

24 March 2026

FOI Ref 22670

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

1. Policies or Procedures for Archiving Mobile-Device Evidence Please provide any recorded policies, procedures, or guidance documents that describe how your Digital Forensics Unit archives mobile-device digital evidence in cold-case investigations.

If held, these may include information on:

Whether evidence is stored using the original device, a forensic image, or both.

The types of files or data normally kept (for example: full extractions, images, or generated reports).

2. Storage Methods and Formats

Please provide any recorded information describing:

The types of storage media used to keep archived mobile-device evidence (e.g., hard drives, servers, cloud storage, etc.).

The file formats in which this evidence is stored (e.g., extraction images, exported reports, etc.).

(Only information already recorded in documents, logs, or inventories is requested.)

3. Reviews or Re-Examinations of Archived Mobile-Device Evidence Please confirm whether statistics on re-examination activity are recorded, and if so, what information is held.

4. Access to Older or Legacy Formats

Please provide any recorded information on whether your Digital Forensics Unit keeps older or legacy forensic software, tools, or viewers to access mobile-device evidence stored in outdated or proprietary formats.

If recorded, please also provide any documented procedures for opening or converting older evidence formats.

5. SOPs for Reviewing Archived Evidence

Please provide any standard operating procedures (SOPs), policies, or guidance documents your Digital Forensics Unit holds that relate to the reviewing of archived mobile-device evidence in cold-case investigations.

If held, please also indicate whether these documents reference the Forensic Science Regulator's Code of Practice.

SP received your request on 16/03/2026 and have processed this under the Freedom of Information Act (FOIA).

SP's response to your enquiry is as follows:



SP holds some of the requested information.

- 1. Policies or Procedures for Archiving Mobile-Device Evidence Please provide any recorded policies, procedures, or guidance documents that describe how your Digital Forensics Unit archives mobile-device digital evidence in cold-case investigations.
- If held, these may include information on:
 - Whether evidence is stored using the original device, a forensic image, or both.
 - The types of files or data normally kept (for example: full extractions, images, or generated reports).
- **- No information held.**
- 2. Storage Methods and Formats
 - Please provide any recorded information describing:
 - The types of storage media used to keep archived mobile-device evidence (e.g., hard drives, servers, cloud storage, etc.).
 - The file formats in which this evidence is stored (e.g., extraction images, exported reports, etc.).
 - (Only information already recorded in documents, logs, or inventories is requested.)
- **- Disclosed, archived mobile device evidence is stored on USBs, CDs, DVDs, SSDs (external and internal) and HDDs (external and internal). All data from the original case file is stored, including extractions, reports, unused material.**
- 3. Reviews or Re-Examinations of Archived Mobile-Device Evidence Please confirm whether statistics on re-examination activity are recorded, and if so, what information is held.
- **- No information held.**
- 4. Access to Older or Legacy Formats
 - Please provide any recorded information on whether your Digital Forensics Unit keeps older or legacy forensic software, tools, or viewers to access mobile-device evidence stored in outdated or proprietary formats.
 - If recorded, please also provide any documented procedures for opening or converting older evidence formats.
- **- Disclosed, no legacy licenses are kept for mobile software, however previous versions of SP's current software are available from the software provider where necessary. No documented procedures are held for opening or converting older evidence formats.**
- 5. SOPs for Reviewing Archived Evidence
 - Please provide any standard operating procedures (SOPs), policies, or guidance documents your Digital Forensics Unit holds that relate to the reviewing of archived mobile-device evidence in cold-case investigations.
 - If held, please also indicate whether these documents reference the Forensic Science Regulator's Code of Practice.
- **- No information held.**

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.



STAFFORDSHIRE
POLICE

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