

## **OSPCC Use of Artificial Intelligence and Large Learning Models**

### **1.0 Use of Artificial Intelligence and Large Learning Models**

- 1.1 Artificial Intelligence (AI) and Large Learning Models (LLM) technology are embedded in many of our everyday activities. It is rapidly becoming part of operational systems used in policing and public safety. You can use AI / LLM (hereafter referred to as just LLM) within your role, however you must be aware that there are stipulations in place. This includes restrictions on the specific LLM provider and limitations on the information you can input. Currently the LLM providers approved by the force are limited to CoPilot, Gemini and ChatGPT.
- 1.2 This document is intended to support you when using LLM for law enforcement purposes and to offer advice when attending partnership meetings where LLM is being used for transcription purposes.
- 1.3 Whilst LLM are widely used in our personal lives, there is a necessity to make a clear distinction with regards its use in operational policing and the potential consequences for breaching Force Policy and potentially Data Protection legislation. This guidance and Force documents will support risk-based decisions to influence and advise on the safe processing of data whilst using LLM.
- 1.4 If you have any questions about the use of LLM within your role, please firstly review the Artificial Intelligence Policy Surrey and Sussex (1236) and Intranet pages. If you have questions / concerns, then email Iain McCulloch.

### **2.0 Use of Large Learning Models in Policing**

- 2.1 The information processed through LLM requires tighter controls and is subject to enhanced scrutiny by members of the public. There are strict expectations on how we manage data, which includes processing using any third-party software. Any processing utilising LLM software is subject to restrictions that must be followed by all staff.
- 2.2 Staff must not use an LLM unless they possess sufficient information and expertise to understand, use and explain the technology and its appropriateness for the purpose intended. If you lack sufficient understanding to explain the technology or its appropriateness, you must not use it for professional activities.
- 2.3 An intranet page has been created to provide support with any questions you might have: Information Security Guidance Hub – AI Guidance (this guidance is not to be shared externally). The How Do I page outlines specific restrictions when utilising LLM in your role. Before you enter any information into LLM you must be cognisant of the fact that this is law enforcement data processed under the UK GDPR and / or Part 3 of the Data Protection Act 2018 (hereafter referred to as Data Protection legislation), therefore is it considered more sensitive and has serious implications if it is incorrectly entered into these systems.

- 2.4 Processing through this technology is for efficiency / expediency and not necessity. It is therefore vital to remember that if incorrectly processed, this information would be in the public domain and therefore accessible / reused by certain LLM technologies to support its learning.
- 2.5 In support of the Information Security guidance, please ensure the below steps are strictly adhered to:
- It is your responsibility to confirm that the specific LLM is authorised using the guidance on the Information Security Guidance Hub - AI Guidance page.
  - Do not enter personally identifiable information (e.g. names, DoB, VRM, IP addresses, etc) into any LLM. Always anonymise your search parameters, for example Person 1, Suspect, last four digits, etc.
  - Do not use LLM to produce statements for a law enforcement purpose. LLM have not been approved for this purpose.
  - Once a response is extracted from the LLM, the user will need to manually review and amend.
  - Only use ChatGPT or CoPilot if you are producing non-operational documents - for example, training materials.
  - Only use Gemini for targeted questions – for example, researching legislation, employment related questions, etc.
  - Outputs from LLM often contain fabricated information, it is essential that all outputs are assumed not to be accurate.
  - It is your responsibility to validate and fact-check all responses and you must not treat them as authoritative sources.
  - Only use work devices (laptop, MDT) when processing law enforcement data into LLM. Any processing of this data on personal devices is a data breach and will be investigated and reported where necessary.
  - The principle of confidentiality requires taking all reasonable steps to preserve the confidentiality of information. In addition to PII, users should adopt the safe and proper approach of assuming that all unpublished information about the Force's affairs is confidential and should not be entered into an LLM.
  - Users must explicitly guard against "automation bias," which is the tendency to favour output generated from automated systems even when human reasoning or contradictory information raises questions about its reliability.
  - When manually reviewing outputs, apply an "inquiring mind". This involves considering the source, relevance, and sufficiency of the information, and specifically considering if the source of the AI's training data might be influenced by bias or if relevant information is missing.
  - When preparing information using LLM outputs, you must exercise discretion to ensure you do not omit anything with the intention of rendering the information misleading or influencing regulatory outcomes inappropriately.
  - To ensure accountability, users are encouraged to document the facts, the courses of action considered, the specific prompts used, and the verification steps taken when using LLM to support a decision.
- 2.6 Whilst appreciative that this new technology can support you, the above is essential before any use of LLM. Police process vast amounts of information about members of the public and as such we face greater scrutiny, not to mention the potential for fines from the Information Commissioners Office.

