



FOI Super Response – Artificial Intelligence (AI)

Disclaimer: Due to the high volume of FOI requests made to Sussex Police and Surrey Police relating to Artificial Intelligence (AI), a single response has been compiled covering the many points detailed in the different requests we have received to date. Any FOI request relating to this subject that is not satisfactorily covered by the following should be re-written and re-submitted specifying what additional information is required.

Introduction, scope and approach (updated Jan 2026)

Artificial Intelligence (AI) today is not a single product or program but a broad family of capabilities - from advanced analytics and statistical models to machine learning (ML), process automation, virtual agents and large language models (LLMs) - that are increasingly embedded across modern software, cloud services and security tooling. Many features operate "under the hood" (e.g., search relevance, OCR, anomaly detection, transcription, routing optimisation), are frequently updated by suppliers, and are integral to off-the-shelf platforms as well as national policing solutions. In that sense, **asking where we use AI is similar to asking where we use computers**: usage is pervasive, varied, and often part of the technology we already rely on. As such, a point-in-time, system-by-system inventory cannot practically be compiled: It would be time-consumingly onerous, would not be definitive and would likely be out of date soon after publication (See College of Policing APP on Data-Driven Technologies and the NPCC AI Strategy for context).

What we will provide in this consolidated response

We summarise AI use by category and the governance/safeguards applied, and we signpost public materials where detail is already available (e.g., AI and Live Facial Recognition policies).

Sensitivity, exemptions and proportionality

Some requested details - such as specific vendor names, configurations, deployment schedules/locations, system versions, watchlist criteria, or contract/licence information - are operationally or commercially sensitive. Where disclosure would, or would be likely to, prejudice law enforcement (FOIA s31), safeguarding national security (FOIA s24), or commercial interests (FOIA s43), we may withhold the information and explain our public-interest reasoning. In certain cases, even confirming or denying whether information is held could itself cause harm; in those cases, we may lawfully issue a "neither confirm nor deny" (NCND) response.

Categories of AI use we will cover

1. Embedded and foundational capabilities: AI features within enterprise/cloud platforms and security tooling (e.g., spam/malware detection, OCR, transcription, search ranking, automated tagging). These are typically configurable but not bespoke.
2. Operational analytics and decision support: Statistical models/ML used for forecasting, demand/workload analysis, triage support, anomaly/exception detection and quality assurance. These inform human decisions, not replace them.
3. Natural language and document technologies: LLM-assisted summarisation, drafting, retrieval-augmented search over policy/case material, transcription and redaction support (subject to governance, audit and supplier assurance).
4. Public-facing augmentation: Where relevant, technologies that enhance service delivery (e.g., messaging portals and chat interfaces). Where new capabilities may significantly affect individuals, additional assessments apply (see DPIA/Article 22).
5. Pilots and innovation: Time-limited trials to evaluate effectiveness, value for money, risks and compliance before any wider adoption; sensitive operational/tactical elements may be withheld under s31/s24 or s43.

Governance, privacy and human oversight

Where AI tools process personal data, our approach is anchored in UK data protection law and policing guidance: we complete Data Protection Impact Assessments (DPIAs) for uses likely to result in high risk, and we do not use AI to take solely automated decisions that produce legal or similarly significant effects about individuals without appropriate safeguards and meaningful human involvement (Article 22 UK GDPR).

Transparency already in the public domain

Public materials include: AI Policy (Surrey Police & Sussex Police); Overt Deployment of Live Facial Recognition (LFR) Policy; LFR overview/FAQs; NPCC AI Strategy (2025); NPCC AI Playbook for Policing (2025).

Responses to common FOI questions (Q1–Q7)

Q1. AI use in operations

We use AI-enabled capabilities across the categories listed above. Practical examples include: the Sussex Police Victim Portal (automated messaging/updates to improve service and reduce duplicate contact), video redaction tools to accelerate disclosures compliant with UK GDPR and the Data Protection Act 2018, and LFR deployments with overt signage and advance notices. Where a tool is embedded within supplier platforms, disclosure of specific vendor, version or configuration details may be withheld under FOIA s43 (commercial interests) and, for security-sensitive capabilities, s31/s24. Where requested information is public, we signpost links.

