

24 September 2026

FOI Ref 23302

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

REQUEST 1:

What would you like to know?:

Software:

- * Please provide a full list of all AI tools and algorithmic systems currently in use by your force, including:
 - o name and description of the tool;
 - o the date it was adopted;
 - o its purpose;
 - o the operational context it is used in; and
 - o the vendor/supplier.
- * Please provide a full list of all AI tools and algorithmic systems which are being piloted, planned for adoption, or have been approved for adoption including:
 - o name and description of the tool;
 - o the start and end date of pilot / planned adoption date;
 - o its purpose;
 - o The operational context in which it was trialled / will be adopted;
 - o the vendor/supplier; and
 - o Whether the pilot was / will be formally evaluated. If so, how and by whom.
- * Has your force ever used or trialled an AI / facial recognition software that scrapes images from the internet?
- * Does your force use or has it considered using polygraph technology. If so, in what contexts, and please provide any policies, guidance, or standards governing such use.

Validation / testing:

- * What criteria does your force use to decide whether a piloted tool should move to full operational deployment i.e. that it is fit for purpose? Please provide copies of any relevant policies or decision-making frameworks
- * Does your force have a defined minimum accuracy threshold that an AI tool must meet before it is considered fit for operational deployment? If so, please provide the relevant policy or standard.
- * For each AI tool currently in operational use, please provide / confirm:
 - o The accuracy rate claimed by the vendor at the point of procurement;
 - o Whether any independent verification has taken place to assess the accuracy of the tool. If so, please provide the independently verified accuracy figures available to your force.
 - o Whether your force has identified any discrepancy between vendor claims and actual performance.
- * For each AI tool in use, please provide copies of any validation or accuracy testing reports conducted prior to or following deployment.
- * Has your force assessed if the AI tools in use perform differently across demographic groups - for example, by race, gender, or age? If so, please provide details and copies of any such assessments or reports



Monitoring/ training :

- * For AI tools, which are currently implemented or have been previously implemented, have any results been produced which were later found to be inaccurate, unreliable, or misleading in an operational context.
- * Does your force conduct ongoing post-deployment monitoring of AI tool performance? If so, please describe the process, including intervals for reviews and what criteria are used for assessment. If any policies are available, please provide these?
- * Has your force conducted any reviews to assess whether AI tools in use have experienced model drift - that is, a decline in performance over time as the data environment changes?
- * Has any AI tool been withdrawn from operational use following a performance review or drift assessment? If so, please provide details of the tool and the reasons for withdrawal.
- * For generative or predictive AI tools, are officers required to record their independent reasoning before acting on an AI-generated output? If so, please provide copies of any relevant policies or recording requirements.
- * In cases where AI tools have been used in an investigation, what information is routinely recorded and retained to enable future disclosure - for example, the name and version of the tool, the confidence score of any match, and the date of use?
- * What mandatory training is provided to officers who use AI tools in operational policing?
- * What measures does your force have in place to audit the use of AI by its officers?
- * In the last three years, have any officers faced disciplinary action over inappropriate use of AI in carrying out their duties? If so, please provide statistics.

SP received your request on 25/08/2026 and have processed this under the Freedom of Information Act (FOIA).

SP's response to your enquiry is as follows:

SP holds/does not hold the requested information.

1. Please provide a full list of all AI tools and algorithmic systems currently in use by your force, including: o name and description of the tool; - **Partially disclosed, Microsoft 365 Copilot.**
SP can neither confirm nor deny that any other information is held in relation to this question, section 24(2) and 31(3).

o the date it was adopted; - **Partially disclosed - January 2025.**
SP can neither confirm nor deny that any other information is held in relation to this question, section 24(2) and 31(3).

o its purpose; - **Partially disclosed - Chatbot integrated with Windows 11, used for a variety of generative tasks.**
SP can neither confirm nor deny that any other information is held in relation to this question, section 24(2) and 31(3).

o the operational context it is used in; and ; - **Partially disclosed - Productivity and Operational Support, Data and Analysis, Knowledge and Research, Idea Generation and Planning.**



SP can neither confirm nor deny that any other information is held in relation to this question, section 24(2) and 31(3).

o the vendor/supplier.; - **Partially disclosed - Microsoft.**

SP can neither confirm nor deny that any other information is held in relation to this question, section 24(2) and 31(3).

