



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

Surrey Data Protection Officer: Kelly Thornton
dataprotection@surrey.police.uk
[Full Privacy Notice](#)

Sussex Data Protection Officer: Jim Collen
DPO@sussex.police.uk
[Full Privacy Notice](#)

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 Surrey Police and Sussex Police utilise Artificial Intelligence (AI) including Large Learning Model (LL) 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 Sussex police and Surrey police are defined as the '[Data Controllers](#)' for the purposes of the legislation and are required to ensure Surrey Police and Sussex Police handles all personal information in accordance with that legislation.

Surrey Police and Sussex Police takes that responsibility very seriously and takes great care to ensure your personal data is processed appropriately to maintain your trust and confidence in the police.

Purpose of this Privacy Notice

Artificial Intelligence (AI) technologies including Large Language Models (LLM) play a crucial role in enhancing workplace efficiency, however Sussex Police and Surrey Police are cognisant of the need to ensure careful handling of your personal data. Where there is a requirement to do so we will use software, some of which may contain AI / LLM, to produce efficiencies and help deliver our operational priorities.

We will be transparent in our use of any AI / LLM tool and offer reassurances that all outputs will be subject to human review. We do not use AI to make automated decisions. There is always a human intervention to review and approve any outputs from the AI tools. Decisions are not made solely by automated means. This document supports existing Privacy Notices and Appropriate Policy Documents published on the Force internet sites.

Implementing such new and fast developing technology requires using a staged approach which is inherently iterative in nature. This means that the considerations in this privacy notice may be subject to change as the technological horizon evolves. This privacy notice will be kept under review accordingly to ensure that it is up to date and accurate.

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

We may use Artificial Intelligence (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:

- No AI provider will be able to 'learn' from law enforcement data.
- No processing outside of the UK, all AI servers must be UK based and therefore protected by UK Data Protection legislation.
- No retention of data processed within the AI provider infrastructure, input criteria will be deleted immediately or retained for the minimum period.

Why do we process personal data?

In most cases, we process your personal data using the AI Tools 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, this allows our resources to 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 is your information used?

- Enhance the services we offer to the public through the use of AI tools where appropriate, such as to communicate with you, provide automated responses, etc.
- Improve internal processes and increase efficiencies of administrative tasks which are necessary for the day to day functioning of our organisation, such as the training of our employees and the auditing of systems and processes.
- For internal research and analysis purposes to help improve our services, for the benefit of you and others.

How long do we keep your personal information?

Our [Retention Schedule](#) details how long your information may be kept for.

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 will 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 a number of 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 Surrey Police and Sussex Police has handled your personal information you should contact our Data Protection Officer by:

Email	Sussex	DPO@sussex.police.uk
	Surrey	dataprotection@surrey.police.uk

Address	Sussex	Data Protection Officer Sussex Police Headquarters Church Lane Lewes East Sussex BN7 2DZ	Surrey	Data Protection Officer 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
Telephone 0303 123 1113
Email casework@ico.org.uk

Changes to our Privacy Notice

We keep our privacy notice under regular review. This privacy notice was last updated on **24/10/2025**.

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.