Q2. AI for decision-making

AI is only used for decision support. Operational decisions remain human-led. Examples include demand forecasting and triage support dashboards; any outputs are reviewed by officers/staff. Where any use could even potentially amount to automated decision-making with legal or similarly significant effects, we apply Article 22 safeguards (transparency, right to human review/contest, and DPIA prior to use).

Q3. AI chatbots and customer interaction

If chat or virtual assistants are deployed, they are scoped to provide information and route enquiries (e.g., guided messaging within the Victim Portal). Any material changes will be accompanied by a privacy notice and, where applicable, a DPIA. Technical specifics may be withheld under s31/s43 where disclosure could prejudice security or commercial interests.

Q4. Policies and governance

We maintain force-level policies and align with national frameworks (NPCC AI Strategy/Playbook; College of Policing APP for Data Ethics and Data-Driven Technologies). Public links are provided below. Pilots of software are governed through DPIAs, supplier assurance and human-in-the-loop review.

Q5. Data protection and ethics

Considerations include: lawfulness, necessity and proportionality; fairness and bias considerations; data minimisation; transparency; appropriate security; supplier assurance; and human-in-the-loop oversight. DPIAs are completed where required by UKGDPR Article 35, the Data Protection Act 2018, and ICO guidance. LFR deployments follow overt signage, watchlist governance and immediate deletion of non-matches, with officer verification of any alert.

Q6. Trials, pilots, or future plans

We run time-limited pilots to evaluate effectiveness and compliance before adoption. Sensitive operational detail (locations, timings, watchlist criteria, or supplier configurations) may be withheld under s31/s24 or s43. Where public materials exist (e.g., LFR deployments), we provide links.

Q7. Staff training and awareness

We provide guidance for responsible use of AI specific to the use case and aligned to national materials and local Standard Operating Procedures (e.g., review of redaction outputs; handling LFR alerts; portal communications). Internal content may be withheld under s31/s43 where disclosure would prejudice security or commercial interests.

The following table summarises current and planned AI-related initiatives:

Project / Use Case	Status
Automated Video Redaction	Operational
Text Redaction	Operational
Live Facial Recognition (LFR) Vans	Operational
Service Management Tool	Planned
AI Server Proof of Value	Planned
Transcription (Speech-to-Text)	Pilot
AI Agent Crime Data Integrity	Exploratory
Demand Forecasting	Operational
Victim Portal	Operational

Use of LLM, specifically Copilot

The only LLM currently approved for use in both Forces is Microsoft Copilot, however there are specific restrictions in place to ensure compliance with the privacy by design principles. The first is the deactivation of ‘Web Grounding’, this being removing the ability for Copilot to upload data to Bing which offers greater risk mitigation and reassurance to the public regarding protection of their data. The second is a strict set of guidelines on the types of data staff and officers can process in Copilot, including restrictions on processing public personal and law enforcement data being entered into Copilot. Copilot is not authorised for use in the Criminal Justice system for the creation of evidential materials (this has been confirmed by the Crown Prosecution Service). This means it must not be used in the preparation of witness statements, MG forms, or any other evidential reports. Any other documents generated using Copilot will include a statement to ensure transparency.

How we apply FOIA exemptions

To assist requesters, the following explains how we generally apply FOIA exemptions. **We will not normally disclose:**

- **Suppliers, contracts, or specific software/algorithms** → Section 43 (Commercial Interests) and may apply NCND if disclosure would prejudice negotiations or supplier security. However, some information may be available via the following links:

[Procuring and acquisition of goods, services and works | Sussex Police](#)

[Contract Standing Orders FINAL \(sussex-pcc.gov.uk\)](#)

<https://www.gov.uk/contracts-finder>

- **Operational tactics or deployment details** → Section 31 (Law Enforcement) and Section 24 (National Security) where disclosure could compromise policing capability or public safety.
- **Information already published** → Section 21 (Information accessible by other means).
- **Sensitive personal data** → Governed by UKGDPR, Data Protection Act 2018, and DPIA requirements; FOIA exemptions may apply if disclosure risks privacy or fairness.

Key Documents and References

Document	Link
AI Policy (Surrey & Sussex Police)	Click here
LFR Policy	Click here
Sussex LFR FAQs	Click here
NPCC AI Strategy (2025)	Click here
NPCC AI Playbook (2025)	Click here
Privacy Notice for LLM use	Click here