

5 June 2026

FOI Ref 22859

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

I am writing to make a request under the Freedom of Information Act 2000. I would be grateful if you could provide the following information relating to Staffordshire Police's telephony and contact centre systems. Much of this information is available through looking at past tenders, but I would really appreciate a more thorough breakdown.

SECTION 1 — CORE TELEPHONY PLATFORM

Q1. What telephony platform(s) does the force currently use? (e.g. Avaya, Mitel, Cisco, Microsoft Teams, other — please name the product and version where known)

Q2. Are these systems hosted on-premise, in a private cloud, or in a public cloud environment?

Q3. Who is the primary supplier/integrator responsible for delivering and supporting the telephony platform?

Q4. When do the contracts expire (month and year)? and are there plans for a new tender

SECTION 2 — CONTACT CENTRE / 999 AND 101 HANDLING

Q5. What platform is used for your force contact operations centre (handling 999 and 101 calls)? (e.g. Avaya Aura Contact Centre, Genesys, NICE CXone, other)

Q6. What Session Border Controller (SBC) product is used to connect your SIP trunks to the public network? (e.g. Oracle/Acme Packet, Avaya SBCE, Cisco CUBE, AudioCodes)

Q7. What workforce management system is used (if any)?

Q8. What call recording system is in use within the contact centre? (e.g. NICE, Verint, Redbox etc)

SECTION 3 — UNIFIED COMMUNICATIONS AND WIDER INFRASTRUCTURE

Q9. Does the force use Microsoft Teams for internal communications? If so, is Teams also used for any telephony (Direct Routing or Operator Connect)?

Q10. What Integrated Communications Control System (ICCS) is in use in the force control room? (e.g. Frequentis, Zetron, other)

Q11. What is the procurement route used for telephony and communications contracts? (e.g. Crown Commercial Service framework, direct award, open tender, regional collaboration)

SECTION 4 — REFRESH AND PIPELINE

Q12. Are there any active or planned procurements for replacement or upgrade of the telephony or contact centre platform in the next 24 months?

SP received your request on 11/05/2026 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.

SECTION 1 — CORE TELEPHONY PLATFORM

- Q1. What telephony platform(s) does the force currently use? (e.g. Avaya, Mitel, Cisco, Microsoft Teams, other — please name the product and version where known) – **Disclosed, Gamma.**
- Q2. Are these systems hosted on-premise, in a private cloud, or in a public cloud environment? – **Withheld.**
- Q3. Who is the primary supplier/integrator responsible for delivering and supporting the telephony platform? – **Withheld.**
- Q4. When do the contracts expire (month and year)? and are there plans for a new tender – **Disclosed, May 2030. No plans for a new tender.**

SECTION 2 — CONTACT CENTRE / 999 AND 101 HANDLING

- Q5. What platform is used for your force contact operations centre (handling 999 and 101 calls)? (e.g. Avaya Aura Contact Centre, Genesys, NICE CXone, other) – **Withheld.**
- Q6. What Session Border Controller (SBC) product is used to connect your SIP trunks to the public network? (e.g. Oracle/Acme Packet, Avaya SBCE, Cisco CUBE, AudioCodes) – **Withheld.**
- Q7. What workforce management system is used (if any)? – **Disclosed, none.**
- Q8. What call recording system is in use within the contact centre? (e.g. NICE, Verint, Redbox etc) – **Disclosed, STORM/Red Box.**

SECTION 3 — UNIFIED COMMUNICATIONS AND WIDER INFRASTRUCTURE

- Q9. Does the force use Microsoft Teams for internal communications? If so, is Teams also used for any telephony (Direct Routing or Operator Connect)? – **Disclosed, Teams is only used for internal communications.**
- Q10. What Integrated Communications Control System (ICCS) is in use in the force control room? (e.g. Frequentis, Zetron, other) – **Withheld.**

- Q11. What is the procurement route used for telephony and communications contracts? (e.g. Crown Commercial Service framework, direct award, open tender, regional collaboration) – **Disclosed, Direct Award through a framework.**

SECTION 4 — REFRESH AND PIPELINE

- Q12. Are there any active or planned procurements for replacement or upgrade of the telephony or contact centre platform in the next 24 months? – **Disclosed, none.**

The following exemptions have 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 24 (1) – 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 (1)(a)(b) Law Enforcement

Information is exempt from disclosure under S31(1)(a)(b) where the release of Information would, or would be 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:

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 have no control over what use is made of that information.

The Police Service is charged with enforcing the law, preventing and detecting crime and protecting communities. In order to achieve these objectives all forces have a telephony and communications network infrastructure to support the vital information technology essential to front line services. Disclosure of specific IT services, capabilities, or the lack thereof, in concert with any formal acknowledgement of strategic deficiency would reveal intricacies of those systems thereby highlighting vulnerabilities and compromising individual force information assurance.

As this request has been received nationally, disclosure would enable a geographical picture to be drawn up by those individuals who are intent on 'hacking' or defeating police systems; some of these individuals may include terrorists or terrorist organisations. In terms of duty of care, this would be detrimental to the public at large as disclosure could assist a malicious actor by highlighting vulnerable forces and leaving those forces open to disruption of Information Technology systems; thus compromising the effective delivery of operational law enforcement which in turn, is met by an increase of criminal offending.

Public Interest Test

Factors favouring disclosure under Section 24 (1) & Section 31(1)(a)(b)

Providing information in respect of SP's network infrastructure would allow the public to be better informed on the health, state and performance of said Information Technology platform. In addition, forces are required to demonstrate efficient services to local taxpayers and satisfy audit requirements. This would provide transparency with regard to the use of public funds by highlighting that funds are being used to correctly and appropriately ensure all forces have adequate infrastructure, which results in the smooth running of force Technology systems.

Factors favouring non-disclosure under Section 24 (1) & Section 31(1)(a)(b)

Whilst there is public interest in providing reassurance that police forces are appropriately and effectively dealing with any threats posed by terrorist organisations against police technology capabilities, there is also a strong public interest in safeguarding National Security and the welfare and safety of the general public at large. Any disclosure has the potential to undermine current and future data integrity. This in turn could compromise the force's mandate to protect the security of the United Kingdom, increasing the risk of significant harm or even death to the community. Any disclosure of information that may lead to force IT systems being compromised, ultimately affects law enforcement capabilities and hinders the prevention and detection of crime or terrorism, is not in the interest of the public.

Balance Test

The security of the country is of paramount importance therefore, the Police service will not divulge any information if to do so would undermine law enforcement and compromise the work of the police service. Whilst there is a public interest in the transparency of policing and force infrastructure, including any initiatives conducted with the private sector, there is a very strong public interest in safeguarding the integrity of these arrangements in this very sensitive area.

The points above highlight the merits for and against disclosure of the requested information. Disclosure would undoubtedly provide a greater openness and transparency to the community at large with regard to the information technology resources available to the police. Whilst there is always a public interest in the transparency of how a police force delivers effective law enforcement and ensures the National Security of the United Kingdom is robust, there is a very strong public interest in safeguarding the intricacies and tactical capabilities of the systems used when dealing with information.

In every case, public safety is the paramount focus and any information which would place individuals at risk and compromise the National Security of the United Kingdom, no matter how generic, is not in the public interest. The effective delivery of operational law enforcement and the National Security of the United Kingdom is crucial and of paramount importance to every force. This would have a negative impact on law enforcement and national security.

All Freedom of Information request responses are published on the SP website although personal details are not included.



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 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