2. Please provide a full list of all AI tools and algorithmic systems which are being piloted, planned for adoption, or have been approved for adoption including:

o name and description of the tool; - **Partially disclosed - BOBBi: Customer facing AI agent**

SP can neither confirm nor deny that any other information is held in relation to this question, section 24(2) and 31(3).

o the start and end date of pilot / planned adoption date; - **Partially disclosed, Planned adoption September 2026.**

SP can neither confirm nor deny that any other information is held in relation to this question, section 24(2) and 31(3).

o its purpose; - **Partially disclosed - Virtual assistant is designed to handle simple queries from members of the public.**

SP can neither confirm nor deny that any other information is held in relation to this question, section 24(2) and 31(3).

o The operational context in which it was trialled / will be adopted; - **Partially disclosed - Triage and respond to 1st contact made via our website.**

SP can neither confirm nor deny that any other information is held in relation to this question, section 24(2) and 31(3).

o the vendor/supplier; and - **Partially disclosed - Salesforce.**

SP can neither confirm nor deny that any other information is held in relation to this question, section 24(2) and 31(3).

o Whether the pilot was / will be formally evaluated. If so, how and by whom. - **Partially disclosed - Formal internal evaluation through our Projects and Business Change teams.**

SP can neither confirm nor deny that any other information is held in relation to this question, section 24(2) and 31(3).

3. Has your force ever used or trialled an AI / facial recognition software that scrapes images from the internet? – **Neither confirm nor deny, Section 24(2) and 31(3).**

4. Does your force use or has it considered using polygraph technology. If so, in what contexts, and please provide any policies, guidance, or standards governing such use. **Partially disclosed – no.**

SP can neither confirm nor deny that any other information is held in relation to this question, section 23(5), Section (30) and 31(3).



Validation / testing:

5. What criteria does your force use to decide whether a piloted tool should move to full operational deployment i.e. that it is fit for purpose? Please provide copies of any relevant policies or decision-making frameworks - **Partially disclosed – Please see the accompanying file entitled ‘FOI 23302 Pilot Product Guidance’. Section 24(2) and 31(3) and Withheld Section (31)**

NPCC AI Checklist - Withheld, section 21.

PDS Standards - Partially disclosed – Please see the accompanying file entitled ‘FOI 23302 Artificial Intelligence Secure Implementation Standard’. Section 24(2) and 31(3) and Withheld Section (31)

NPCC AI Checklist - Withheld, Section 21.

NCSP Artificial Intelligence & LLM (Large Language Models) Standard - Withheld, Section 21. Artificial Intelligence Secure Implementation Standard – Partially disclosed – Please see the accompanying file entitled ‘FOI 23302 Artificial Intelligence Secure Implementation Standard’. Section 24(2) and 31(3) and Withheld Section (31)

6. Does your force have a defined minimum accuracy threshold that an AI tool must meet before it is considered fit for operational deployment? If so, please provide the relevant policy or standard. – **No information held.**

7. For each AI tool currently in operational use, please provide / confirm: – **No information held in respect of Co – Pilot.**

SP can neither confirm nor deny that further information is held.

o The accuracy rate claimed by the vendor at the point of procurement; – **No information held in respect of Co – Pilot.**

SP can neither confirm nor deny that further information is held.

o Whether any independent verification has taken place to assess the accuracy of the tool. If so, please provide the independently verified accuracy figures available to your force. – **No information held in respect of Co – Pilot.**

SP can neither confirm nor deny that further information is held.

o Whether your force has identified any discrepancy between vendor claims and actual performance. – **No information held in respect of Co – Pilot.**

SP can neither confirm nor deny that further information is held.

8. For each AI tool in use, please provide copies of any validation or accuracy testing reports conducted prior to or following deployment. . – **No information held in respect of Co – Pilot.**

SP can neither confirm nor deny that further information is held.

9. Has your force assessed if the AI tools in use perform differently across demographic groups - for example, by race, gender, or age? If so, please provide details and copies of any such assessments or reports – **Withheld, section 21.**

SP can neither confirm nor deny that further information is held.

Monitoring/ training :

10. For AI tools, which are currently implemented or have been previously implemented, have any results been produced which were later found to be inaccurate, unreliable, or misleading in an operational context. – **No information held in respect of Co – Pilot.**

SP can neither confirm nor deny that further information is held.

11. Does your force conduct ongoing post-deployment monitoring of AI tool performance? If so, please describe the process, including intervals for reviews and what criteria are used for assessment. If any policies are available, please provide these? – **No information held in respect of Co – Pilot.**

SP can neither confirm nor deny that further information is held.

