Freedom of Information Request Reference Nº: FOI 002606-20

I write in connection with your request for information received by Suffolk Constabulary on the 30 July 2020 in which you sought access to the following information:

"I wish to submit a request for some of the organisation's information around the internal plans and strategy documents around ICT.

The ICT documents I require is the most recent update.

I wish to obtain the following documents:

1. *ICT/IM&T/IS Strategy- The IT department strategy or plans, highlights their current and future objectives.*

2. *ICT Org Chart- A visual document that presents the structure of the IT department, please include name and job titles. If this cannot be sent, please work towards a structure with job titles.*

3. *ICT Annual or Business Plan- Like the ICT strategy but is more annually focused.*

4. *ICT Capital Programme/budget- A document that shows financials budget on current and future projects.*

If some of these documents are not valid, please state when the 2020 ICT documents are planned to be published."

Response to your Request

The response provided below is correct as of 18 September 2020

Suffolk Constabulary has considered your request for information and the response is below.

The following documents have been identified as relevant to the request and have been attached. Elements of the documents have been redacted as a result of exemptions within the Act.

1. The Digital Policing Strategy 2018-2023
2. ICT Department Structure 2020
3. ICT Business Plan 2020/21
4. With regards to the ICT capital programme/budgets, this information is published on the

Suffolk Police and Crime Commissioners website.

Section 17 of the Freedom of Information Act 2000 requires that Suffolk Constabulary, when refusing to provide such information (because the information is exempt) is to provide you the applicant with a notice ban which:

(a) States that fact
(b) Specifies the exemption(s) in question and
(c) States (if that would not otherwise be apparent) why the exemption(s) applies.

The information is exempt from disclosure by virtue of the following exemptions;

Section 21(1) – Information reasonably accessible by other means
Section 40(2) – Personal Information
Section 31(1) – Law Enforcement

Information concerning the ICT medium term financial plans are published on the PCCs website and are therefore reasonably accessible by other means as per Section 21 of the Freedom of Information Act 2000.

The following links will take you to the 'Decisions' section of their website, where relevant information can be found in PCC Decisions 2018, 2019 and 2020:
https://suffolk-pcc.gov.uk/key-info/decisions

Section 40 is an absolute and class based exemption and there is no requirement to consider the public interest. This relates specifically to the information redacted from the departmental structure.

One of the main differences between the Data Protection Act and the Freedom of Information Act is that any information released under FOI is released into the public domain, not just to the individual requesting the information. As such, any release that identifies an individual through releasing their personal data, even third party personal data, is exempted unless there is a strong public interest in its release. The public interest is not what interests the public but what benefits the community as a whole.

Personal data is defined under the Data Protection Act as data that is biographical in nature, has the applicant as its focus and/or affects the data subject's privacy in his or her personal, professional or business life. It is defined by information relating to an identifiable living person who can be identified, directly or indirectly, by the disclosure of an identifier such as a name or an identification number. A name would therefore be considered relevant to this definition.

Principle (a) of Article 5(1) states that information must be processed fairly, lawfully and in a transparent manner. When considering this principle, we first consider the lawfulness aspect in the disclosure of the officer's names. Lawfulness refers to occasions where disclosure would breach statute or common law obligations.

It is important to strike a balance between personal information that relates to an individual in their private life, or that which relates to them, in their professional capacity. It is clear that the information relates to the officers in their professional role, however that would not always mean information should be disclosed.

We have a duty to ensure that the Data Protection Act is not breached as a result of disclosures under the Freedom of Information Act. The Constabulary would generally only release names of persons in a managerial position. The roles where names have been redacted relate to staff who would not have an expectation on their names being released as they are in a non-facing public role. They would therefore expect the Constabulary to ensure the information pertaining to them is kept confidential.

The Constabulary considers that the transparency element has been met by the provision of the job titles.

It is for these reasons outlined above; that I feel the principle would be breached by this disclosure and the Section 40 exemption remains in place. I am not obliged to consider any further principle in my arguments.

This is an absolute, class-based exemption and, as such, there is no requirement to consider the public interest test.

Section 31 is a qualified and prejudice-based exemption and there is a requirement to consider the harm in the information being disclosed, and conduct a public interest test. This relates to information redacted from the ICT business plan.

