7 January 2026 **FOI Ref 22247**

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

I am seeking information on what is captured and logged in chain of custody (CoC) and audit trails (AT) during the analysis of audio and textual evidence, including common analysis tasks such as transcription, translation, redaction and summarisation.

The scope of interest is for when these tasks are performed, be it with or without the use of AI tools like automatic speech recognition (ASR) and natural language processing (NLP), like large language models (LLMs).

The relevant teams are the digital forensics department and investigation unit, or the equivalent within your force.
If CoC and AT are recorded, please provide the following information (for CoC and AT separately where applicable):

1. Information recorded
Please describe the types of information that are routinely captured in CoC and AT documentation for digital evidence (including any paradata, if recorded).

2. Methods of recording/tracking
Please describe the systems or processes used to record or track CoC and AT, and indicate whether these are manual, automated, or hybrid.

3. Verification and validation
Please indicate whether the force has procedures to confirm that digital evidence is genuine and unmodified at the point of acquisition or during analysis.

4. Policies and guidance
Please provide copies or references to any current policies, or guidance documents governing CoC and AT for digital evidence.

5. Management and responsibility
Please indicate whether CoC and AT documentation is managed in house or outsourced, and identify the responsible role(s) or department(s).

6. Use of AI tools
Does the force use AI tools such as automatic speech recognition (ASR), natural language processing (NLP), or large language models (LLMs) in the analysis of audio or textual evidence?
If yes, please provide:
* the types of tools used
* the names of the tools
* the providers/suppliers

* the tasks in which they are applied (e.g., transcription, translation, redaction, summarisation)

Search period: Current procedures and policies only.

Glossary

* Artificial Intelligence (AI): This refers to a machine that learns, generalises, or infers meaning from input, thereby reproducing or surpassing human performance. The term AI can also be used loosely to describe a machine's ability to perform repetitive tasks without guidance.

* Audit Trail (AT): Refers to the documentation processes that capture, record, and report the sequence of actions applied to digital evidence. An AT may include details such as model configurations, parameters used, error rates, human interventions, and system-generated logs. It functions as a transparency mechanism, enabling the reconstruction and evaluation of how evidence has been processed, analysed, and interpreted.

* Automatic Speech Recognition (ASR): A subfield of AI that processes spoken human language (audio) and converts it into written text, useful for tasks like transcription and speaker diarisation.

* Chain of Custody (CoC): This is the record of how evidence is handled from the point of collection through processing to presentation in court. This may include the identity of the person handling the evidence, date/time of transfer, storage details, and digital identifiers. Alternative terms include 'continuity', 'chain of evidence' and 'provenance'.

* Forensic Audio evidence: This refers to recorded sound collected, preserved, and analysed for legal or investigative purposes. This often includes spoken language from sources including body-worn cameras, dashcams, police radio communications, and interview or interrogation recordings.

* Forensic Textual evidence: This refers to written or encoded content, stored or transmitted in digital form, collected, preserved, and analysed for legal or investigative purposes. It includes unstructured human language (e.g., transcripts, emails, chat logs, social media posts), semi-structured data (e.g., system or network logs, ASR outputs), and structured data (e.g., metadata, timestamps).

* Paradata: This refers to information generated as a by-product of human interaction with AI systems during evidence processing. This includes prompts, edit histories, data discards, interaction logs, correction logs, reviewer annotations, parameter adjustments, and iterative outputs. Such records provide traceable documentation of how humans and AI jointly contribute to outputs, supporting transparency and accountability in evidential practice.

* Large Language Models (LLMs): A type of Natural Language Processing (NLP) system trained on vast amounts of text to perform sophisticated language tasks like summarisation, translation, or text generation.

* Natural Language Processing (NLP): A subfield of AI focused on the interaction between computers and human (natural) language. It involves programming computers to process, analyse, understand, and generate human language. It is useful for tasks like translation, document generation, summarisation and redaction.

SP received your request on 16/12/2025 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. Information recorded
   - Please describe the types of information that are routinely captured in CoC and AT documentation for digital evidence (including any paradata, if recorded). **– Disclosed, continuity of evidence for the physical exhibit/media recorded on force systems.**

2. Methods of recording/tracking
   - Please describe the systems or processes used to record or track CoC and AT, and indicate whether these are manual, automated, or hybrid. **– Withheld.**

3. Verification and validation
   - Please indicate whether the force has procedures to confirm that digital evidence is genuine and unmodified at the point of acquisition or during analysis. **– Disclosed, no.**

4. Policies and guidance
   - Please provide copies or references to any current policies, or guidance documents governing CoC and AT for digital evidence. **– No information held.**

5. Management and responsibility
   - Please indicate whether CoC and AT documentation is managed in house or outsourced, and identify the responsible role(s) or department(s). **– No information held.**

6. Use of AI tools
   - Does the force use AI tools such as automatic speech recognition (ASR), natural language processing (NLP), or large language models (LLMs) in the analysis of audio or textual evidence? If yes, please provide:
     * the types of tools used
     * the names of the tools
     * the providers/suppliers
     * the tasks in which they are applied (e.g., transcription, translation, redaction, summarisation)

     – Disclosed, no.

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

Specific details of any digital forensic software or providers used by SP would be extremely useful to those involved in criminality as it would enable them to create a map of those most used by police forces. Providing information that disclosed digital forensics software and/or providers and descriptions of such processes used would mean that force by force, a malign individual could identify the software and/or providers most critical to law enforcement and specifically target those proving 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 and descriptions 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 information that revealed digital forensic software or providers and descriptions of forensic processes 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 or descriptions of digital forensic software or providers 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 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