6 November 2026 **FOI Ref 23532**

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

Under the Freedom of Information Act 2000, please provide the following information regarding the use of Live Facial Recognition (LFR) and algorithmic or generative artificial intelligence technologies within your police force.

For this request, please restrict your date range from 2021 to 2026.

Please provide me with the following information:

Section 1

1. In your constabulary, are LFR vehicles used?

IF YES TO THE PREVIOUS QUESTION:

2. How many Live Facial Recognition capable vehicles are available as of the 13th October 2026, including those owned by your force or accessible through shared regional/national agreements?

3. What is the average or estimated cost per deployment of an LFR vehicle?

4. How long is biometric data retained when an individual is scanned and matched as a person of interest in an LFR vehicle?

5. Of all persons matched as a person of interest, what percentage are false positives, and what percentage leads to arrests?

Section 2

6. In your constabulary, are statistical algorithms/generative artificial intelligence technologies used?

IF YES TO THE PREVIOUS QUESTION:

7. What technologies do you use in your police force which requires the use of statistical algorithms/generative artificial intelligence technologies (such as, heat-maps for crime hot-spots)?

8. What companies are contracted to provide these services to your constabulary?

9. How much does it cost per quarter to contract these companies to provide these services?

SP received your request on 13/10/2026 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.

- Under the Freedom of Information Act 2000, please provide the following information regarding the use of Live Facial Recognition (LFR) and algorithmic or generative artificial intelligence technologies within your police force.

- For this request, please restrict your date range from 2021 to 2026.

- Please provide me with the following information:

- Section 1

- 1. In your constabulary, are LFR vehicles used?
  - Disclosed, no.
- IF YES TO THE PREVIOUS QUESTION:

- 2. How many Live Facial Recognition capable vehicles are available as of the 13th October 2026, including those owned by your force or accessible through shared regional/national agreements?
  - Not applicable.
- 3. What is the average or estimated cost per deployment of an LFR vehicle?
  - Not applicable.
- 4. How long is biometric data retained when an individual is scanned and matched as a person of interest in an LFR vehicle?
  - Not applicable.
- 5. Of all persons matched as a person of interest, what percentage are false positives, and what percentage leads to arrests?
  - Not applicable.

- Section 2

- 6. In your constabulary, are statistical algorithms/generative artificial intelligence technologies used?
  - Disclosed, yes.
- IF YES TO THE PREVIOUS QUESTION:

- 7. What technologies do you use in your police force which requires the use of statistical algorithms/generative artificial intelligence technologies (such as, heat-maps for crime hot-spots)?
  - No information held. The statistical algorithms/generative artificial intelligence technologies used by SP are standalone. No technologies used by SP require the use of statistical algorithms/generative artificial intelligence technologies. SP can neither confirm nor deny that any further information is held, please see sections 24(2) and 31(3) exemptions below.
- 8. What companies are contracted to provide these services to your constabulary?
  - Not applicable. SP can neither confirm nor deny that any further information is held, please see sections 24(2) and 31(3) exemptions below.

- 9. How much does it cost per quarter to contract these companies to provide these services?
  - Not applicable. SP can neither confirm nor deny that any further information is held, please see sections 24(2) and 31(3) exemptions below.

All Freedom of Information request responses are published on the SP website although personal details are not included.

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.

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 high-level 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 disapplied 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.

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

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

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