

10 June 2025

FOI Ref 21292

Request - You asked us the following:

I write to request information under the Freedom of Information Act 2000. With respect to multimedia forensic processes, could you please provide me with a copy of the most recent Standard Operating Procedures (SOPs), guidance documents, or policy documents held by your force.

For clarity, by multimedia forensics I refer specifically to the forensic analysis, enhancement, authentication, interpretation, and presentation of audio, video, and still-image material. This does not include general digital forensics (such as the extraction of data from computers, mobile devices, or other storage media). I am solely concerned with processes dealing directly with audio, video, and image evidence. Specifically, please provide the material requested in the following four bullet points:

1. A copy of the SOPs, guidance documents, or policy documents covering the forensic processing, enhancement, analysis, interpretation, and presentation of audio, video, and image material for investigative or evidential purposes.
2. Any internal multimedia forensic workflows, protocols, or standard practices related to handling such material.
3. The names of software, tools, or systems used for these processes, including any associated training or operational guidance.
4. The quality assurance, validation, or review procedures used to ensure the accuracy, authenticity, and admissibility of multimedia forensic evidence.

If the full SOPs or documents cannot be shared, I kindly request the following information in place of the SOP as per the following seven points:

5. A summary or description of the multimedia forensic processes followed.
6. SOP titles, version numbers, and the dates of their creation, last update, and validation/approval.
7. The roles, departments, or individuals responsible for authoring, validating, or approving the SOPs.
8. The legislation, policies, standards, or external guidance referenced during the development and/or review of the SOPs.
9. Whether the SOPs have undergone any ethical review or approval, and details of any such review processes or bodies involved.
10. Whether the SOPs have been externally validated, peer-reviewed, or accredited by any agency, professional body, or external organization.
11. Whether any SOPs are currently under review, have recently been amended, or are scheduled for updates, and the relevant timelines if applicable.

In addition to the previous, please provide responses to the following four points regarding the use of emerging technologies:

12. Please detail whether your multimedia forensic unit currently uses or has trialled artificial intelligence (AI) or machine learning (ML) tools for:
 - o Authentication (e.g., detecting edits, deepfakes, or tampering) o



Enhancement (e.g., audio/video/image quality improvement) o Analysis or interpretation (e.g., transcription, object recognition, pattern matching) Note: a simple response is acceptable here such as "Authentication: Use. Enhancement: Trialled. Analysis: Not used"

13. If applicable, the names or vendors of the AI/ML tools used.

14. Whether the use of these tools is governed by any SOPs, internal policies, or ethical guidelines.

15. Whether the adoption and use of AI/ML tools have been subject to ethical review, oversight, or risk assessment, and any details of such reviews or assessments.

I understand some content may be subject to exemptions, and I would appreciate any available redacted, summary, or contextual information where full disclosure is not possible

We received your request on 01/05/2025 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. A copy of the SOPs, guidance documents, or policy documents covering the forensic processing, enhancement, analysis, interpretation, and presentation of audio, video, and image material for investigative or evidential purposes. – **Partially disclosed, please see accompanying file titled 'FOI 21292 Multimedia Forensic Processes Data.PDF'.**
- 2. Any internal multimedia forensic workflows, protocols, or standard practices related to handling such material. – **Withheld.**
- 3. The names of software, tools, or systems used for these processes, including any associated training or operational guidance. – **Withheld.**
- 4. The quality assurance, validation, or review procedures used to ensure the accuracy, authenticity, and admissibility of multimedia forensic evidence. – **No information held.**
- 5. A summary or description of the multimedia forensic processes followed. – **No information held.**
- 6. SOP titles, version numbers, and the dates of their creation, last update, and validation/approval.
 - **Disclosed, SPF-GF-999 Request for Custody CCTV Images Issue 1.0 – 08/08/2022 (creation, approval and last updated).**
 - SPF-GP-1105 Major Incident Forensic Strategy SOP for CCTV recovery Issue 2.0 – 15/08/2023 (creation), 02/06/2023 (approval) and 15/08/2023 (last updated).**
 - SPF-GP-1157 CCTV RETRIEVAL FROM SCENE OVERVIEW Issue 1.0 – 11/08/2023 (creation, approval and last updated).**
 - SPF-GP-1158 CCTV Downloading at Scene Issue 1.0 – 15/08/2023 (creation, approval and last updated).**
 - SPF-GS-1114 CCTV MG22a Example Not Accredited V1.0 – 03/06/2023 (creation, approval and last updated).**



SPF-GS-1207 SFR and Declaration Guidance CCTV Evidence V1 – 25/03/2024 (creation, approval and last updated).