12. Has your force conducted any reviews to assess whether AI tools in use have experienced model drift - that is, a decline in performance over time as the data environment changes? – **No information held in respect of Co – Pilot.**

SP can neither confirm nor deny that further information is held.

13. Has any AI tool been withdrawn from operational use following a performance review or drift assessment? If so, please provide details of the tool and the reasons for withdrawal. – **No information held in respect of Co – Pilot.**

SP can neither confirm nor deny that further information is held.

14. For generative or predictive AI tools, are officers required to record their independent reasoning before acting on an AI-generated output? If so, please provide copies of any relevant policies or recording requirements. – **Partially disclosed, sec 21 2357.**

15. In cases where AI tools have been used in an investigation, what information is routinely recorded and retained to enable future disclosure - for example, the name and version of the tool, the confidence score of any match, and the date of use? What mandatory training is provided to officers who use AI tools in operational policing? – **Partially disclosed, no information held in respect of Co – Pilot and there is no mandatory training.**

16. What measures does your force have in place to audit the use of AI by its officers? – **Partially disclosed, through 365/Purview, administrators can access copilot audit logs.**

17. In the last three years, have any officers faced disciplinary action over inappropriate use of AI in carrying out their duties? If so, please provide statistics. – **Disclosed, nil.**

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

- Section 21 - 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 23(5) – Information supplied by, or relating to, bodies dealing with security matters
Section 23 is an absolute class-based exemption and as such does not require the application of a Public Interest Test.

- Section 31 (1)(a)(b) Law Enforcement

Information is exempt from disclosure under S31(1)(a)(b) where the release of Information would, or would be likely to, prejudice the prevention and detection of crime and/ or the apprehension or prosecution of offenders. This exemption is qualified and prejudice-based and, as such, we are required to evidence the harm in disclosure and apply the public interest test.

Harm:

To provide detailed frameworks could undermine existing or future investigations, operations and police tactics. It would allow those with ill intent to cause disruption to operational policing and prejudice the prevention and detection of crime. Knowing detailed frameworks and associated information for specific areas would allow individuals to speak on the policing network with a level of validity that could lead to major disruption to the force communications network. It would also aide criminals in disrupting events involving these areas.

Public Interest Test

Factors favouring disclosure under Section 31(1)(a)(b)

To disclose this information would adhere to the basic principle of being open and transparent, it would also lead to a better public awareness of the workings of the police force and the communications used with operations and during routine policing.

Factors favouring non-disclosure under Section 31(1)(a)(b)

Releasing such data would give those individuals with the intent to do so, the intelligence required to disrupt police activity. This knowledge would allow those with ill intent to target their offending more effectively which would inevitably lead to an increased likelihood of criminal activity and an increased danger to the public. Any disclosure of information which is likely to undermine the ability to serve the public in preventing and detecting crime can only be considered as being harmful to the public.

Balance test

When considering whether disclosure is appropriate, we must weigh the strongest reason for disclosure against the strongest reasons for non-disclosure. In this case, whilst the factors favouring disclosure are important in that it would adhere to the basic principle of being open and transparent, we believe when weighed against the risk of disclosure undermining our ability to prevent and detect crime and hindering our ability to protect the public, then non-disclosure takes precedence.

SP can neither confirm nor deny whether 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 30(3) – Criminal Investigations SP are required to apply the public interest test.
- Section 31(3) – Criminal Investigations SP are required to apply the public interest test.

Section 24(2) National Security

Factors in favour of confirming or denying

There is a strong public interest in transparency regarding the use of artificial intelligence (AI) within policing. Confirming or denying whether the requested information is held would contribute to an informed public debate about the deployment of emerging technologies, the safeguards and governance structures that may be in place, and whether their use is consistent with legal, ethical, and human rights obligations. Greater openness in this area promotes accountability, enhances public confidence, and provides reassurance that any use of AI is subject to appropriate oversight and scrutiny.

There is also a significant public interest in understanding how public funds are spent. Confirming or denying whether the information is held would help the public understand whether resources are being invested in technologies and capabilities designed to support policing objectives, including the prevention and detection of serious crime and terrorism. Such transparency enables the public to assess whether public money is being used effectively and responsibly.

