

26 May 2026

FOI Ref 22802

Request - You asked Staffordshire Police (SP) the following:

I am writing to request information under the Freedom of Information Act 2000 regarding your force's use of generative artificial intelligence tools — including but not limited to Microsoft Copilot, OpenAI ChatGPT, Google Gemini, and Anthropic Claude — by officers or staff for any purpose connected to operational policing.

This request relates specifically to generative AI / large language model tools. It does not cover other forms of AI such as facial recognition technology, predictive analytics, or automated data matching, which are outside the scope of this request.

I request disclosure of the following recorded information:

1. Policies and governance

(a) Copies of all policies, standard operating procedures, guidance documents, or directives — whether issued at force level or adopted from national guidance — that govern the use of generative AI tools by officers or staff, in force since 1 January 2023.

(b) If no such policy or guidance exists, please confirm this.

2. Risk assessments and compliance

(a) Copies of any Data Protection Impact Assessment (DPIA) completed in relation to the use of generative AI tools by officers or staff for any purpose, including administrative, investigative, or operational tasks.

(b) If no DPIA has been completed for any generative AI tool, please confirm this.

3. Deployed tools and licensing

(a) A list of any generative AI tools (including products bundled within existing software suites, such as Microsoft Copilot within Microsoft 365) that have been made available to officers or staff, and the date from which each tool was made available.

(b) Whether access to any generative AI tool has been suspended or restricted since 1 January 2023, and if so, which tool, on what date, and any recorded reason for the suspension or restriction.

4. Training

(a) Whether any training, e-learning, briefing, or written guidance on the use, limitations, or risks of generative AI tools has been provided to officers or staff, and if so, the date it was first made available.

(b) Whether completion of such training is mandatory before officers or staff may use generative AI tools, or whether it is optional or advisory.

(c) The number of officers and staff who have completed such training, if this figure is recorded, and the total number of officers and staff who currently have access to one or more generative AI tools.

(d) If no training has been provided, please confirm this.

5. Incident recording and quality assurance



(a) The number of occasions, if recorded, on which output from a generative AI tool used by officers or staff was subsequently identified as containing factual inaccuracies, fabricated information, or material errors — whether identified internally or by an external party — since 1 January 2023.

(b) If no such records are held, please confirm this.

6. Audits and reviews

(a) Copies of any audit, review, or evaluation — whether conducted internally or by an external body — of the force's use of generative AI tools.

(b) If no audit or review has been conducted, please confirm this.

Scope and cost clarification: To assist with cost estimates under Section 12, I confirm that this request covers only generative AI / large language model tools as defined above. I am not requesting information about other forms of AI, algorithmic tools, or automated decision-making systems.

If you estimate that compliance would exceed the appropriate cost limit, I would ask that you comply with questions 1(a), 1(b), 2(a), 2(b), 3(a), and 3(b) as a priority, and advise me which remaining questions you are unable to answer within the cost limit so that I may submit a refined request.

SP received your request on 27/04/2026 and have processed this under the Freedom of Information Act (FOIA).

SP's response to your enquiry is as follows:

SP holds some of the requested information.

- I am writing to request information under the Freedom of Information Act 2000 regarding your force's use of generative artificial intelligence tools — including but not limited to Microsoft Copilot, OpenAI ChatGPT, Google Gemini, and Anthropic Claude — by officers or staff for any purpose connected to operational policing.
- This request relates specifically to generative AI / large language model tools. It does not cover other forms of AI such as facial recognition technology, predictive analytics, or automated data matching, which are outside the scope of this request.
- I request disclosure of the following recorded information:
 - 1. Policies and governance
 - (a) Copies of all policies, standard operating procedures, guidance documents, or directives — whether issued at force level or adopted from national guidance — that govern the use of generative AI tools by officers or staff, in force since 1 January 2023.
 - (b) If no such policy or guidance exists, please confirm this.
 - **Withheld, please see the below exemption (S21).**
 - 2. Risk assessments and compliance
 - (a) Copies of any Data Protection Impact Assessment (DPIA) completed in relation to the use of generative AI tools by officers or staff for any purpose, including administrative, investigative, or



operational tasks.

(b) If no DPIA has been completed for any generative AI tool, please confirm this.

- No Information held.

