

21 January 2025

FOI Ref 17512

Request - You asked us the following:

Please advise the products that your forces uses for;

Command & Control Application
ICCS Application
Mobile Working Application(s)
Mobile Working Hardware
Airwave Handsets
Airwave Mobile Sets
ICCS Desktop Sets
ICCS Portable Sets
ICCS Infrastructure

Detail if these products are owned outright, leased or part of a managed service. Where products are owned outright, list any support contracts for these.

Detail any managed service contracts, start dates & renewal dates.

If any of the above products & technologies are due to be replaced and their replacement has been chosen, also detail the requested information for these.

Where products are shared with another service/force/agency, please detail this and who the lead service/force/agency is.

Where there is more the one instance of an application in your organisation, please also detail that.

For example, you may have multiple, single site, unconnected ICCS setups rather than one, mjlti-site, connected ICCS setup. In this context, the former would be considered more than one instance whereas the latter would be considered a single instance.

CLARIFICATION RECEIVED ON 06/12/2024

When referring to the products, it is the systems described in my original request.

The sharing with other agencies refers to being one of many forces/agencies on the product. For example, you may share an ICCS platform with a neighbouring force.

We received your request on 25/11/2024 and have processed this under the Freedom of Information Act (FOIA).

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



Staffordshire Police holds some of the requested information.

- Please advise the products that your forces uses for;
- Command & Control Application – **Disclosed, STORM License, support and maintenance.**
- ICCS Application – **Withheld.**
- Mobile Working Application(s) – **Disclosed, Pronto Software Licence and Professional Services.**
- Mobile Working Hardware – **Disclosed, Samsung Warranty.**
- Airwave Handsets – **Disclosed, Sepura SC20 Warranty.**
- Airwave Mobile Sets – **Withheld.**
- ICCS Desktop Sets – **No information held.**
- ICCS Portable Sets – **No information held.**
- ICCS Infrastructure – **Withheld.**
- Detail if these products are owned outright, leased or part of a managed service. Where products are owned outright, list any support contracts for these. – **Disclosed, Pronto is a licence subscription and we pay a subscription charge which includes support along with fixed professional service fees for new development. STORM we have the right to use the software only whilst in contract with the supplier. The contractual charges relate to support and maintenance of the software. The following hardware is all owned, Mobile Working Hardware and Airwave Handsets.**
- Detail any managed service contracts, start dates & renewal dates. – **Disclosed**
Command & Control Application: STORM 01/04/2024 – 31/03/2027
Mobile Working Application(s): Pronto 01/04/2023 – 31/03/2026
Mobile Working Hardware: Samsung Various Dates
Airwave Handsets: Sepura SC20 Various Dates
- If any of the above products & technologies are due to be replaced and their replacement has been chosen, also detail the requested information for these. – **Withheld.**
- Where products are shared with another service/force/agency, please detail this and who the lead service/force/agency is. – **Not applicable.**
- Where there is more the one instance of an application in your organisation, please also detail that. – **Not applicable.**
- For example, you may have multiple, single site, unconnected ICCS setups rather than one, multi-site, connected ICCS setup. In this context, the former would be considered more than one instance whereas the latter would be considered a single instance. – **Not applicable.**
- CLARIFICATION RECEIVED ON 06/12/2024
- When referring to the products, it is the systems described in my original request.
- The sharing with other agencies refers to being one of many forces/agencies on the product. For example, you may share an ICCS platform with a neighbouring force.

Please note that this data has been provided to the best of our ability, subject to the limitation of current recording protocols and systems/software.

Every effort is made to ensure that the data presented is accurate and complete. However, it is important to note that this has been extracted from multiple sources, developed for specific policing purposes, for which data extraction methods have not been specifically designed to directly correlate with the terminology of this request. Therefore, the data presented is subject to the inaccuracies and idiosyncrasies inherent in any large-scale recording system.

As a consequence, care should be taken in the interpretation and presentation of this data, so as to not misrepresent the whole or any part of the data disclosed.

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 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 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.

- Section 43(2) Commercial Interests

Section 43 is a class based qualified exemption which means there is no requirement to provide the harm but a public interest test needs to be considered.

Evidence of Harm – Section 24(1) and Section 31(1)

Every effort should be made to release information under Freedom of Information. However an FOI 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 the communities we serve. 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 for Section 24(1) and Section 31(1)

Providing information in respect of Staffordshire Polices 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 in so much as 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 for Section 24(1) and Section 31(1)

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 force Technology capabilities, there is 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, which in turn compromises the force's mandate to protect the security of the United Kingdom, e.g. counter-terrorism activity. The risk of significant harm or even death to the community at large would be increased. Any disclosure of information that may lead to compromise of force IT systems which ultimately affects law enforcement capabilities and hinders the prevention and detection of crime or terrorism, is not in the interest of the public.

Factors favouring disclosure for Section 43(2)

Disclosure of the requested information would allow the public to be aware of how public funds are spent or allocated and thereby would provide transparency and accountability, showing that funds from the public purse are used appropriately and proportionally.

Factors favouring non-disclosure for Section 43(2)

Through disclosure of the requested information, Staffordshire Police would find that its negotiating position would be greatly impaired through the release of details that would not only likely be prejudicial to Staffordshire Police but also to the agencies/companies involved. Releasing this information would be expected to have a detrimental effect on their ability to be competitive in the future and would be exceedingly likely to deter further enterprises submitting offers for tender in the future. This then would impede Staffordshire Police obtaining the most competitive or appropriate services in the future and negatively impact upon the public purse.

Balance Test

The security of the country is of paramount importance and the Police service will not divulge any information if to do so would undermine law enforcement and therefore 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 in relation to impacting on the crime or terrorist threat,

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, and 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.

It is the responsibility of Staffordshire Police, when dealing with commercial businesses, to not only protect their commercial interest but also that of Staffordshire Police. Commercial interests must be protected so that the best possible value for money is obtained through open competition, both for businesses and Staffordshire Police. This would not be achieved if full details were to be made available to the market. Although the use of public funds must be open and transparent, Staffordshire Police is accountable for the money that it spends and utilizes and if to release the information means the force is unable to negotiate future tendering and have the ability to secure value for money due to business relationships have been impaired, then this would not be in the public interest.

Having considered the public interest test factors, we are required to determine whether, on balance, the factors favouring disclosure outweigh those which are against disclosure. It is our view that the factors favouring disclosure do not outweigh those which favour withholding the details. Therefore, Staffordshire Police declines to provide the information for the reasons stated above.

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
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