

16 September 2026

FOI Ref 23317

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

Thank you for your response. I have narrowed the scope of request and would be grateful if you could consider this amended request:

Please provide a list of any systems or tools currently operational that are used by the force that:

1. use statistical modelling, predictive analytics, machine learning, or other algorithmic processing to combine or analyse data and produce a risk score, probability, ranking, classification or prioritised list relating to offending, victimisation, vulnerability, harm or another policing outcome; or
2. use artificial intelligence to analyse or generate material for policing purposes, including image or video analysis, automated identification of people or objects, cold-case analysis, transcription or AI-assisted statements, or AI-assisted call handling and/or triage.

For each system, please provide its name and a brief description of its purpose.

This request excludes systems that merely store, manage or display information, and risk assessments completed manually by police personnel, such as DASH.

Your assistance in this matter is much appreciated.

Original FOI 23189 request

Please provide a list of any systems, tools or projects currently in use, being trialled, procured but not yet operational, or under development by or on behalf of the force that fall within the following definition of “data-driven policing.”

For the purposes of this request, data-driven policing refers to systems, tools or projects that use data analytics, statistical modelling, algorithmic processing, risk assessment, predictive analytics, machine learning or artificial intelligence to inform or support policing decisions, assessments, prioritisation or operational activity.

For each system, tool or project, please provide:

1. The name of the system, tool or project and a brief description of its purpose.
2. Whether it is:
 - operational;
 - being trialled;
 - procured but not yet operational; or
 - under development.

3. Whether it uses, or is intended to use, data that:
 - originates solely from the force or other policing bodies; or
 - also includes data originating from non-police organisations, such as local authorities, NHS bodies, other public-sector organisations or private organisations.
4. Copies of any Data Protection Impact Assessments (DPIAs), or equivalent Privacy Impact Assessments, held in relation to each system, tool or project. Where a document is already publicly available, a link to it is sufficient.

For clarity, this request includes systems that identify or present patterns, trends, associations, links, risks or other data-derived contextual information, or that produce scores, classifications, predictions, alerts, recommendations, prioritised lists or other analytical outputs.

This includes systems used to inform or support human judgement where the final decision remains with a human user, including systems described as providing only information or additional context and systems that the force does not formally describe as “artificial intelligence.”

SP received your request on 27/08/2026 and have processed this under the Freedom of Information Act (FOIA).

SP's response to your enquiry is as follows:

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

SP holds/does not hold the requested information.

Please provide a list of any systems or tools currently operational that are used by the force that:

1. use statistical modelling, predictive analytics, machine learning, or other algorithmic processing to combine or analyse data and produce a risk score, probability, ranking, classification or prioritised list relating to offending, victimisation, vulnerability, harm or another policing outcome;
 - **Partially disclosed: SP have two business intelligence platforms: Business Objects; Power Bi. These turn data into useful information.**
2. use artificial intelligence to analyse or generate material for policing purposes, including image or video analysis, automated identification of people or objects, cold-case analysis, transcription or AI-assisted statements, or AI-assisted call handling and/or triage.
 - **Partially disclosed: In Evidence.com, SP use**
 - **“Axon Auto-Transcribe” This uses AI to transcribe audio from digital evidence.**
 - **“Redaction Studio” This uses AI to locate objects (notebooks, screens, license plates, heads, and ID cards) for the purpose of redaction **Please note, it does not do facial recognition”**

For each system, please provide its name and a brief description of its purpose.

SP can neither confirm nor deny whether further 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

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:

Having disclosed the information for high-level, routine, non-sensitive use of these technologies, we can neither confirm nor deny whether we hold any further information that the technology is used to support counter-terrorism, serious and organised crime or covert intelligence activity 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 its' use in counter-terrorism, serious and organised crime, or covert intelligence would enable hostile actors to infer the presence, absence or maturity of 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 - S24(2) National Security:

Factors in favour of confirming or denying: There is a strong public interest in openness and transparency about the use of advanced technologies 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 its' use is subject to appropriate oversight.

Factors against confirming or denying: There is an overriding public interest in protecting national security. Confirming or denying the existence of information about this technology in CT, SoC, or covert intelligence 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.



Public Interest Test - S31(3) Law Enforcement:

Factors in favour of confirming or denying: There is a public interest in understanding how advanced technology 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: Confirming or denying the existence of information relating to advanced technologies' use in CT, SoC, or covert intelligence 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, we can neither confirm nor deny whether we hold information indicating advanced technology is used in CT, SoC, or covert intelligence activity to support 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.

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



STAFFORDSHIRE
POLICE

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