

# APPENDIX A

## Prosecutors' Center for Excellence AI POLICY TEMPLATE

### INTRODUCTION

Artificial Intelligence (AI) is a valuable tool that is rapidly becoming integrated into our work. AI has many potential benefits, but it also presents ethical and legal concerns for prosecutors. Before implementing AI tools, we need to consider all of these implications. Of primary concern is that improper use of AI tools can make public otherwise confidential case-related information; can endanger victims, witnesses, and the integrity of our cases; and can expose our lawyers to violations of the ethical rules. This document's goal is to help ensure our office implements AI tools responsibly.

### BACKGROUND ON AI

AI refers to a machine-based system that can make predictions, recommendations, or decisions. AI systems use machine and human-based inputs to perceive environments, abstract such perceptions into models through automated analysis, and use model inference to formulate options.

AI is being integrated into applications and programs used by prosecutors and law enforcement at a rapid rate. AI based on "machine learning" has been present in criminal justice work for some time. With machine learning, algorithms are designed to detect patterns and predict outcomes. Examples include risk assessment tools used in setting bail and algorithms used for fingerprint and DNA analysis. New forms of AI continue to emerge, including generative AI (GAI), which uses Large Language Models (massive inputs of data, including textual, audio, graphic, and video) to produce coherent, unique answers and written material in response to human queries. ChatGPT is an example of a GAI program.

### AI AND PROSECUTION: IMPORTANT CONSIDERATIONS

This policy addresses three types of AI tools relevant to our work:

- 1) AI tools that are currently embedded in existing office-approved programs. AI tools are now embedded into websites and applications that you may use every day. This means that office programs we have been using for years may require us to consider whether and how they can be used in light of newly introduced AI features.
- 2) Publicly available AI tools. Numerous GAI tools are available to the public online. These tools are typically free, chat-based systems in which users can feed the program questions, textual data, audio, graphics, or videos and request analytical or generative output.



- 3) AI tools that the office and our criminal justice partners may acquire, including tools being developed specifically for prosecutors and law enforcement. AI tools designed to assist lawyers and law enforcement are quickly coming on the market. Our office, the courts, law enforcement agencies, and other criminal justice partners may now integrate these tools into their work.
- 4) [IF APPLICABLE] In-house AI tools developed by the office. The office is working with its IT staff and service providers to develop AI tools specifically for our use. These tools will rely on internal office data and assist staff with various office needs and tasks.

Each set of AI tools presents its own set of issues and risks. Before you use any AI tools for work-related projects, you must exercise caution and consider what kind of information you are providing the AI tool. This policy relates mainly to GAI tools, but many of the concerns raised about the use of GAI are relevant to other forms of AI. Employees must bear this in mind whenever they are using an application or program in which AI has been integrated. **If you have questions about whether the use of a particular AI tool is problematic, seek help before using it.**

As AI tools and platforms continue to develop, the Office recognizes that these tools and platforms represent innovation that may improve our efficiency, transparency, and our ability to serve the public. However, we also recognize that our duties of competence and confidentiality are paramount and must adhere to the legal and ethical rules that govern our work.

In light of these concerns, we must always be sensitive to several issues in our use of AI, including:

- Confidentiality – We must ensure that the confidential data and materials – such as case and witness details, evidence, and work product – are not improperly disclosed by using an AI tool. Some AI tools may absorb and utilize inputted information to train its AI model, or to answer the questions of future users. This possibility raises serious concerns, as much of the information and data our office gathers, receives, and creates is confidential, and disclosure may be prohibited by statute, ethical provision, or other governing body. **A determination must be made about what data can safely be entered into a specific AI tool before you use it.**
- Human oversight required – AI is an aid to us as a prosecutor office, not a replacement for human judgment, especially in making final decisions about cases. AI tools are not inherently unreliable. They can pick up misinformation and use it to generate convincing but false or erroneous responses, a phenomenon called “hallucination.” Because we are ultimately responsible for our work, **employees must review all AI output for accuracy and reliability.**
- Transparency – Our use of AI should be explainable and transparent. We must be prepared to disclose to the court and the defense when AI tools are being used and for what purposes.
- Data Privacy and Security – All sensitive data must be handled securely and in a manner that does not lead to the potential compromise of office data, systems, and networks. Certain types of data – such as personal identifiers, victim information, medical treatment



information, and criminal histories – may have specific legal protections. **Extra care must be given when handling sensitive information using AI tools.**

- Supervision and Accountability – Supervisors within the office are responsible for ensuring staff members are using AI tools appropriately and in accordance with office policies. Employees using AI tools improperly will face supervisory action.
- Bias Mitigation – We must take steps to mitigate the risk of bias in our use of AI, which may include periodic audits and validation testing to ensure fairness across demographics.
- Feedback – We must be receptive to feedback from judges, defense attorneys, our law enforcement partners and the community about our use of AI, so that we can improve fairness and ensure public accountability.

## OFFICE USE OF AI

Based on the above considerations, this section outlines the acceptable use of AI tools for conducting office work. Attorneys and non-legal staff may use only those AI tools that have been vetted and approved by the Office. Publicly available tools may not provide the necessary security, and information entered into such tools could compromise the confidentiality of our work and our cases.

**Attorneys and non-legal staff are NOT PERMITTED to do the following:**

- **Use publicly available AI tools for any work-related function.** To the extent that you have downloaded any such tools to your office computer or device, you must delete them. Nor may you use such AI tools on your personal devices for any work-related function.

