

WILTSHIRE POLICE



Force Disclosure Unit

Police Headquarters
London Road
DEVIZES
Wiltshire
SN10 2DN

Date: 16th April 2024

Ref: FOI 2024/030

Dear,

I write in connection with your request for information dated 7th January 2024 concerning our ICT services. My apologies for the delay.

I am required by the Freedom of Information Act 2000 to handle all requests in a manner that is blind as to the identity and motives of the requestor. Any information released as a response to a request is regarded as being published and therefore in the public domain without caveat.

Your request for information has now been considered and after having consulted our ICT department – I am now able to respond as follows.

You wrote & our response:

Who provides your WAN and internet connectivity and the annual spend on each?
BT provide both – MPLS spend – £219,000 p.a. – Internet - £55,108 p.a.

Have you or do you plan to deploy SD Wan services?
We don't have any SD-WAN services – currently reviewing if we will use them in the future.

Have you got SIP trunks? If so, who from and confirm annual spend?
Yes – from BT cost £23,575 p.a.

Please confirm who provides your LAN, WIFI and Security infrastructure and can you please confirm your annual spend on each?
LAN – Juniper – approximately £25k per year.
Wifi – HPE Aruba – £49,000 per year.
Firewalls – Checkpoint – £32,000 per year.

Please confirm your data centre switching and security infrastructure and have you deployed cloud-based security and threat management?
Wiltshire Police can neither confirm nor deny that it holds any information in relation to this question as the duty in S1(1)(a) of the Freedom of Information Act 2000 does not apply, by virtue of the following exemptions:

Proud to serve and protect our communities

- Section 24(2) National Security;
- Section 31(3) Law Enforcement;

Sections 24(2) and 31(3) are qualified, prejudice-based exemptions and require evidence of harm and a public interest test to be carried out before they can be relied upon.

Evidence of 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 the communities they serve. In order to achieve these objectives all forces utilise Information Technology essential to front line services. Disclosure of information regarding certain IT services, capabilities and security infrastructure in concert with any formal acknowledgement of strategic deficiency, would reveal intricacies of those systems thereby highlighting vulnerabilities and compromising individual force information assurance.

To confirm or deny whether information is held in relation to data centre switching, security infrastructure and cloud based security and threat management, would release sensitive information around the force's network infrastructure. It would place the network infrastructure at increased risk of attack, as the information could be used by individuals with criminal intent to help identify and navigate around current security measures. This subsequently impacts on the effective delivery of operational law enforcement as it would leave forces open to cyber-attack which could render computer devices essential to critical policing functions obsolete.

This type of information would be extremely beneficial to offenders, including terrorists and terrorist organisations. It is vitally important that information sharing takes place to support counter-terrorism measures in the fight to deprive terrorist networks of their ability to commit crime. To confirm or deny information is held about data centre switching, security infrastructure and cloud based security and threat management, would be extremely useful to those involved in terrorist activity as it would enable them to map vulnerable information security databases. These risks are all the more relevant when requests are made to multiple forces as disclosure would enable a geographical picture to be drawn up by those individuals who are intent on 'hacking' police systems.

Public Interest Considerations

Section 24(2) National Security

Factors favouring complying with Section 1(1)(a) confirming that information is held:

The public are entitled to know how public funds are spent and how resources are distributed within an area of policing. To confirm or deny whether information is held, would enable the general public to hold the police to account on the appropriate security measures and systems they have in place, and enable improved public debate into this subject in terms of the use of public funds.

Proud to serve and protect our communities

Factors against complying with Section 1(1)(a) confirming or denying that information is held:

Security measures are put in place to protect the community we serve. As evidenced within the harm to confirm information is held would highlight to terrorists and individuals intent on carrying out criminal activity vulnerabilities within the police service.

Taking into account the current security climate within the United Kingdom, no information (such as the citing of an exemption which confirms information pertinent to this request is held, or conversely, stating 'no information is held') which may aid a terrorist should be disclosed. To what extent this information may aid a terrorist is unknown, but it is clear that it will have an impact on a force's ability to monitor terrorist activity.

Irrespective of what information is or isn't held, the public entrust the Police Service to make appropriate decisions with regard to their safety and protection and the only way of reducing risk is to be cautious with what is placed into the public domain.

The cumulative effect of terrorists gathering information from various sources would be even more impactful when linked to other information gathered from various sources about terrorism. The more information disclosed over time will give a more detailed account of the tactical infrastructure of not only a force area, but also the country as a whole.

Any incident that results from such a disclosure would, by default, affect National Security.

Section 31(3) Law Enforcement

Factors favouring complying with Section 1(1)(a) confirming that information is held:

Confirming whether or not information exists, would lead to a better informed public and may encourage individuals to provide intelligence in order to reduce the risk of police networks being hacked.

Factors against complying with Section 1(1)(a) neither confirming nor denying that information is held:

Confirmation or denial information is held in relation to data centre switching, security infrastructure and cloud based security and threat management would undermine current and future technological integrity, which in turn compromises the force's mandate to protect the safety of the public through effective policing practices. Confirming or denying information is held is intelligence to those who would wish to exploit vulnerabilities in the service and compromise of force IT systems. Ultimately this negatively affects law enforcement capabilities, hinders the prevention and detection of crime and risks public safety.

Confirmation or denial that information is held would suggest the police take their responsibility to protect information and information systems from unauthorised access, destruction, etc., dismissively and inappropriately.

Can you provide contact details for your procurement lead / category manager for these services?

Proud to serve and protect our communities

Mark Levitt – Mark.levitt@wiltshire.police.uk.

Can you provide names and contact details for the following people within your organisation?

- CIO / IT Director – N/A.
- Head of IT – Mark Levitt – Mark.levitt@wiltshire.police.uk.
- Head of Digital Transformation – N/A.
- Head of Infrastructure – N/A.
- Head of Networking – Justin Buszard – Justin.buszard@wiltshire.police.uk.
- Information/Cyber Security Manager – Neil Cowling – neil.cowling@wiltshire.police.uk.

Section 17 of the Freedom of Information Act 2000 requires the Wiltshire Police, when refusing to provide such information (because the information is exempt) to provide you the applicant with a notice which: (a) states that fact, (b) specifies the exemption in question and (c) states (if that would not otherwise be apparent) why the exemption applies.

The exemption applicable to the information requested is:

- Section 24(2) National Security;
- Section 31(3) Law Enforcement;

In accordance with Section 17 of the Act, this letter represents a Refusal Notice for this particular request.

I am satisfied that all the relevant information has been passed to me and been considered in the light of your request within the time constraints applicable under the legislation.

Wiltshire Police would like to thank you for the interest that you have shown in the Force.

Yours sincerely,

Force Disclosure Decision Maker

Wiltshire Police offers a re-examination of your case under its review procedure.



Force Disclosure Unit

Wiltshire Police HQ, London Road, Devizes, Wiltshire SN10 2DN

Freedom of Information Request Appeals Procedure

1. Who Can Ask for a Review

Any person who has requested information from Wiltshire 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 to the:

Force Disclosure Unit
Wiltshire Police Headquarters,
London Road, Devizes,
Wiltshire,
SN10 2DN

Email at disclosure@wiltshire.police.uk.

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 Force Disclosure Unit within 20 working days of the Force's response to the original FOI request.

3. Review Procedure

Receipt of a request for review will be acknowledged in writing to include confirmation of the reasons for the review. The review will be conducted by another Decision Maker, who is independent from the original Decision Maker. The Force 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 twenty 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.

Proud to serve and protect our communities

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
Tel: 01625 545 700
Fax: 01625 524 510
Email: mail@ico.gsi.gov.uk