

OSPCC Use of Artificial Intelligence

1.0 What is AI?

- 1.1 Artificial Intelligence (AI) is simply the ability of computer systems to perform tasks that typically require human intelligence.
- 1.2 In practical terms, AI systems can recognise patterns, learn from data, make predictions, and even understand or generate text, images, or speech. Without realising it, we are using AI every day, from Siri or Alexa, spam filters in our emails, facial recognition on smartphones to chatbots that answer questions online.

2.0 From simple to sophisticated

- 2.1 AI is not one single technology; it covers a wide range, from relatively simple automation to advanced models capable of complex reasoning. Here are some of the main types of AI you will come across:
 - 2.1.1 Rule-Based AI – Follows pre-programmed rules or "if-then" logic [i.e. an access control system that blocks a card if it is reported lost]
 - 2.1.2 Machine Learning – Learns patterns from data rather than explicit rules [i.e. identifying suspicious financial transactions based on past examples]
 - 2.1.3 Deep Learning – A form of machine learning inspired by the human brain, good at recognising complex patterns in large amounts of data [i.e. facial recognition, voice analysis, etc.]
 - 2.1.4 Generative AI – AI that can create new content — text, images, audio or video [i.e. tools like ChatGPT (for text) or image generators fall into this category]
- 2.2 These systems learn from huge datasets and can produce realistic outputs but may also produce inaccurate or misleading information if unchecked.

3.0 Use of AI within policing

- 3.1 We know that AI is already part of many everyday activities and it is rapidly becoming part of operational systems used in policing and public safety. You are able to use versions of AI within Sussex Police and Surrey Police, including CoPilot, Gemini and ChatGPT, with rules in place.
- 3.2 To assist you to figure out how AI can help you day-to-day, a decision flow chart has been created on the following page for you to use whenever you are wanting to use this technology.

AI Decision Flow - Appendix

This document supports the Surrey & Sussex Police AI Decision Flowchart. It explains each step in the flow, offers examples, and provides references to national policy and legislation.

Pre-requisite checks

Prior to using AI it is essential that you are able to confirm that you:

- Have completed the mandatory College Learn (NCALT) “Managing Information” (operational/Non-operational) assessment in the last 12 months. The course covers the safe handling and processing of data. The use of AI for professional purposes without completing the training may result in a policy breach and could trigger a review by Information Management
- Will be using one of the force approved AI tools on a work-issued device or Force-approved systems.
- Approved tools are limited to: ChatGPT (<https://chat.openai.com>), Gemini (<https://gemini.google.com>), and Microsoft Copilot (<https://m365.cloud.microsoft/chat/>). Only browser-based versions should be used.

If you are not able to confirm the above you should STOP until these pre-requisites have been satisfied.

If Yes: Proceed to Step 1.

Reference: AI Policy 11.2

Step 1: Is the purpose of using AI to complete assignments, essays, or exam responses?

AI must not be used to generate original content for assessed academic, promotional, or professional development work — including internal training, coursework, or accredited qualifications.

However, AI may support you by:

- Helping structure reflective writing, if the insights remain your own.
- Improving grammar and clarity in your own draft.
- Acting as a research tool (note: verify facts — AI can be wrong).

Misuse may breach academic or professional standards. If unsure, speak to your line manager or Learning & Development lead.

If Yes: STOP. You must NOT proceed. Seek advice from your line manager or L&D lead if unclear.

If No: Move to Step 2.

Reference: AI Policy 11.4

Step 2: Does the input include ANY personal data (e.g., names, DOBs, identifiers) or sensitive categories such as race, gender, or health?

Personal data means any information relating to an identified or identifiable living person. This is someone who can be identified, directly or indirectly, by identifiers such as a name, badge number, vehicle index, location data and online identifiers (IP address, email, etc.). Special / Sensitive Category Data and Law Enforcement Data are particularly sensitive and require stricter controls. Examples:

- Including a victim, Witness or suspect’s name, address, VRM or DOB in a prompt
- Describing an officer’s shift pattern or vehicle assignment
- Uploading a document with arrest records or interview transcripts

If Yes: STOP. Consult the Force Information Management Team. Do NOT proceed until authorised.

If No: Proceed to Step 3.

Reference: AI Policy 5.1, 11.2 | UK GDPR Articles 4, 5, 9

AI Decision Flow – Appendix (continued)

Step 3: Does the input contain Operational or Sensitive Police Data?

Operational/sensitive data includes material relating to law enforcement that is not public. This includes tactics, intelligence, live operations, or system details. Examples:

- Describing covert operation methods
- Referring to suspect profiles or surveillance plans
- Summarising internal risk assessments

If Yes: **STOP**. Consult Information Assurance. Risk assessment required.

If No: Proceed to Step 4.

Reference: AI Policy 11.2

Step 4: Is the data classified as OFFICIAL-SENSITIVE or higher?

Government Security Classification levels above OFFICIAL (e.g., OFFICIAL-SENSITIVE, SECRET) require special handling and must not be shared in unapproved tools. Examples:

- Witness statements, or information obtained from other partners that has been classified as Official Sensitive
- Intelligence logs on organised crime groups
- Counter-terrorism operation data

If Yes: **STOP**. Consult Information Assurance.

If No: Proceed to Step 5.

Reference: GSC Guidance

Step 5: Could the AI output be used to support operational decision-making or create Criminal Justice (CJ) documents?

AI outputs that influence operational decisions or CJ files must be fully auditable, reviewed, and not relied upon without sign-off. Examples:

- Using AI to draft MG11 witness statements
- AI suggesting bail conditions or arrest strategies

If Yes: **STOP**. Seek review from Legal, Ops and Info Management.

If No: Proceed to Step 6.

Reference: AI Policy 11.2

Step 6: Could this use of AI undermine public trust or harm the Force's reputation if misunderstood or challenged?

Public perception is crucial. Consider if the AI use could be viewed as inappropriate, biased, or misleading. Examples:

- Chatbot use with victims without disclosure
- AI-generated social posts that mislead
- AI producing offensive or biased responses

If Yes: **STOP**. Escalate to AI Governance Lead or Comms.

If No: Proceed with caution and ensure compliance with the AI Policy and this Decision Flow.

Reference: AI Policy 3.1, 13.1 | Code of Ethics

- 3.2 Remember, do not input personal, Sensitive or Operational data into any AI platform without approval from the Risk Owner and sign-off from the Data Protection Officer (DPO).

3.3 Any unapproved input of personal, sensitive or operational data into an AI system must be reported as a data breach. For further information on the use of AI, check out the policy below or get in touch with us and we would be happy to help!

Created: January 2026
Graham Kane, Head of Performance