SPF-TF-958 HQ CCTV Request Form - v1.1 – 01/04/2023 (approval) and 31/08/2023 (creation and last updated).

SPF-TF-1073 HQ CCTV DVR Examination Request Form v1 – 01/04/2023 (creation, approval and last updated).

SPF-TP-1271 Staffordshire Police CCTV Systems and Downloads v1 – 05/09/2024 (creation, approval and last updated).

- 7. The roles, departments, or individuals responsible for authoring, validating, or approving the SOPs. – **Disclosed, Forensic Investigation: Digital Forensic Media Supervisor, Forensic Coordinator, Forensic Area Manager. Digital Forensics: Digital Forensic Media Investigator, Digital Forensic Coordinator, Digital Forensic Technical Manager. Forensic Quality Services: Forensic Quality Assistant, Forensic Quality Service Officer, Forensic Quality Service Manager.**
- 8. The legislation, policies, standards, or external guidance referenced during the development and/or review of the SOPs. – **Disclosed, Forensic Regulator's Code, NPCC Framework for Video Based Evidence.**
- 9. Whether the SOPs have undergone any ethical review or approval, and details of any such review processes or bodies involved. – **Disclosed, no.**
- 10. Whether the SOPs have been externally validated, peer-reviewed, or accredited by any agency, professional body, or external organization. – **Disclosed, no.**
- 11. Whether any SOPs are currently under review, have recently been amended, or are scheduled for updates, and the relevant timelines if applicable. – **Disclosed, none currently. SOPs are reviewed against the process and if required changes are requested.**
- 12. Please detail whether your multimedia forensic unit currently uses or has trialled artificial intelligence (AI) or machine learning (ML) tools for:
 - o Authentication (e.g., detecting edits, deepfakes, or tampering)
 - o Enhancement (e.g., audio/video/image quality improvement)
 - o Analysis or interpretation (e.g., transcription, object recognition, pattern matching)Note: a simple response is acceptable here such as "Authentication: Use. Enhancement: Trialled. Analysis: Not used" – **Disclosed, none used or trialled.**
- 13. If applicable, the names or vendors of the AI/ML tools used. – **Not applicable.**
- 14. Whether the use of these tools is governed by any SOPs, internal policies, or ethical guidelines. – **Not applicable.**
- 15. Whether the adoption and use of AI/ML tools have been subject to ethical review, oversight, or risk assessment, and any details of such reviews or assessments. – **Not applicable.**

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:

To provide further documents, workflows, protocols, policies or standard practices that disclose police tactics and processes for the recovery and handling of digital forensics could undermine existing or future investigations, operations and police tactics. It would allow those with ill intent to cause disruption to operational policing and would also prejudice the prevention and detection of crime and the apprehension or prosecution of offenders.

Public Interest Test

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

To disclose this information would adhere to the basic principle of being open and transparent, it would also lead to a better public awareness of the workings of the police force and the processes used with operations and evidence gathering.

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

Releasing such data would give those individuals with the intent to do so, the intelligence required to disrupt police activity. This knowledge would allow those with ill intent to target their offending more effectively which would inevitably lead to an increased likelihood of criminal activity and an increased danger to the public. Any disclosure of information which is likely to undermine the ability to serve the public in preventing and detecting crime and apprehending and prosecuting offenders can only be considered as being harmful to the public.

Balance test

When considering whether disclosure is appropriate, we must weigh the strongest reason for disclosure against the strongest reasons for non-disclosure. In this case, whilst the factors favouring disclosure are important in that it would adhere to the basic principle of being open and transparent, we believe when weighed against the risk of disclosure undermining our ability to prevent and detect crime, apprehend and prosecute offenders and hindering our ability to protect the public, then non-disclosure takes precedence.

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



STAFFORDSHIRE
POLICE

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