Harm

Disclosure of information under the Freedom of Information Act 2000 (FOIA) is considered to be a release to the world, as once the information has been published on the Disclosure Log pages of the Constabulary's external website, the Constabulary has no control over access to that information. Whilst not questioning an applicant's motive for requesting information, it could be of use to persons who are involved in criminal activity.

Although there is a call for openness and transparency, this needs to be balanced against the harm in disclosure of the requested information. The Police Service has a clear responsibility to prevent and detect crime and disorder and to protect the communities we serve.

Disclosing the details of the Constabulary's ICT programme could assist those who plan to attempt an attack on police systems and infrastructure. It is essential that Police sites and systems are secure, as they contain a variety of information which relates to policing activities, including investigations, police intelligence and personal information. Such attacks could take the form of data theft, denial of service and other deliberate disruptions. This would have the effect of reducing the ability of the Police to undertaken relevant activities.

There would be a significantly increased risk of a security compromise, undertaken by a malicious act against our infrastructure. Should a security compromise actually be successful, the harm would be a compromise of the force's ability to use its own ICT (including radio and telephony), potentially leading to direct harm to the public, as a result of not being able to access systems and data. Also, a compromise of the forces' data, could result in information being released into the public domain.

The Police Service needs to keep up to date with new technologies in order to ensure that they can continue to detect and investigate offences that are committed online. Disclosing the details of projects that are ongoing would identify Constabulary ICT planning and this would benefit persons involved in committing computer-based crimes.
The Constabulary has a duty to enforce the law and protect the public. Disclosure under the Freedom of Information Act could be used to identify if there are any areas of potential weaknesses. This would lead to a security risk and this would consequently undermine the Police Services' law enforcement ability and this would be harmful.

Factors Favouring Disclosure

The management of ICT systems, including associated upgrades and purchases, costs money and the public have a right to know where public funds are being allocated. This allows for public scrutiny and an understanding of policing budgetary demands.

The provision of the Constabulary's ICT programme would reassure the public that the Constabulary takes all steps to ensure that systems are up to date, appropriately protected and that sufficient public funds are allocated for this purpose. The public would be in possession of up to date information which would allow for accurate public debate regarding the Constabulary's ICT planning and ongoing projects.

Openness and transparency are fundamental aspects of the Freedom of Information Act.

SUFFOLK CONSTABULARY
Taking pride in keeping Suffolk safe

Factors favouring non-disclosure

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 information we supply will be published on the Constabulary's website and will be available for any person to view and use to their advantage.

Provision of the information would suggest that the Constabulary take its responsibility to protect information, and information systems, from unauthorised access, destruction, etc, dismissively and inappropriately.

The IT infrastructure is vital to the ability of the Constabulary to effectively prevent and detect crime, share information and maintain a proficient law enforcement capability. Details of the systems used by the Constabulary could be used by individuals to identify potential vulnerable areas which they could use to plan a cyber-attack.

Releasing details of the systems that the Constabulary uses, or plans to use, to detect crimes and identify offenders, could result in persons taking steps to avoid detection. This would result in the need for additional planning and resources to ensure that the Constabulary continually keep ahead of criminal activity.

Any disruption to Constabulary systems would result in the need for additional resources and increased expenditure to ensure that policing activities are not compromised or data lost.

Balancing Test

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. Whilst there is a public interest in the transparency in how the Police Service delivers effective law enforcement and ensures information security, there is a strong public interest in safeguarding police systems and information.

Additionally, we also need to consider the safety of the public and the impact on National Security. This would be severely compromised if an attack was successful and police systems compromised.

The security of force systems is of paramount importance and this should not be jeopardised by the any release of information under the Freedom of Information Act. Therefore, it is our opinion that the balance lies in favour of non-disclosure and Section 31 is engaged. This letter serves as a refusal notice under section 17(1) of the Act.

SUFFOLK CONSTABULARY
Taking pride in keeping Suffolk safe

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/

Suffolk Constabulary is 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.

SUFFOLK CONSTABULARY
Taking pride in keeping Suffolk safe

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 Suffolk Constabulary to review their decision.

Ask Suffolk Constabulary to look at the decision again.

If you are dissatisfied with the decision made by Suffolk Constabulary under the Freedom of Information Act (2000), regarding access to information, you must notify Suffolk Constabulary that you are requesting a review within 40 working 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 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 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