



Artificial Intelligence (AI) and Large Learning Models (LLM) **Privacy Notice**

Surrey Data Protection Officer: Kelly Thornton
dataprotection@surrey.police.uk

Sussex Data Protection Officer: Jim Collen
DPO@sussex.police.uk

The use and disclosure of your personal information is governed in the United Kingdom by UK Data Protection Legislation. This incorporates requirements from both the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (Law Enforcement purposes), these require organisations to process data in a fair, lawful and transparent manner. It mandates that certain information must be communicated to data subjects to ensure that they are as well informed as possible about how their data will be processed.

Our Privacy Notice tells you how Sussex Police and Surrey Police (hereafter referred to as The Forces) utilise Artificial Intelligence (AI) including Large Learning Model (LLM) tools for law enforcement purposes. We are committed to being transparent about how we collect and use that data to meet our data protection obligations.

The Chief Constables for the Forces are defined as the 'Data Controllers' for the purposes of the legislation and are required to ensure the Force handles all personal information in accordance with that legislation. The Forces take great care to ensure your personal data is processed appropriately to maintain your trust and confidence in the police.

Purpose Of This Privacy Notice

This Privacy Notice demonstrates a commitment from the Forces to deploy the use of Artificial Intelligence (AI), specifically Copilot as the preferred Large Learning Model (LLM) responsibly, ethically and transparently to ensure it aligns with the values and legal standards of UK policing. This document defines how the Forces will integrate Copilot, including Generative AI (this creates new and original text content rather than just analysing existing data) into day-to-day policing processes.

The Forces have restricted use of Artificial Intelligence (AI) 'chat' functions to Copilot only, as using a single platform like ensures consistency across the organisation, simplifies integration with existing tools and makes governance and security easier to manage. This Privacy Notice will not address processing using AI in other bespoke systems, they are subject to their own specific governance.

AI technologies play a crucial role in enhancing workplace efficiency, however the Forces are cognisant of the need to ensure careful handling of your personal data. This document supports the existing Force Policy [Artificial Intelligence Policy](#).

AI has the potential to support policing by offering advanced tools for crime prevention and to support officers with decision-making and resource allocation. AI must only be used in response to a clearly defined problem or opportunity, it must not be treated as a default solution. However, usage comes with serious ethical considerations and privacy concerns. Although AI can significantly improve efficiency in policing in relation to preventing, detecting / investigating crime and improving public engagement, it must be balanced with considered human review, governance, public accountability and adherence to ethical principles.

Use of AI to generate information is prone to simple errors, hallucinations and AI sycophancy. This is where the AI generates a response that it believes to be correct / most pleasing response as opposed to extracting data from a source that is known to be factually correct and proven. For this reason, our staff will receive clear guidance on accountability and the necessity for thorough human review prior to any further usage.

We do not use AI to make automated decisions and there is always a human intervention to review all outputs from the AI tools. Privacy by design and by default will be at the forefront of all AI processing and the Forces have published a Data Protection Impact Assessments (DPIA) for Copilot usage (this is available on the 'Information About The Police' section of the Force internet).

The National Police Chiefs Council (NPCC) drives AI standards for policing to ensure technologies adopted adhere to existing legal frameworks, Data Protection regulations and privacy standards. Sussex Police and Surrey Police have embedded the NPCC Core Principles in usage of AI for law enforcement purposes. The Core Principles ensure restrictions of processing personal data, accuracy of responses and assurance of human review of all AI outputs prior to ingestion into Force systems.

Roles And Responsibilities

Successful and responsible AI implementation requires a robust governance framework, underpinned by a shared understanding of roles and responsibilities across the Force. By clearly defining roles and responsibilities, fostering collaboration, and embedding ethical considerations into every stage of the AI lifecycle, the Forces will uphold the highest standards of accountability and public trust. Full details of roles and responsibilities can be found in **Appendix 1**.

NPCC Core Principles

The Forces will implement the below AI standards in support of the NPCC AI principles:

Accountability:

- Provide guidance to all personnel involved in AI processing to ensure they understand the ethical implications and their roles in ensuring responsible use.
- Develop clear protocols for documenting AI-driven decisions and actions, enabling effective oversight and audit trails.
- Establish mechanisms for internal review and feedback to continuously improve accountability practices related to AI.

Robustness:

- Implement robust data quality management processes to ensure the integrity of AI systems.

Transparency:

- Communicate openly with the public about our use of AI, outlining its purpose, capabilities, and limitations.
- Provide clear and accessible information about how AI is being used to inform policing decisions.

Evidence led:

- Prioritise AI solutions with a proven track record of security and ethical protections success in similar policing contexts.
- Conduct pilot programs and evaluations to assess the effectiveness of AI technologies before widespread deployment.