- 3. Deployed tools and licensing

(a) A list of any generative AI tools (including products bundled within existing software suites, such as Microsoft Copilot within Microsoft 365) that have been made available to officers or staff, and the date from which each tool was made available.

(b) Whether access to any generative AI tool has been suspended or restricted since 1 January 2023, and if so, which tool, on what date, and any recorded reason for the suspension or restriction.

- Partially disclosed, generative AI functionality within existing corporate systems is used to support efficiency or administrative tasks. This has been from October 2025 and has not been suspended or restricted.

SP can neither confirm nor deny that any other information is held in relation to this question. Please see the below exemptions.

- 4. Training

(a) Whether any training, e-learning, briefing, or written guidance on the use, limitations, or risks of generative AI tools has been provided to officers or staff, and if so, the date it was first made available.

(b) Whether completion of such training is mandatory before officers or staff may use generative AI tools, or whether it is optional or advisory.

(c) The number of officers and staff who have completed such training, if this figure is recorded, and the total number of officers and staff who currently have access to one or more generative AI tools.

(d) If no training has been provided, please confirm this.

- Partially disclosed, no.

SP can neither confirm nor deny that any other information is held in relation to this question. Please see the below exemptions.

- 5. Incident recording and quality assurance

(a) The number of occasions, if recorded, on which output from a generative AI tool used by officers or staff was subsequently identified as containing factual inaccuracies, fabricated information, or material errors — whether identified internally or by an external party — since 1 January 2023.

(b) If no such records are held, please confirm this.

- Partially disclosed, nil.

SP can neither confirm nor deny that any other information is held in relation to this question. Please see the below exemptions.

- 6. Audits and reviews

(a) Copies of any audit, review, or evaluation — whether conducted internally or by an external body — of the force's use of generative AI tools.

(b) If no audit or review has been conducted, please confirm this

- Partially disclosed, no audit or review has been conducted.

SP can neither confirm nor deny that any other information is held in relation to this question. Please see the below exemptions.

The following exemptions have been applied:

In accordance with Section 17(1) of the Freedom of Information Act, this letter represents a refusal notice for parts of this request.

- Section 21(1) - Information reasonably accessible by other means.

Section 21 is an absolute, class-based exemption and as such there is no requirement to quantify the harm that may arise from the disclosure, nor is there a requirement to perform a Public Interest Test.

- Section 40(2) Personal Information

Section 40(2) is an absolute exemption which means that there is no need to quantify the harm that may arise from the disclosure; neither is it subject to a public interest test.

To release personal or third-party information held by SP, would breach the data protection principles; namely –

- Data is lawfully and fairly processed.
- Processed in line with an individual's rights.
- Data is secure.

Personal and third-party information cannot be released under the Freedom of Information Act.

Disclosure under Freedom of Information is a release of information to the world in general and not an individual applicant.

SP can neither confirm nor deny whether any other information relevant to this request is held, as the duty in Section 1(1)(a) of the Freedom of Information Act 2000 does not apply by virtue of the following exemptions:

- Section 24 (2) – National Security

Section 24 is a qualified exemption and as such there is a requirement to articulate the harm and conduct a test of the public interest.

- Section 31(3) Law Enforcement

Section 31 is a qualified and prejudice-based exemption and, as such, we are required to evidence the harm in disclosure and apply the public interest test

Harm

Having disclosed information about routine, non-sensitive uses of Artificial Intelligence (AI), SP will neither confirm nor deny whether it holds any further information that would indicate whether AI is, or is not, used in connection with counter-terrorism, serious and organised crime, covert intelligence activity, or specialist digital forensics supporting those functions. The duty to confirm or deny is applied by virtue of sections 24(2) (national security) and 31(3) (law enforcement) of the Freedom of Information Act 2000. This response should not be taken as an indication of whether any additional information is held.

Confirming or denying whether AI is used by SP in counter-terrorism, serious and organised crime, covert intelligence or specialist digital forensics would enable hostile actors to infer the presence, absence or maturity of particular policing capabilities. This type of capability insight is of practical value to adversaries who routinely adapt their behaviour to exploit perceived weaknesses, overwhelm less technologically equipped forces, or adjust methods to avoid detection. Even a single confirmation or denial could be combined with publicly available information from other forces to build a detailed national picture of capability. This mosaic effect represents a realistic and actionable risk, providing information that could materially undermine national security and the effectiveness of law-enforcement operations.

