Request for information under the Freedom of Information Act – 2022.1074
Released – 2 March 2022

Thank you for your email received 21 January 2022 requesting information regarding IT devices and systems.

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

Summary of your original request:
How many staff do you employ?

5046

Do you have a critical care function?

No

Are you actively involved in/contributing to ICS level initiatives?

Yes

How many desktop devices do you have in the Trust?

5983

What makes & models are most used?

We are unable to provide makes and models for this part of your request as to do so could compromise the security of systems. This information is therefore exempt under Section 31(1) Prevention and Detection of Crime. 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 this information 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.

Sections 31(1) is a prejudice-based exemption 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.

What is your main web browser?

MS Edge

How many trust mobile devices do you have? (phones/tablets)

6711

What are the main makes and models?

Exempt under section 31(1), see above for full exemption.

As a whole, does the Trust favour Apple or Android devices?

Neither

Are employees encouraged to use their personal devices for work?

No

Do you use an MDM solution to manage devices?

Yes

Who is your Internet provider?

Exempt under section 31(1), see above for full exemption.

Do you have any known Wifi dead zones?

This information is not held.

Who is your cellular provider?

Vodafone and EE

Do you have known cellular coverage dead zones?

Yes

Do you use pagers/bleeps?

Yes

Who is your current pager/bleep service provider?

PageOne

Do you rely on commercial apps such as whatsapp to communicate internally?

Yes

Which commercial/external apps do you use?
Do you use any of the following supplier's services: Careflow Connect, Hospify, Vocera, Ascom, Multitone, Netcall?

Exempt under section 31(1), see above for full exemption.

Do you use any software to manage tasks at night? If yes, what software do you use?

Yes – patient management system

If not, how do you manage your tasks at night (word of mouth, whiteboard etc)?

Not applicable

Which roles are responsible for managing the workload at night?

Nursing staff and healthcare assistants

Which authentication protocol(s) do you use (ie. SAML, O Auth 2, OIDC)?

Exempt under section 31(1), see above for full exemption.

What PAS/EPR system do you use?

EPR - Servelec

Do you have APIs to integrate with the PAS/EPR?

Yes

Do you use Business Intelligence software? If so, what?

Microsoft PowerBI

Do you raise alerts/send emails triggered by data? If yes, please provide any examples you can.

No

Do you have other mechanisms to raise an alert/alarm other than a bleep? If yes, please specify examples

No