Furthermore, the fact that information may relate to national security does not, in itself, mean that confirming or denying whether it is held would result in prejudice. The public has a legitimate interest in understanding, at a high level, what measures and capabilities law enforcement may utilise and how public resources are allocated. Confirming or denying whether business is conducted using online intelligence-gathering tools or platforms would contribute to a better-informed public and support wider public understanding of modern policing.

Factors against confirming or denying

There is a paramount public interest in safeguarding national security and protecting the public from the threats posed by terrorism and serious and organised crime. Confirming or denying whether information is held relating to the deployment of artificial intelligence (AI) within Counter Terrorism Policing, Serious and Organised Crime investigations, covert intelligence activity, or specialist forensic capabilities would provide valuable insights into law enforcement capabilities, priorities, and areas of operational focus.

Even a simple confirmation or denial could assist hostile actors in assessing policing capabilities, adapting their methods, identifying potential gaps, or testing the extent of law enforcement activity. The resulting prejudice to national security would be real, significant, and more than trivial.

This risk is not mitigated by the fact that similar information may have been disclosed elsewhere.

Confirming or denying whether information is held by individual police forces contributes to the wider intelligence picture. When combined with information available from other sources, such disclosures can create a "mosaic effect", whereby seemingly innocuous pieces of information collectively reveal sensitive operational capabilities and national priorities.

Furthermore, confirming or denying whether information is held in relation to areas such as polygraph testing, intelligence sharing, or online intelligence-gathering tools would undermine the effectiveness of policing and security measures. Information shared between law enforcement partners may relate to a broad spectrum of criminality, including threats to life, serious organised crime, and terrorist activity. Confirmation or denial could enable individuals intent on criminality to determine whether particular methods, capabilities, or information-sharing arrangements exist, allowing them to alter their behaviour to evade detection.

Effective intelligence-led policing relies upon preventing hostile actors from gaining insight into law enforcement tactics and capabilities. The public entrusts the police service to make appropriate decisions to protect their safety and security, and this requires caution when considering the disclosure of information, even where the information sought appears generic in nature. Confirming or denying whether information is held would risk undermining operational effectiveness, compromising current or future investigations, and weakening measures designed to protect the United Kingdom's national security interests.

Section 30 Investigations

Factors in favour of confirming or denying the information is held

There is a public interest in the transparency of policing operations and providing assurance that SP is appropriately and effectively dealing with Counter Terrorism. Confirming or denying whether any other information is held would allow the public to make informed decisions about these matters.

Factors in favour of neither confirming or denying the information is held

Whilst there is a public interest in the transparency of policing operations and providing assurance that SP is appropriately and effectively dealing with the threat of Terrorism, there is a strong public interest in safeguarding the integrity of police investigations and operations and in maintaining confidence in the Police Service. Any ongoing or future investigations, or operations to protect the security and infrastructure of the UK would be compromised as terrorists could map the level of Counter-Terrorist activity and intelligence sharing across the country, providing them with the knowledge of individual force capability as well as valuable knowledge concerning the vulnerability of individual force areas.

Section 31(3) Law enforcement

Factors in favour of confirming or denying

There is a clear public interest in understanding how artificial intelligence (AI) is used within policing and the functions it supports, including its role in enhancing the efficiency and effectiveness of core policing processes. There is also a legitimate public interest in ensuring that emerging technologies are deployed lawfully, proportionately, and with appropriate oversight. Confirmation or denial of such use would enable informed public scrutiny and help maintain confidence in policing practices.

SP has a responsibility to conduct its business in an open and transparent manner. Disclosure regarding the use of technologies and investigative techniques, including polygraph testing where applicable, would demonstrate the police service's commitment to preventing and detecting crime, protecting the public, and ensuring that policing activities are subject to appropriate accountability. Greater transparency can also improve public understanding of the safeguards, processes, and methods used by law enforcement to protect communities.

Furthermore, confirming or denying whether AI is used in facial recognition technology would provide valuable insight into modern policing capabilities and how intelligence is gathered and utilised. Such information would contribute to a more informed public debate, reducing the risk of speculation, misinformation, or misunderstanding surrounding the use of these technologies. Given that public funds are used to develop, procure, and operate such systems, there is a strong public interest in accountability, transparency, and demonstrating that public money is being spent appropriately and effectively.

