Request for information under the Freedom of Information Act – 2020.478
Released – 8 June 2020

Thank you for your email dated 22 May 2020, requesting information regarding IT software.

Please find detailed below a summary of your request, together with our response.

Summary of your request:
Could you please supply the information to the below questions:

- ***What reseller do you buy your Software through?***

Softcat

- ***Are there any favored frameworks you tend to use?***

Yes - SBS IT Solutions

- ***Who is the decision maker for IT Purchasing?***

Joint agreement between IT and Procurement teams

- ***Who is your mobile phone provider?***

Vodafone is main provider (90%); EE also used

- ***How many mobile devices, (laptops, mobiles, tablets do you have?***

Active Tablets: 1947
Mobiles (Smartphones and Basic Handsets): 3,800
Laptops: 5184
Desktops: 2161

- ***What Mobile Device Management Solution are you using and when is the renewal date?***

We currently use VDSM via Vodafone. There is no renewal date as we have a rolling monthly contact dependent on the amount of devices we have.

- ***What Mobile Threat Detection do you have in place for mobile devices and when is the renewal date?***

We are withholding this information under section 31(1) Prevention and Detection of Crime and section 24(1) National Security of the Freedom of Information Act 2000 as if it was released it could compromise the security of the systems used. Please see the full exemption detailed below.

What Virtual Desktop Software do you have in place for remote workers and when is the renewal date?

Information withheld under sections 31(1) and 24(1). Please see the full exemption detailed below.

- ***Do you currently use a document security or digital rights management tool and when is the renewal date?***

None

- ***What are you using for instant messaging?***

"Nationally procured Applications" by NHS Digital. Specific information relating to this is withheld under sections 31(1) and 24(1). Please see the full exemption detailed below.

- ***Who do you currently use for your Annual IT health checks and when is your next one due?***

We use companies provided free to us by NHS digital; we do not choose the company. The next audit will be within the next 3 months.

- ***What email exchange server are you running? Cloud or on premise?***

We have no servers. We use Cloud "Nationally procured Applications" by NHS Digital.

What antivirus software/tool do you use and when is the renewal date?

We can confirm renewal is in July 2021; however further information is withheld under sections 31(1) and 24(1). Please see the full exemption detailed below.

- ***What endpoint detection & response solution do you currently use?***

Information withheld under sections 31(1) and 24(1). Please see the full exemption detailed below.

- ***Do you have an incident response team within your IT department?***

Yes

· ***Who Currently provides services described below?***
o Assurance Services
· ***Pen Testing*** NHS Digital nominated supplier
· ***Breach Simulation*** NHS Digital nominated supplier
· ***Adversarial Attack*** NHS Digital nominated supplier
o Breach Management
· ***Compromise Assessments***

· ***Incident Response***	None (inhouse)
· ***Digital Forensics***	None, but outsource to TIAA if required
o Strategic Services	
· ***Maturity Reviews***	NHS Digital nominated supplier
· ***Policy/procedure Reviews***	TIAA, and NHS Digital nominated suppliers
o ***Framework Reviews***	NHS Digital nominated supplier

We can confirm that we hold the information requested regarding mobile threat detection, virtual desktop software, instant messaging, antivirus software/tool and endpoint detection and response solution, but we are unable to release this information as to do so could compromise the security of the systems. This information is therefore exempt under Sections 31(1) Prevention and Detection of Crime and 24(1) National Security of the Freedom of Information Act 2000 (the FOIA). Disclosure of this information would be likely to both prejudice law enforcement and increase the vulnerability of the Trust, which could ultimately aid potential attackers.

Prejudice

Providing details of systems used may lead to the Trust being vulnerable to a cyber-attack. This information could aid attackers in selecting targets, thereby increasing the vulnerability of public authorities. The Trust believes that this would prejudice both the prevention and detection of cybercrime and national security. NHS organisations including the Trust hold large amounts of personal, sensitive and confidential data and there is a considerable public interest in protecting NHS organisations' systems from potential cyberattack.

Both Sections 31(1) and 24(1) are prejudice based exemptions and subject to a public interest test. This means that not only does the information have to prejudice one of the purposes listed, but before the information can be withheld, the public interest in preventing that prejudice must outweigh the public interest in disclosure.

Public Interest Test

Considerations in favour of disclosure:

- The inherent public interest in the openness and transparency of public authority dealings

Considerations against disclosure:

- Disclosing this information could expose the IT security systems of the Trust to the risk of a targeted attack
- Disclosing this information would increase the vulnerability of specific NHS organisations on a national level leading to the disruption of NHS organisations' ability to conduct business
- Disclosing this information could aid an attacker by highlighting areas or organisations that could be more vulnerable to attack than others
- Applying this exemption will prevent the disclosure of information that would facilitate or encourage criminal activity
- A successful attack would have a direct impact on patient care

Conclusion:
The Trust recognises that there is a public interest in the disclosure of information which facilitates the accountability and transparency of public bodies for decisions taken by them. However, there is also a public interest in the security of information held by the Trust which is put to the wider public interest.

Having undertaken the balancing exercise, the Trust has concluded that the public interest in maintaining the exemption significantly outweighs the public interest in disclosing the requested information. Particular weight has been placed on the severity of the prejudice which may be caused were the Trust to release details of products used.

Given that the definition of 'public' under the Act is considered to be the public at large, rather than just the individual applicant or a small group of people and that 'public interest' is not necessarily the same as what interests the public, it is considered that to release this information is likely to result in prejudice to the security systems of NHS organisations including the Trust which is not outweighed by the wider public interest for disclosure.

The Information Commissioner's Office (ICO) has confirmed that they consider that the safeguarding of national security also includes protecting potential targets even if there is no evidence that an attack is imminent. In recent months there have been published vulnerabilities against NHS organisations, including the very significant incident in May 2017. The Trust considers that the greater public interest lies with the security of the type of information held by them and that of third parties. In the Trust's opinion, the additional risk to clinical data held by the Trust and the impact a successful attack would have on direct patient care means disclosure cannot be justified.