Public Interest Test

Factors in favour of confirming or denying - Section 24(2)

There is a strong public interest in openness and transparency about the use of AI in policing. Confirming or denying the existence of information could contribute to informed public debate about how emerging technologies are deployed, the safeguards in place, and whether they align with legal and ethical standards. Disclosure can enhance accountability, promote trust, and reassure the public that AI use is subject to appropriate oversight.

Factors against confirming or denying - Section 24(2)

There is an overriding public interest in protecting national security. Confirming or denying the existence of information about AI deployment in CT, SoC, covert intelligence, or linked specialist forensics would provide adversaries with useful insights into operational capabilities and priorities. Even a simple confirmation or denial could enable hostile actors to adjust methods, exploit potential gaps, or test thresholds. The resulting risk to national security would be real and more than trivial, and is not mitigated by partial or local confirmations, because the cumulative mosaic effect across multiple forces would still disclose sensitive capability at a national level.

Factors in favour of confirming or denying - Section 31(3)

There is a general public interest in understanding how AI is used to support policing functions, including the efficiency and effectiveness of core processes, and in ensuring that novel technologies are used lawfully and proportionately. Confirmation or denial could support external scrutiny and promote confidence in policing practice.

Factors against confirming or denying - Section 31(3)

Confirming or denying the existence of information relating to AI use in CT, SoC, covert intelligence, or specialist digital forensics would be likely to prejudice the prevention and detection of crime, the apprehension or prosecution of offenders, and the operation of law enforcement tactics and methodologies. Knowledge of whether specific capabilities exist, or do not exist, enables offenders to adapt behaviour, exploit capability gaps, frustrate investigations, and increase the cost and complexity of counter-measures. The public interest strongly favours maintaining an NCND to preserve the effectiveness of law enforcement and the safety of the public.

Balance Test

For the reasons set out above, SP will neither confirm nor deny whether it holds information indicating AI is used in CT, SoC, covert intelligence activity, or specialist digital forensics supporting those functions.

The public interest in maintaining the NCND position under sections 24(2) and 31(3) outweighs the public interest in confirmation or denial. This response should not be taken as an indication of whether any relevant information is held.

Advice and assistance

To comply with our obligations under Section 16 of the Act, the obligation to provide advice and assistance, please find below links to the information requested.

[foi-22357-staffordshire-police-ai-usage-policy-v1.0.pdf](#)

Please be advised that all Freedom of Information request responses are published on the SP website although personal details are not included.

Freedom of Information Request Appeals Procedure

1. Who Can Ask for a Review

Any person who has requested information from SP, which has been dealt with under the Freedom of Information Act, is entitled to complain and request an internal review, if they are dissatisfied with the response they received.

2. How to Request a Review

Requests for review of a Freedom of Information request must be made in writing within two months of the date of receipt of this email, and should be addressed to:

IAT@staffordshire.police.uk

Or by Post to:

Information Access Team
Staffordshire Police HQ
PO Box 3167
Stafford
ST16 9JZ

The reference number, date of the request and details of why the review is being requested must be included. Requests for review should be brought to the attention of the Information Access Team within two months of the SP response to the original FOI request.

3. Review Procedure

Receipt of a request for review will be acknowledged in writing. The review will be conducted by a supervisor who is independent from the original Decision Maker. The Information Access Team will set a

target date for a response. The response will be made as soon as is practicable with the intention to complete the review within twenty working days. In more complex cases the review may take up to forty working days.

The independent supervisor will conduct a review of the handling of the request for information and of decisions taken, including decisions taken about where the public interest lies in respect of exempt information where applicable. The review enables a re-evaluation of the case, considering the matters raised by the complaint.

4. Conclusion of the Appeal

On completion of the review the independent supervisor will reply to the appellant with the result of the review. If the appellant is still dissatisfied following the review they should contact the Information Commissioner to make an appeal. The Information Commissioner can be contacted via the following link: <https://ico.org.uk/make-a-complaint/foi-and-eir-complaints/foi-and-eir-complaints/>

Freedom of Information
Information Access Team