

T/Chief Constable
T/Chief Constable Darren Martland
Police Headquarters
Carleton Hall Penrith,
Cumbria
CA10 2AU



14th January 2026

Dear

FREEDOM OF INFORMATION REQUEST – FOI 1603/25 Chain of Custody (CoC) and Audit Trails (AT)

I refer to your request for information which was received by Cumbria Constabulary on 15th December 2025. I note you seek access to the following information:

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.

The scope of interest is for analysis done with or without the use of AI tools like automatic speech recognition (ASR) and natural language processing (NLP), like large language models (LLMs).

Department: Digital forensics department and investigation unit, or the equivalent within your force.

Stage of evidence lifecycle: Analysis

Timeframe: I am only interested in the current practice. In terms of a definitive timeframe, 1st January 2025 till the date of the request.

Request:

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 audio and textual evidence.

Please indicate if paradata is 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 audio and textual 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).



EMPLOYER RECOGNITION SCHEME

BRONZE AWARD

Proudly supporting those who serve.



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).*

Glossary

Artificial Intelligence (AI): Computer systems that perform tasks such as recognising speech, analysing text, or making inferences from data. The term is also used more broadly to describe automated or semi automated tools used in evidence processing.

Audit Trail (AT): Documentation that records the sequence of actions applied to digital evidence. This may include system logs, processing steps, parameters used, and human interventions, enabling reconstruction and review of how evidence was handled.

Automatic Speech Recognition (ASR): Technology that converts spoken audio into written text, commonly used for tasks such as transcription and, where applicable, speaker identification or diarisation.

Chain of Custody (CoC): A record of how evidence is handled from collection through processing to presentation in court. It may include who handled the evidence, when transfers occurred, storage details, and digital identifiers. Also known as "continuity" or "provenance."

Forensic audio evidence: Recorded sound collected, preserved, and analysed for investigative or legal purposes, including material from body worn video, dashcams, radio communications, and interview recordings.

Forensic textual evidence: Written or digital text collected, preserved, and analysed for investigative or legal purposes, including transcripts, emails, chat logs, and social media posts.

Paradata: Information generated as a by product of human interaction with digital or AI assisted tools during evidence processing (e.g., prompts, edits, interaction logs). Paradata helps document how outputs were produced.

Large Language Models (LLMs): AI systems trained on large text datasets to perform tasks such as summarisation, translation, or text generation.

Natural Language Processing (NLP): AI methods used to process, analyse, or generate human language, supporting tasks such as translation, summarisation, redaction, and document analysis.

Your request for information has now been considered, and I can confirm Cumbria Constabulary does hold some information relevant to your request, however the Constabulary is not obliged to disclose the requested information to you.

Section 17 of the Freedom of Information Act 2000 requires Cumbria Constabulary when refusing such information (because the information is exempt) to provide you the applicant with a notice which: -

- (a) states the fact,
- (b) specifies the exemption and
- (c) states (if it would not be apparent) why the exemption applies.

The exemption applicable in this case are:

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



EMPLOYER RECOGNITION SCHEME

BRONZE AWARD

Proudly supporting those who serve.



Information is exempt from disclosure under Section 31(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.

Evidence of Harm

Every effort should be made to release information under Freedom of Information. However, a FOIA response is considered to be a release to the world, as once the information is published, the public authority has no control over what use is made of that information.

Specific details of any digital forensic software or providers used by Cumbria Constabulary 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 – 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. In addition, forces are required to demonstrate efficient services/systems to local taxpayers and satisfy audit requirements.

Factors favouring non-disclosure – 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. Any disclosure has the potential to undermine current and future technological integrity, which in turn compromises Law Enforcement, and could jeopardise the daily running of policing activity. The risk of affecting the function of the police service would be much greater. In addition, by revealing systems used, this is intelligence to those who would wish to exploit vulnerabilities in the service. This may lead to the compromise of force systems which ultimately affects law enforcement capabilities and hinders the prevention and detection of crime or terrorism.

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.



EMPLOYER RECOGNITION SCHEME

BRONZE AWARD

Proudly supporting those who serve.



I am aware of the immense importance for Public Authorities to demonstrate a level of openness and transparency, I am of the opinion that protecting the tactical capability of Cumbria Constabulary must take precedence in this case. With this in mind, it is my decision that the balance of the public interest lies in the non-disclosure of the exempted information.

Notwithstanding the above, in anticipation it will still be of interest to you, it is possible to provide you with some of the information requested in the remaining questions. This is information I would otherwise have advised you to submit a revised request to seek disclosure of in accordance with the duty to provide advice and assistance.

Question 1. Information recorded

The types of information that are routinely captured in CoC and AT documentation for audio and textual evidence is continuity of evidence for the physical exhibit/media recorded on force systems.

Question 3. Verification and validation

Cumbria Constabulary does have procedures to verify and validate all extractions to ensure a true image is taken.

Question 4. Policies and guidance

The response to question 4 is no information held.

Question 5. Management and responsibility

The response to question 5 is no information held.

Question 6. Use of AI tools

Cumbria Constabulary does not use AI tools.

Complaint Rights

If you believe your request has not been properly handled, or you are otherwise dissatisfied with the outcome of your request, you have the right to request an internal review.

In the first instance, please email freedomofinformation@cumbria.police.uk quoting the FOI reference number and explain why you are dissatisfied. Your complaint will be considered, and a response will be provided to you after your complaint has been investigated.

If you remain dissatisfied following conclusion of the internal review, you have the right, under section 50 of the Freedom of Information Act, to complain directly to the Information Commissioner.

The address for the Information Commissioner can be found below:

The Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Complaints to the Information Commissioner can also be made online:

[Make a complaint | ICO](#)



EMPLOYER RECOGNITION SCHEME

BRONZE AWARD

Proudly supporting those who serve.

