Freedom of Information Request Reference Nº: FOI 002400-20

I write in connection with your request for information received by Suffolk and Norfolk Constabularies on 14 July 2020 which you sought access to the following information:

1. *"How many people are employed by your organisation, including full time and part time?*
2. *What is your current intranet solution? (Sharepoint, Wordpress, Invotra, etc)*
3. *How long have you been using this intranet solution?*
4. *When is your intranet contract up for renewal?*
5. *What is your annual intranet budget?*
6. *Do you share an intranet/IT services with other organisations, if so who?*
7. *Which team and/or individual(s) are responsible for managing your intranet internally?*
8. *Are you using the Office 365 suite? If so, which applications from the suite are in use?*
9. *Which team and/or individual(s) are responsible for your intranet's procurement within the organisation?*
10. *Is your Active Directory hosted on-premise, or in the cloud?*
11. *Could you provide us with a link to your Digital Workplace Strategy?"*

Response to your Request

The response provided below is correct as of 17 July 2020

Suffolk and Norfolk Constabularies have considered your request for information and the response is below.

1. The total number of employees within Norfolk and Suffolk Constabularies is provided below:

	Norfolk		Suffolk	
	Head count	**FTE**	**Head count**	**FTE**
OFFICER	1683	1633.9	1227	1201.3
PCSO			44	41.2
STAFF	1323	1179.4	981	867.6
Grand Total	**3006**	**2813.3**	**2252.0**	**2110.**

2. The Constabularies intranet solution is Sharepoint.

3. This has been used for over 6 years.

4. The contract was up for renewal in April 2020

5. There is no budget for the intranet.

6. We do not share intranet/IT services with other organisations.

7. The Digital Media Team are responsible for managing the intranet.

8. Suffolk and Norfolk Constabularies can neither confirm nor deny whether it uses Office 365, as the duty in Section 1(1)(a) of the Freedom of Information Act 2000 does not apply by virtue of the following exemptions:

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

   Sections 24 and 31 being prejudice based qualified exemptions, both evidence of harm and public interest considerations need to be articulated to the applicant.

   Harm in Confirming or Denying that Information is held

   Policing is an information-led activity, and information assurance (which includes information security) is fundamental to how the Police Service manages the challenges faced. In order to comply with statutory requirements, the College of Policing Authorised Professional Practice for Information Assurance has been put in place to ensure the delivery of core operational policing by providing appropriate and consistent protection for the information assets of member organisations, see below link:

   https://www.app.college.police.uk/app-content/information-management/

   To confirm or deny whether The Constabularies use a certain operating system would identify vulnerable computer systems and provide actual knowledge, or not, that this software is used within individual force areas. In addition, 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 type of information would be extremely beneficial to offenders, including terrorists and terrorist organisations. It is vitally important that information sharing takes place with other police forces and security bodies within the UK to support counter-terrorism measures in the fight to deprive terrorist networks of their ability to commit crime.

   To confirm or deny whether or not the Constabularies rely on a certain operating system would be extremely useful to those involved in terrorist activity as it would enable them to map vulnerable information security databases.

Public Interest Considerations

Section 24(2) National Security

Factors favour 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 whether the Constabularies utilise Office 365 would enable the general public to hold constabularies to account by highlighting forces who use out of date software. In the current financial climate of cuts and with the call for transparency of public spending this would enable improved public debate into this subject.

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 forces.

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 impactive 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 that information exists relevant to this request would lead to a better informed public which 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 that information is held in this case would suggest the Constabularies take their responsibility to protect information and information systems from unauthorised access, destruction, etc., dismissively and inappropriately.

Balancing Test

The points above highlight the merits of confirming or denying the requested information exists. The Police Service 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.

In order to comply with statutory requirements and to meet NPCC expectation of the Police Service with regard to the management of information security a national policy approved by the College of Policing titled National Policing Community Security Policy has been put in place. This policy has been constructed to ensure the delivery of core operational policing by providing appropriate and consistent protection for the information assets of member organisations. A copy of this can be found at the below link:

http://library.college.police.uk/docs/APP-Community-Security-Policy-2014.pdf

In addition, anything that places that confidence at risk, no matter how generic, would undermine any trust or confidence individuals have in the Police Service.

Therefore, at this moment in time, it is our opinion that for these issues the balance test favours neither confirming nor denying that information is held.

9. The 7 Force Procurement Department are responsible for the intranet's procurement.

10. The active directory is on-premise.

11. The Constabularies digital media strategy is attached.

Should you have any further queries concerning this request, please contact Clair Pack, FOI Decision Maker, quoting the reference number shown above.

A full copy of the Freedom of Information Act (2000) can be viewed on the 'Office of Public Sector Information' web-site;
http://www.opsi.gov.uk/

Norfolk and Suffolk Constabularies are not responsible for the content, or the reliability, of the website referenced. The Constabulary cannot guarantee that this link will work all of the time, and we have no control over the availability of the linked pages.

Your Right to Request a Review of Decisions Made Under the Terms of the Freedom of Information Act (2000).

If you are unhappy with how your request has been handled, or if you think the decision is incorrect, you have the right to ask the Norfolk and Suffolk Constabulary to review their decision.

Ask Norfolk and Suffolk Constabularies to look at the decision again.

If you are dissatisfied with the decision made by Norfolk and Suffolk Constabularies under the Freedom of Information Act (2000), regarding access to information, you must notify the Norfolk and Suffolk Constabulary that you are requesting a review within 20 days of the date of its response to your Freedom of Information request. Requests for a review should be made in writing and addressed to:

Freedom of Information Decision Maker
Information Management Department
Suffolk Constabulary
Police Headquarters
Martlesham Heath
Ipswich
Suffolk
IP5 3QS
OR
Email: information@suffolk.pnn.police.uk

In all possible circumstances Norfolk and Suffolk Constabulary will aim to respond to your request for us to look at our decision again within 40 working days of receipt of your request for an internal review.

The Information Commissioner.

After lodging a request for a review with Norfolk and Suffolk Constabulary, if you are still dissatisfied with the decision, you can apply to the Information Commissioner for a decision on whether the request for information has been dealt with in accordance with the requirements of the Act.

For information on how to make application to the Information Commissioner please visit their website at www.ico.org.uk or contact them at the address shown below:

The Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Telephone: 01625 545 700