Factors against confirming or denying

Confirming or denying the existence of information relating to the use of AI in counter-terrorism, serious and organised crime investigations, covert intelligence activities, or specialist digital forensics would be likely to prejudice the prevention and detection of crime, the apprehension or prosecution of offenders, and the effectiveness of law enforcement tactics and methodologies. Knowledge of whether particular capabilities exist, or do not exist, could enable criminals, extremists, and terrorists to adapt their behaviour, exploit perceived capability gaps, frustrate investigations, and increase the cost and complexity of law enforcement activity. The public interest therefore strongly favours maintaining a Neither Confirm Nor Deny position in order to preserve operational effectiveness and protect public safety.

Similarly, confirming or denying whether AI is used within facial recognition technology would be likely to disclose information about policing capabilities and intelligence-gathering methodologies. It is recognised that disclosures made under the Freedom of Information Act are accessible to all, including those who may seek to undermine law enforcement activity. Revealing whether such capabilities are, or are not, employed could assist criminal or terrorist actors in evaluating police tactics and adapting their methods accordingly.

The Police Service relies upon a wide range of overt and covert techniques to fulfil its law enforcement responsibilities. Disclosure of information relating to the existence, non-existence, or extent of such capabilities would risk revealing operational tactics and methodologies, thereby reducing their effectiveness. In turn, this could place additional demands on police resources, hinder investigative activity, and increase the risk of criminality and terrorist offending.

Furthermore, there are significant risks associated with disclosing information concerning investigative techniques and security-related capabilities. Confirming or denying whether information is held may reveal vulnerabilities, limitations, or strengths within policing and wider national security arrangements.

Confirming or denying whether information is held would effectively place sensitive information into the public domain and may compromise law enforcement tactics and capabilities, thereby hindering the prevention and detection of crime. This is particularly relevant in relation to polygraph testing and any information that may be held by the force directly or obtained through partnership working with other law enforcement agencies in support of counter-terrorism investigations. Disclosure could:

- a) Enable criminals or extremists to evade detection or prosecution if they believe such techniques are not available or not being used for intelligence-gathering purposes; or
- b) Cause criminals or extremists to alter their behaviour if they become aware of the tactics, techniques, and operational capabilities that may be available to the police.

Accordingly, confirming or denying whether such information is held could undermine ongoing and future investigations, compromise operational capabilities, and prejudice the prevention and detection of crime, including terrorism-related offences.

Balance test

For the reasons detailed about, SP will neither confirm nor deny whether it holds information indicating AI is used in Counter Terrorism, Serious and Organised Crime, covert intelligence activity, or specialist digital forensics supporting those functions.

The public interest in maintaining the NCND position in relation to AI by virtue of S24(2) and S31(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.

A separate response has already provided high level information about routine, nonsensitive AI use. To go further would risk disclosing sensitive capability by inference.

The Police Service will not divulge information if to do so would place the safety of an individual at risk or undermine Law Enforcement. Whilst there is a public interest in the transparency of policing operations, and in this case providing assurance that SP is appropriately and effectively engaging with the threat posed by criminal and terrorist activity (either at force level or through the provision of assistance to, or from partners) there is a very strong public interest in safeguarding law enforcement, which by extension includes National Security.

As much as there is public interest in knowing that policing activity is appropriate and balanced about such matters, this will only ever be overridden in exceptional circumstances. Matters in relation to crime and terrorism are sensitive issues of intelligence value to those who would do harm, and therefore it is our opinion that for these issues the balancing test for confirming or denying whether any other information is held in relation to Polygraph tests and Counter Terrorism would not be in the public interest.

Whilst there is a public interest in the transparency of policing operations and providing assurance that the SP is appropriately and effectively engaging with the threat posed by various groups or individuals, there is a very strong public interest in safeguarding the integrity of police investigations and all areas of operations carried out by police forces throughout the UK.

As much as there is public interest in knowing that policing activity is appropriate and balanced this will only be overridden in exceptional circumstances. The use of technology can be a sensitive issue that would reveal police tactics and therefore it is our opinion that for these issues the balancing test for confirming or denying whether any information is held regarding the police and the use of AI in facial recognition technology is not made out.

However, this should not be taken as necessarily indicating that any information that would meet your request exists or does not exist.

Advice and assistance

In order 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.

- Q5 - [NCSP Artificial Intelligence Large Language Models](#), [Responsible-AI-checklist-for-policing-2025.pdf](#)
- Q9 - [Published items - 22357 | Staffordshire Police](#)

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



STAFFORDSHIRE
POLICE

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 Force's 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 20 working days. In more complex cases the review may take up to 40 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