

26 November 2025

FOI Ref 21960

Request - You asked us the following:

Please treat the following as a request for information under the Freedom of Information Act.

From 1 January 2017 to today, does Staffordshire Police hold any licence, tenancy, or paid access (directly or via a supplier) to Relativity products.

- e-disclosure / e-discovery
- disclosure for major inquiries or criminal investigations
- Data Subject Access Requests (DSARs)
- Freedom of Information (FOI) review

If so, please provide:

- a. Whether access is direct or through a supplier (e.g., Epiq, Anexsys/Consilio, FTI, Deloitte, CCL)
- b. The contract reference(s)
- c. The first start date and current status (active or expired)
- d. Whether the tooling is used for criminal matters, civil litigation, DSAR/FOI, or public inquiries
- e. Whether the installation is SaaS, on-prem or hosted by a third party
- f. Which department or departments of the force use the software

If this information is held only in part, please provide the details that are available.

We received your request on 14/10/2025 and have processed this under the Freedom of Information Act (FOIA).

We initially responded to your request on 27/10/2025, however we have revised our response since that date. Please destroy the previous response to this FOI request and treat this as the final response from Staffordshire Police.

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

Staffordshire Police can neither confirm nor deny whether information relevant to this request is held, as the duty in Section 1(1)(a) of the Freedom of Information Act 2000 does not apply by virtue of the following exemptions:

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

- Section 24 (2) – National Security

Section 24 is a qualified exemption and as such there is a requirement to articulate the harm and conduct a test of the public interest.

- Section 31 (3)- Law Enforcement.

Section 31 is a qualified and prejudice-based exemption and, as such, we are required to evidence the harm in disclosure and apply the public interest test.

Harm

After careful consideration, Staffordshire Police (SP) can neither confirm nor deny whether the requested information is held.

Any disclosure under FOI is a release to the public at large. Under the Act, we cannot, and do not request the motives of any application for information. We have no doubt that most requests made under the Act are legitimate and the applicants do not have any ulterior motives. Whilst not questioning the motives behind this specific request, confirming or denying whether Relativity Software is used would reveal details about the technological capabilities and security posture of SP. This information could be exploited by hostile actors or organised crime groups to identify vulnerabilities, target specific systems, or develop countermeasures. Such knowledge could undermine national security by facilitating cyberattacks or compromising sensitive investigations that intersect with counter-terrorism or serious organised crime.

Confirming or denying whether Relativity Software, or other such systems, are in use could prejudice the prevention and detection of crime by indicating the technological capabilities available to SP. Awareness of specific platforms could enable individuals' intent on criminal activity to adjust their methods (such as avoiding creating digital evidence that a system is designed to detect), exploit potential weaknesses in the platform, or attempt to compromise secure environments, such as crafted cyberattacks. This would risk undermining investigative effectiveness, jeopardise evidential integrity, and ultimately threaten the safety of victims, witnesses, and officers.

Confirming or denying whether these systems are used would not only risk compromising the security posture of SP but, when combined with responses from other forces, could create a mosaic of intelligence about law enforcement capabilities nationally. Adversaries could use this aggregated information to identify which forces employ certain technologies, infer operational strengths and weaknesses, and target specific systems or regions. This would prejudice the prevention and detection of crime, undermine investigative effectiveness, and increase the risk of cyberattacks and exploitation across multiple forces. For these reasons, maintaining a consistent neither confirm nor deny position is essential to protect law enforcement operations and public safety.

Public Interest Test

Factors favouring Confirming or Denying for Section 24

The information, if held, relates to national security and transparency could reassure the public that appropriate measures are in place. By confirming or denying if business is conducted with Relativity Software, or any other likeminded eDiscovery provider, would lead to a better informed public.

Factors against Confirming or Denying for Section 24

By confirming or denying whether any information is held would render policing and security measures less effective. This would lead to the compromise of ongoing or future operations to protect the security or infra-structure of the UK and increase the risk of harm to the public.

Factors favouring Neither Confirming or Denying for Section 31

Confirming or denying whether business is conducted with Relativity Software, or similar eDisclosure providers, could enhance public understanding of the Police Service's effectiveness and technology choices. Transparency in this area would help ensure accountability for public spending and demonstrate that resources are being used appropriately. It would also support informed public debate about law enforcement's digital capabilities, reducing speculation and misinformation. Where significant investment in technology occurs, there is a legitimate public interest in knowing how funds are allocated and whether such tools contribute to operational efficiency.

Factors against Confirming or Denying for Section 31

Confirming or denying whether any information is held regarding engagement with Relativity Software or similar eDisclosure providers, would risk compromising law enforcement tactics and investigative processes. FOIA disclosures are monitored by individuals intent on criminal activity and hostile actors; therefore, acknowledging the use of specific platforms could provide insight into operational capabilities. This knowledge could enable adversaries to adapt their methods, exploit potential weaknesses, or attempt to compromise secure environments.

The Police Service relies on a range of techniques and technologies to gather intelligence and manage evidence, and revealing whether such tools are in use would prejudice the ability to prevent and detect crime. It could undermine investigations, increase the risk of cyberattacks, and ultimately place victims, witnesses, and officers at greater risk. Confirming or denying this information may also indicate relative vulnerabilities in law enforcement systems, which could be exploited to defeat security measures.

Balance Test

The security of the country and the integrity of law enforcement operations are of paramount importance. SP will not confirm or deny whether any information is held regarding business with Relativity Software, or any similar third-party provider, if doing so would place individuals at risk, undermine national security, or compromise policing tactics.

While there is a legitimate public interest in transparency around police technology choices and assurance that SP are effectively addressing threats, this is outweighed by the very strong public interest in safeguarding investigative integrity and operational security across UK policing. Confirming or denying the existence of such information could reveal sensitive capabilities, expose vulnerabilities, and assist those intent on criminal activity or hostile acts.

Although the public has an interest in knowing that policing activity is appropriate and proportionate, this interest will only override operational security in exceptional circumstances. The use of technology in investigations is a sensitive matter, and disclosure—even by confirmation or denial—could prejudice law enforcement functions. Therefore, the balance of the public interest lies firmly in maintaining a Neither Confirm Nor Deny position.

This should not be taken as indicating that any information meeting your request does or does not exist.



STAFFORDSHIRE
POLICE

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 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 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 20 working days. In more complex cases the review may take up to 40 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, taking into account 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