Publicly available tools include:

- ChatGPT
- Gemini (formerly Bard)
- Grammarly
- GoogleTranslate
- DALL-E
- DeepAI
- AlphaCode
- Q Developer
- OpenAI
- *[OFFICES MAY WISH TO ADD OTHER TOOLS TO THIS LIST]*



*[IF APPLICABLE, SOME OFFICES MAY WISH TO LIST PERMITTED USES OF PUBLICLY AVAILABLE AI TOOLS AS EXCEPTIONS, SUCH AS:*

The following uses of publicly available AI tools are permitted:

- Google Translate or Zoom/Teams for translations that do not involve the input of confidential information (see below definition), such as directions to the office or a request for a meeting.
- Online map applications to search for locations relevant to prosecutions.]
- Translation and transcription services that are produced in a “closed” AI system that does not leak information into the internet.

### **Consult A Supervisor Before Using Any Online AI Tool To Determine If Its Use Is Permitted.**

- **Enter any confidential information into any publicly available software, applications, and chatbots, regardless of whether they use AI**, unless the software, application, or chatbot has been installed by the IT department for that specific purpose. This prohibition includes, but is not limited to, ChatGPT, grammar checkers such as Grammarly, translation assistants such as GoogleTranslate, etc.

“Confidential information” includes details of an investigation or case, evidence, witness information, criminal history information, and other personal identifying information.<sup>6</sup> It also includes confidential information pertaining to office employees, office policies, and programs. Nor can you endeavor to “anonymize” such confidential data by, for example, changing the names or posing a question using the fact pattern of your case hypothetically.

- **Use any publicly available AI tools to analyze digital evidence**, including but not limited to cellphone, computer, or social media records, or any information obtained via subpoena or search warrant.
- **Rely upon AI in forming legal conclusions or advice**, or rely upon it as a credible source or citation in any court filings or representations to the court or defense counsel. AI may be used to do legal research, as long as the results are verified.
- **Use AI programs to write codes, scripts, or queries** or use programs such as DALL-E to generate photo-realistic images.

---

<sup>6</sup>For purposes of this policy, “Personal Identifying Information” means a person’s name, address, telephone number, driver’s license number, social security number, credit card number, bank account number, or any other unique identifier or number that could be used to discover the identity of the person.



- *[IF OFFICE ISSUES DEVICES TO STAFF]* **Download AI tools onto work computers, laptops, or cell phones.** You must delete any AI tools you may already have downloaded on these devices.
- **Use AI programs on personal devices to perform work in a manner inconsistent with this policy.** Employees must follow the office's policies on the use of AI tools when using personal phones, computers, and other devices to conduct office work.
- **Rely upon AI to produce the final version of any letters, reports, policies, or any other document.** All AI output must be reviewed and verified.

**Attorneys and non-legal staff are PERMITTED to do the following provided:**

- **Your responsibility.** The use of any office-approved AI application or AI program does not negate or undermine your responsibility to make an informed decision about if and how to use the output of an AI application or AI program. For example, if you use an office-approved AI program to summarize the contents of a case file, you must still determine if that summary is accurate and useful for decision-making and comports with the standards of professional conduct required of all employees. You, not the AI program, are responsible for the decisions that flow from an AI-generated work product.
- **Consult a supervisor** before using these tools or if you have any questions about permitted use. *OR* To use these tools, you must attend/view the introductory training module.

**Permitted Uses:**

- **Use AI features embedded in MS Office, Adobe, and case management programs.** Employees may use AI features embedded in these existing office programs installed on an office device. *[SPECIFY ADDITIONAL PROGRAMS AS NEEDED]*
- **Use videoconferencing platforms with AI features to communicate.** You may also use communication platforms such as *[CHOOSE APPLICABLE]* Zoom and Microsoft Teams to communicate with witnesses, victims, defense attorneys, etc. However, you may not use the translation features on these platforms to conduct witness interviews, nor may you generate transcripts of your conversations on these platforms for any case-related work. Likewise, you should not allow any parties to the meeting to do so.
- **Use VLex in Lexis and CoCounsel in Westlaw to conduct legal research.** However, all research results must be independently verified. Confidential information may not be inputted into VLex or CoCounsel. *[CHOOSE OR ADD APPLICABLE LEGAL RESEARCH PROGRAM]*
- **Use AI tools specifically acquired by the office.** The Office has procured the following AI tools to assist with our work:



- Whisper (translation tool)
- *LIST OTHER APPLICABLE TOOLS*

OR

The Office has not yet procured any AI tools. We will continue to update you when we do so and will provide further guidance at that time.

- *[IF APPLICABLE]* **Use AI tools developed internally by the office.** The office has developed certain AI tools specifically for our internal use. You may use these tools for their designated purposes.
- **Evaluate law enforcement use of AI tools.** Local law enforcement agencies *[NAME AGENCY OR AGENCIES]* is currently using an AI tool(s) for the following purpose:
  - Identifying suspects using facial recognition
  - Identifying vehicles using license plate readers
  - Drafting police reports
  - *[NAME OTHER RELEVANT PURPOSES]*

If, in reviewing a case for prosecution, you become aware that law enforcement has used an AI application or AI program as part of the investigation, you must determine that the information produced by the AI application or AI program is accurate. For example, if a law enforcement agency used facial recognition software to identify a suspect, you must review the evidence and determine that there is sufficient information proving the person being charged is indeed the same person that the facial recognition software identified. You may be required to disclose to the defense and to the court that AI was used for these purposes.

*[IF APPLICABLE]* The office does not accept cases involving the use of the following AI tools:

- *LIST PROHIBITED AI TOOLS HERE*

## POLICY UPDATES

Please be aware that our AI policies may change, based on our experience and how new tools evolve. Rapid changes in technology will require us to monitor continuously whether our policies continue to serve us well, and we will need to adjust. We issue this guidance, and the policies outlined above to protect our staff and maintain the confidentiality of information in our possession.

