

8 April 2025

FOI Ref 17877

Request - You asked us the following:

I am requesting information regarding AI use in digital forensic departments nationwide. The questions relate only to your digital forensics departments, including units that process digital images, video and audio evidence. The responses given will be used in said dissertation to aid in my research. The three questions for my research are:

1. Do any of your digital forensic departments employ tools/software that incorporate AI technology? This could include software that uses AI such as enhancement software or systems used for facial recognition.

If your response is "yes", then please include the name of the software(s) and details of what they used for.

2. What guidelines, regulations, or legislation do you follow in relation to AI use within your digital forensic departments?

3. Are there any AI tools/software that you plan on using in the near future?

Please do feel free to provide any further information you feel might be relevant regarding the use of AI within your digital forensics departments that are not covered within the questions above.

We received your request on 24/02/2025 and have processed this under the Freedom of Information Act (FOIA).

Staffordshire Police's response to your enquiry is as follows:

Staffordshire Police holds/does not hold the requested information.

- 1. Do any of your digital forensic departments employ tools/software that incorporate AI technology? This could include software that uses AI such as enhancement software or systems used for facial recognition.
If your response is "yes", then please include the name of the software(s) and details of what they used for. – **Partially disclosed, yes.**
- 2. What guidelines, regulations, or legislation do you follow in relation to AI use within your digital forensic departments? – **No information held.**
- 3. Are there any AI tools/software that you plan on using in the near future? – **Partially disclosed, yes.**

The following exemption has been applied:

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

- 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 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:

Policing is an information-led activity, and information assurance (which includes information security) is fundamental to how the Police Service manages the challenges faced. In order to comply with statutory requirements, the College of Policing Authorised Professional Practice for Information Assurance has been put in place to ensure the delivery of core operational policing by providing appropriate and consistent protection for the information assets of member organisations, see below link:

<https://www.app.college.police.uk/app-content/information-management/>

Commercial Forensic Service Providers and the software they offer are vitally important in the Criminal Justice system - not only do they play a crucial role by supporting UK Policing with backlogs in the Digital Forensics arena, but they provide Defence teams with access to independent forensic experts to support their clients.

Whilst not questioning the motives of the applicant, it must be taken into account when considering potential harm that a disclosure under the Freedom of Information Act 2000 is made to the world at large, rather than a private correspondence. Specific details of any digital forensic software used by the force would be extremely useful to those involved in criminality as it would enable them to create a map of tools and, by extension, providers most used by police forces. Forensic Service Providers can, and have, be targeted by malicious actors. For example in 2019 Eurofins suffered a highly sophisticated ransomware attack which severely disrupted UK Policing and the Criminal Justice system.

Providing a list of digital forensics software used would mean that force by force, a criminal or individual with criminal intent could identify the software and/or providers most critical to law enforcement and specifically target those providing the most assistance. This would have a huge impact on the effective delivery of operational law enforcement as it would leave companies open to cyberattacks which could have devastating consequences.

Public Interest Test

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

Confirming details of the software used would be of interest to the public, namely give insight into the forensic processes used to solve crimes.

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

Measures are put in place to protect the community we serve and as evidenced within the harm, to provide a detailed list of digital forensic software would allow individuals intent on disrupting law enforcement to target specific companies using the information obtained to maximise the impact.

Taking into account the current security climate and the increasing risk of cyber-attack within the United Kingdom, no information which may aid criminality should be disclosed. It is clear that it would have an impact on a Force's ability to carry out the core duty of enforcing the law and serving the community.

The public entrust the Police Service to make appropriate decisions with regard to their safety and protection and the only way of reducing risk is to be cautious with what is placed into the public domain.

Balance test

The Police Service is charged with enforcing the law, preventing and detecting crime and protecting the communities we serve. In order to effectively and robustly carry out those duties, services are utilised which are vital to investigating criminal activity. Weakening the mechanisms used to investigate any type of criminal activity would have a detrimental impact on law enforcement as a whole. To provide the names of digital forensic software currently in use by the force increases the known risks of cyber-attacks and would undermine any trust or confidence the public have in the Police Service. Therefore, at this moment in time, it is our opinion that the balance test favours against the disclosure.

Please be advised that all Freedom of Information request responses are published on the Staffordshire Police 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 Staffordshire Police, 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:

foi@staffordshire.police.uk

Or by Post to:

Central Disclosure Unit
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 Central Disclosure Unit 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 another Decision Maker who is independent from the original Decision Maker. The Central Disclosure Unit 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 Decision Maker 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, taking into account the matters raised by the complaint.

4. Conclusion of the Appeal

On completion of the review the Independent Decision maker will reply to the complainant with the result of the review. If the complainant 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 details:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

ICO Website for complaints link: <https://ico.org.uk/make-a-complaint/foi-and-eir-complaints/foi-and-eir-complaints/>

Freedom of Information
Central Disclosure Unit