Explainability:

- Only use AI systems that offer clear and understandable explanations for their outputs, particularly when used in decision-making processes and work with agencies (such as the CPS) to ensure the AI outputs can be utilised.
- Support staff to interpret AI-generated outputs to ensure accountability of accuracy and ownership of the data.

Responsibility:

- Develop a clear governance structure for AI implementation, outlining roles and responsibilities for decision-making.
- Foster a culture of responsible AI use through awareness-raising initiatives.

Lawfulness:

- Establish clear guidelines for data handling and AI usage that comply with all relevant legislation, including the Data Protection Act, UK GDPR, Human Rights Act and other relevant privacy laws.

Force Policy

The Force AI policy can be found [here](#). The Forces will only use Microsoft 365 Copilot chat functions for the processing of limited and approved personal data. This offers additional reassurances for the data we process as it is secured on our infrastructure and web grounding (the ability for the data to be uploaded to the internet) is deactivated as default.

The Forces will only process the minimum amount of data necessary for the specific AI application. This reduces privacy risks and promotes data protection by design though compliance with the data minimisation principles. We will ensure there are rigorous processes in place for data accuracy and review. This is crucial to ensure fair and equitable policing and reflect the diversity of the target demographic to remove bias in the AI generated output. In support of this, we will:

- place human intervention and review at the core of all AI impacted decision-making.
- prioritise the safety and wellbeing of the public and their personal data.
- operate with fairness, impartiality to not discriminate against or disadvantage individuals, particularly those who are most vulnerable, nor individuals or groups based on their 'protected characteristics' as defined in the Equality Act 2010.
- show the highest standards of respect and dignity towards individuals and groups as set out in the Code of Ethics.
- be transparent, proportionate and respect sensitive personal data and human rights in accordance with UK legislation.

Use of Artificial Intelligence (AI) in Law Enforcement Data Processing

We may use AI technologies to support law enforcement processing, such as for the purposes of the prevention, detection, investigation and prosecution of criminal offences. We may also use AI technologies for administrative processing of staff details or in the case of locating Missing Persons.

All processing of law enforcement data using AI is conducted in accordance with Part 3 of the Data Protection Act 2018 whereas processing for missing persons or human resource purposes will fall under the UK GDPR and Part 2 of the Data Protection Act 2018. All processing using AI technologies will be subject to stringent governance processes to ensure personal, special, sensitive and criminal data is handled lawfully, fairly, and transparently.

We are committed to ensuring that AI systems are used fairly and transparently. AI systems will assist in identifying patterns, assessing risk, or prioritising resources, and are deployed under strict lawful and ethical safeguards.

AI outputs are often based on probability which can lead to inaccuracies. AI may fabricate a response based on the statistical patterns it has learned which are not necessarily factual. To protect against this, appropriate safeguards are in place to ensure necessary oversight for all processing of AI generated responses. AI outputs will always undergo human review prior to acceptance and further processing, we do not rely on automated decision making for any processing utilising AI generated outputs.

We conduct Data Protection Impact Assessments (DPIAs) to evaluate risks and ensure compliance with data protection principles and to ensure all data processed by AI systems is handled securely, with measures in place to prevent unauthorised access, loss, or misuse. We ensure that only relevant, necessary and proportionate data is processed.

AI systems used by law enforcement are subject to regular review and oversight to ensure compliance with legal and ethical standards. We follow guidance from the Information Commissioner's Office (ICO) and other relevant bodies to maintain best practices in data protection and AI governance.

Reassurances To Protect Your Data

We are the data controller for the information we process. Strict restrictions are placed on the processing of law enforcement data through any AI. System specific processing will also be subject to a Data Protection Impact Assessments (DPIA). To ensure transparency of processing and enhance trust by assuring members of the public, the following are stipulated for all current uses of AI across both Forces to ensure there is no:

- AI provider is be able to 'learn' from law enforcement data.
- processing outside of the UK, all AI servers must be UK based and therefore protected by UK Data Protection legislation.
- retention of data processed within the AI provider infrastructure, input criteria will be deleted immediately or retained for the minimum period.

Training And Awareness

To effectively use and manage AI technologies, Sussex Police and Surrey Police personnel will be adequately informed and equipped with the necessary skills and knowledge to use AI. Training initiatives will focus on delivering an understanding of:

- AI Fundamentals: AI concepts, techniques and applications.
- AI Tools and Technologies: restrictions on processing law enforcement data using AI tools.
- Ethical: ethical considerations in AI bias, fairness and transparency.
- Data Management: data management and governance, including data quality, security and privacy.

Why Do We Process Personal Data?