### 3.0 Use of LLM Transcription in Multi Agency Meetings:

- 3.1 Partner agencies (including NHS, Local Authorities, etc) have informed the Police that they are testing the use of LLM technology to transcribe meeting audio into written format. Whilst this is similar to transcription using MS Teams, it carries serious concerns and caveats.
- 3.2 We must accept that the chair of the meeting has carried out the necessary due diligence with their Information Security and Information Governance teams. However, as Data Controller it is ultimately our decision whether we share personal data (this can also be exercised by the partner agencies at Police led meetings).
- 3.3 As with all processing utilising an LLM, the outputs are not an accurate representation of what was discussed. It is therefore essential that any minutes generated through an LLM are assumed to be inaccurate and require your review. It is your responsibility to validate and fact-check all information identified as being shared by you. The minutes could be disclosable under Freedom of Information (FoI) or Subject Access Rights (SAR), so it is essential to ensure their accuracy.
- 3.4 As gatekeeper for policing information, you are entitled to ask about the LLM being used. If you are informed prior to the meeting, please consult with your Information Management team.
- 3.5 Prior to any disclosures at meetings, please verify:
  - the provider of the LLM transcription software?  
**The provider must use either ChatGPT, CoPilot or Gemini to support its LLM. If this is not the case, then as per the AI policy and flow chart, you should not share information.**
  - that the LLM will not retain a copy of this information?  
**The LLM must only be used to transcribe, under no circumstance should it retain any copies. All copies of the transcript must be deleted from the LLM as soon as the minutes / transcription has been exported by the lead agency.**
  - that the LLM will not use this information as part of its learning?  
**It must be confirmed that in support of the above, no data is retained by the LLM to influence its learning.**
  - that the LLM has been assured by your Information Security and Information Management teams?  
**This should always be a 'yes', however it is necessary to ensure as this should have resolved the above processing concerns in their Risk Assessment and Data Protection Impact Assessment.**
- 3.6 If you are not entirely satisfied, or they have answered 'no' to any of the above, you must not share any information which is operationally sensitive or is the identifiable personal data of any victim, suspect or other associated person. The mitigations will support you if you are not comfortable sharing:
  - You can state that "To ensure necessary protections of data processed under Data Protection legislation, I request the transcription software be paused and I will provide a written statement for inclusion in the minutes".

- You can anonymise the information given by stating 'Offender', 'Suspect 1', etc. Whilst the data subject will be indirectly identifiable from the other partner updates, any potential data breach through a non-compliant LLM will be their responsibility.
- If the transcription software cannot be paused and / or data cannot be anonymised, give the following statement: 'I have been advised that to ensure compliance with the Artificial Intelligence Policy Surrey and Sussex (1236) and data protection legislation, additional reassurances are needed before personal / criminal data can be transcribed through your chosen LLM. I will provide a written disclosure to support the minutes of this meeting.'

#### **4.0 Sources**

4.1 The following sources have been used to create this document:

- *Artificial Intelligence Policy Surrey and Sussex (1236/2024)*  
<https://www.sussex.police.uk/SysSiteAssets/foi-media/sussex/policies/artificial-intelligence-policy-surrey-and-sussex-1236.pdf>
- *Institute of Chartered Accountants in England and Wales (ICAEW) Code of Ethics 2025*  
<https://www.icaew.com/-/media/corporate/files/technical/ethics/code-of-ethics/icaew-code-of-ethics-2025.ashx>