



20th March 2020

Freedom of Information Request Reference N^o: FOI 000801/20

I write in connection with your request for information received by the Norfolk and Suffolk Constabularies on the 21st February 2020 in which you sought access to the following information:

- 1 Are the Data Centre's operated by or for the organisation fit for purpose? For example, is there a Business Continuity Plan, is there Disaster Recovery in place or is it a single site?
- 2 Is there any capital investment in data centres planned in the next 36 months? For example, Mechanical & Electrical or refresh of equipment within the DC such as network, storage area network?
- 3 Is data privacy and or information security compliance a priority for the organisation's board?
- 4 On your Organisation's risk register, are there any Information Technology related risks?
 - i If time/ cost allows, please list the top three related risks.
- 5 Are the cyber security vulnerabilities within the organisation's existing Information Technology estate increasing?
 - i Has the organisation had a security breach in the past 12 months?
- 6 Did the organisation meet its Information Technology savings target in the last Financial Year?
- 7 What percentage of Information Technology budget is currently allocated to "on-premises" capability vs "cloud" capability?
- 8 Does the organisation have the skills and resource levels necessary for moving to the cloud?
- 9 What percentage of the Information Technology department headcount are software developers?
- 10 In relation to contracts with Amazon Web Services, Microsoft for Azure and/or Google for Google Cloud, was the monthly expenditure higher than budgeted?
 - i If yes, has the organisation been able to subsequently reduce the cost whilst maintaining service levels for users?

Response to your Request

The response provided below is correct as of 19th March 2020.

Norfolk and Suffolk Constabularies have considered your request and our response is below.

- Q1 The Constabularies will neither confirm nor deny whether relevant information is held in respect of this question.
- Q2 Yes
- Q3 Yes, data privacy and information security compliance is a priority for the Information Assurance Board.

- Q4/5 The Constabularies will neither confirm nor deny whether relevant information is held in respect of this question.
- Q6 Yes, the Constabularies met its savings target.
- Q7 The Constabularies will neither confirm nor deny whether relevant information is held in respect of this question.
- Q8 The Constabularies will neither confirm nor deny whether relevant information is held in respect of this question.
- Q9 This information is not held and there is no requirement to create information in order to respond to a request.
- Q10 The Constabularies will neither confirm nor deny whether relevant information is held in respect of this question.

Norfolk and Suffolk Constabularies can **neither confirm nor deny** whether they hold any information in respect of the questions referred to above, by virtue of the following exemptions:

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

Sections 24 and 31 are prejudice based qualified exemptions and there is a requirement to articulate the harm that would be caused by the confirmation or denial of whether any information is held, as well as carrying out a public interest test.

Harm in confirmation or denial as to whether information is or isn't held

Every effort should be made to release information under the Freedom of Information Act. However, a response under the Act is considered to be a release to the world and not just to the applicant, as responses are published and therefore access to all.

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 Data Centres to house and support Information Technology which is essential to front line services. Disclosure of specific IT services, force capabilities, (or the lack thereof) in concert with any formal acknowledgement of strategic deficiency (such as a lack of Data Recovery plan), would reveal intricacies of those systems, thereby highlighting any vulnerabilities and compromising individual force information assurance.

For national requests, disclosure would enable a geographical picture to be drawn up by individuals who are intent on 'hacking' police systems. 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 act 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 in criminal offending.

Public Interest Test

Section 24 – factors favouring confirmation or denial as to whether information is held

Confirming or denial that any information exists relevant to the request would lead to a better informed public and the public are entitled to know how public funds are spent.

Section 24 – factors against confirmation or denial as to whether information is held

Whilst there is a 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 a strong public interest in safeguarding National Security and the safety and welfare of the general public.

Any disclosure has the potential to undermine current and future Data Centre integrity, which in turn compromises the forces mandate to protect the security of the UK, eg counter-terrorism activity.

By confirming or denying whether information is or isn't held, would render national security measures less effective. This would lead to the compromise of ongoing or future operations to protect the security or infra-structure on the UK and increase the risk of harm to the public.

Section 31 – factors favouring confirmation or denial as to whether information is held

Confirming or denying whether any information is held that confirms whether the Constabularies, (a), have contingency planning in place in respect of a Data Centre, and (B), details of any on-site or Cloud base capabilities, would allow the public to be better informed on the health state and performance of the Constabularies 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 as much as highlighting that funds are being used to correctly and appropriately ensure all Data Centres have adequate hardware and software, which results in the smooth running of force technology systems.

Section 31 – factors against confirmation or denial as to whether information is held

By confirming or denying whether information is held could compromise the Constabulary's law enforcement capabilities and the effectiveness of the force would be reduced.

By confirming or denying whether the Constabularies have partnered with third party companies by revealing budget information, is intelligence to those who would wish to exploit vulnerabilities in the service. This may lead to the compromise of force IT systems which ultimately affects law enforcement capabilities and hinders the prevention and detection of crime, including terrorism.

Balance Test

The security of the Country is of paramount importance. The Police Service will not divulge whether information is or isn't held, 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 confirming whether information is or isn't held. Confirmation or denial would undoubtedly provide greater openness and transparency to the community at large with regard to information technology. Whilst there is always a public interest in the transparency of how a force delivers effective law enforcement, and ensures the National Security of the UK is robust, there is a very strong public interest in safeguarding the intricacies and tactical capabilities of data systems used when dealing with information.

In every case, public safety is the paramount focus and any information which would place individuals at risk, or compromise the National Security of the UK, no matter how generic, is not in the public interest. The effective delivery of operational law enforcement and National Security of the UK is crucial and of paramount importance to the Constabularies.

Therefore, for these reasons, the balancing test for confirming or denying whether any of the requested information is held, is not made out.

This response will be published on the Constabularies web-site under the Freedom of Information pages:-

<https://www.norfolk.police.uk/about-us/our-data/disclosure-log>

<https://www.suffolk.police.uk/services/freedom-information/disclosure-logs>

Should you have any further queries concerning this request, please contact Amanda Gibson, 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 40 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
Norfolk Constabulary
Operations and Communications Centre
Jubilee House
Falconers Chase
Wymondham
Norfolk NR18 0WW
OR
Email: freedomofinformation@norfolk.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 20 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