



21 October 2024

FOI Ref 17085

Request - You asked us the following:

Networks

1. What network vendor(s) / service provider does your emergency service currently use for their LAN, WAN,, wireless and core network (e.g., BT, Virgin, Cisco)?
2. Is the network managed / run internally, or is the network managed and/or supplied by a third party? Please specify which elements of the network are outsourced and to which companies.
3. Please may you provide an indication of the size of the network (e.g., number of switches, routers, access points etc.)?
4. How much money was spent on the last major network refresh (referring to replacement of the LAN / WAN / core network)?
5. When was the last major network refresh (month & year)?
6. When is the next major network refresh likely to take place (month & year)?
7. What frameworks are likely to be used when releasing a tender for a network refresh?

Cyber Security

1. Which cyber security providers / vendors are used, and for what technologies (e.g., firewalls, SOC etc.)?
2. When is your service due for a renewal of these technologies (month & year)?
3. Is all cyber security managed in-house, or is it / parts of it outsourced to a third party? Please specify which elements are outsourced and to which companies.

Command and Control

1. Which technology suppliers / vendors are used in your command and control rooms?
2. Is your command and control room managed in-house, or is it / parts of it outsourced to a third party? Please specify which elements are outsourced and to which companies.
3. How much was spent on the last major command and control technology refresh (referring to the replacement of the CAD / ICCS)?
4. When was the last command and control technology refresh (month & year)?
5. When is the next command and control technology refresh likely to take place (month & year)?

We received your request on 24/07/2024 and have processed this under the Freedom of Information Act (FOIA).

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

Staffordshire Police holds the requested information.

Networks

- 1. What network vendor(s) / service provider does your emergency service currently use for their LAN, WAN,, wireless and core network (e.g., BT, Virgin, Cisco)? – **Partially disclosed, Virgin Media is our WAN provider. Other elements are Withheld.**



- 2. Is the network managed / run internally, or is the network managed and/or supplied by a third party? Please specify which elements of the network are outsourced and to which companies. – **Disclosed, managed internally.**
- 3. Please may you provide an indication of the size of the network (e.g., number of switches, routers, access points etc.)? – **Disclosed, Switches x 170, Routers x 45, APs x 200, interfaces 10k.**
- 4. How much money was spent on the last major network refresh (referring to replacement of the LAN / WAN / core network)? – **Disclosed, nil.**

The purchases were undertaken by Staffordshire Police and the delivery continued in house following the transition in force.

- 5. When was the last major network refresh (month & year)? – **Disclosed, 2020.**
- 6. When is the next major network refresh likely to take place (month & year)? – **Disclosed, 2025/26.**

Please keep in mind that this projection begins in 2025/26, thus we cannot specify a specific month.

- 7. What frameworks are likely to be used when releasing a tender for a network refresh? – **Disclosed, this would be assessed at the time as part of the procurement planning process.**

Cyber Security

- 1. Which cyber security providers / vendors are used, and for what technologies (e.g., firewalls, SOC etc.)? – **Withheld.**
- 2. When is your service due for a renewal of these technologies (month & year)? – **Disclosed, May 2025.**
- 3. Is all cyber security managed in-house, or is it / parts of it outsourced to a third party? Please specify which elements are outsourced and to which companies. – **Partially disclosed, this includes a mix of in-house and 3rd party. Further breakdown is withheld.**

Command and Control

- 1. Which technology suppliers / vendors are used in your command and control rooms? – **Disclosed, Storm.**
- 2. Is your command and control room managed in-house, or is it / parts of it outsourced to a third party? Please specify which elements are outsourced and to which companies. – **Disclosed, in-house.**
- 3. How much was spent on the last major command and control technology refresh (referring to the replacement of the CAD / ICCS)? – **Disclosed, £460,000.**

- 4. When was the last command and control technology refresh (month & year)? – **Disclosed, May 2022.**
- 5. When is the next command and control technology refresh likely to take place (month & year)? – **Disclosed, February 2025.**

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 31 (1) (a) (b) - Law Enforcement.

Information is exempt from disclosure under section 31 (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

This is a prejudice based qualified exemption which means there is a requirement to provide evidence of harm and a public interest test needs to be considered.

Harm:

To provide the individual for network and cyber security providers could highlight successful attacks and potential vulnerabilities. This knowledge could help attackers refine their methods to improve their chances of success. Moreover, to combat criminal and terrorist activities, it is crucial for the police and other agencies to collaborate, sometimes covertly, to gather intelligence within the bounds of current legislation. This collaboration is essential for the arrest and prosecution of individuals who commit or plan to commit acts of terrorism, which may include cyber-attacks on secure databases. Effective information sharing among police forces and security bodies across the United Kingdom is vital to support counter-terrorism efforts and disrupt terrorist networks.

Therefore, releasing certain details about breaches in information technology and security would be highly beneficial to those engaged in terrorist activities, as it would help them identify vulnerable information security databases. This would have a huge impact on the effective delivery of operational law enforcement as it would leave forces open to cyberattack which could render computer devices obsolete. This would allow individuals to speak on the policing network with a level of validity that could lead to major disruption to the force communications network. It would also aide criminals in disrupting events involving these areas.

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 communications used with operations and during routine policing.

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 can only be considered as being harmful to the public.

Factors favoring disclosure under 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 favoring non-disclosure under 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

Staffordshire Police is charged with enforcing the law, preventing and detecting crime and protecting the communities we serve. As part of that policing purpose, information is gathered which can be highly sensitive relating to high profile investigative activity. Weakening the mechanisms used to monitor any type of criminal activity, and specifically terrorist activity would place the security of the country at an increased level of danger.

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 and hindering our ability to protect the public, then non-disclosure takes precedence.

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.



STAFFORDSHIRE
POLICE

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.

Next steps

You can ask us to review our response.

If you would like us to carry out a review of our response, please let us know within two months of the date of receipt of this email, review requests should be addressed to:

foi@staffordshire.police.uk

Or by Post to:

Central Disclosure Unit
Staffordshire Police HQ
PO Box 3167
Stafford
ST16 9JZ

Please remember to quote the reference number in any future communications.

Freedom of Information
Central Disclosure Unit