review and report on the use of artificial intelligence technology. The Department shall host these reports on our public web page describing the use of these products throughout the Department.