In most cases, we process your personal data using the AI to improve the efficiency, quality, and speed of our business processes. A lot of these processes are already happening manually but by using AI to automate these processes, our resources can be deployed where they are needed most. We may use AI tools to support in amending, transcribing or summarising documents or meetings to increase efficiency.

How long do we keep your personal information?

We will only utilise AI software that does not retain (store) or repurpose (use) the personal data that we input into the prompt. The use of AI does not change how long we retain information, all AI generated outputs will be stored as a document type detailed in the Forces [Retention Schedule](#).

Automated Decision Making

AI responses are often based on probability which can lead to inaccuracies. AI may fabricate a response based on the data it has learned which are not necessarily factual. To protect against this for law enforcement processing, all responses must undergo human review prior to acceptance and further processing. Users will not rely on automated decision making for any processing of AI generated responses.

Staff are personally accountable for the information generated using AI. It is their responsibility to conduct a detailed review to ensure the response is accurate and a true representation of the facts before used.

AI Generated Data Statement

All AI generated data must be clearly marked with the Government Security Classification Official – Sensitive and include the below statement:

This document was created with assistance from Artificial Intelligence (AI) tools. While it has been reviewed by a human for accuracy, it may contain errors, inaccuracies, or incomplete information. The recipient must independently verify critical information with the sender / author prior to actions being taken.

What Are Your Rights Over Your Personal Data We Process, And How Can You Exercise Them?

Under the Act you have Rights that you can exercise in relation to personal data we process about you. You do not have to pay to exercise your rights (other than a reasonable fee if a request for access is clearly unfounded or excessive but we agree to fulfil it anyway). Full details of your Subject Rights can be found on the Force Privacy Notice [here](#).

Contact Us

If you have any concerns about how the Forces has handled your personal information you should contact our Data Protection Officer by:

Sussex

DPO@sussex.police.uk
Sussex Police Headquarters
Church Lane
Lewes
East Sussex
BN7 2DZ

Surrey

dataprotection@surrey.police.uk
Surrey Police
PO Box 101
Surrey
Guildford
GU1 9PE

If You Want To Raise A Concern With The Supervisory Authority

The Information Commissioner is the independent Authority responsible within the UK for ensuring we comply with data protection legislation. If you have a concern about how we have used your personal information or you believe you have been adversely affected by our handling of your data you may wish to contact them using the information below. Further information about the ICO can be found [here](#).

The Information Commissioner's Office, Wycliffe House, Wilmslow, Cheshire, SK9 5AF

Email casework@ico.org.uk

Telephone [0303 123 1113](tel:0303 123 1113)

Changes To Our Privacy Notice

We keep our privacy notice under regular review. This privacy notice was last updated on **14/10/2026**. If we plan to use your personal information for a new purpose we will update our privacy notice and communicate the changes before we start any new processing.

Appendix 1: Roles And Responsibilities

Successful and responsible AI implementation requires a robust governance framework, underpinned by a shared understanding of roles and responsibilities across the force. By clearly defining roles and responsibilities, fostering collaboration, and embedding ethical considerations into every stage of the AI lifecycle, the Forces will uphold the highest standards of accountability and public trust.

- **Police and Crime Commissioner (PCC):** Acting as a critical link between the police force and the public, the PCC ensures that AI initiatives align with community values and address public concerns. They provide independent oversight, holding the Chief Constable accountable for responsible AI implementation.
- **Chief Constable:** The Chief Constable is the Data Controller for their respective Force. They retain ultimate accountability for ethical, legal, and operational risks of AI deployment, providing strategic direction for the force's AI strategy. While maintaining accountability, they are likely to delegate final sign-off authority for AI solutions to the Data Protection Officer, with greater involvement expected in contentious external applications compared to lower-risk, back-office implementations.
- **Senior Information Risk Owner (SIRO):** Responsible for overseeing data governance practices, ensuring compliance with relevant legislation, and oversight of governance and security risk assessments for all AI solutions and the processing of personal or anonymous data.
- **Data Protection Officer (DPO):** The DPO is responsible for ensuring that the Forces' use of data is compliant with legislation, providing expert advice and guidance on the processing of all personal data. The DPO ensures compliance with the processing of personal and criminal data within the organisation. The DPO is also responsible for approval of Data Protection Impact Assessments (DPIA) for new systems and processing.
- **Procurement:** Responsible for ensuring that vendors and technology providers adhere to the force's ethical and legal requirements. This includes conducting due diligence on potential vendors to assess their commitment to responsible AI principles, negotiating contracts that clearly define data handling responsibilities, intellectual property rights, and ethical considerations, and monitoring vendor compliance throughout the AI lifecycle.
- **Change management functions:** Play a vital role in supporting the successful integration of AI solutions. They provide expertise and support to facilitate smooth adoption by addressing training needs, developing effective communication strategies, and proactively managing potential resistance to change.