Our Ref: 126/2020
May 2020

Doncaster and Bassetlaw Teaching Hospitals
NHS Foundation Trust

Re: Your request made under the Freedom of Information Act 2000

Could you please supply the information to the below questions:

1) What reseller do you buy your Software through?

- **Softcat**
- **Insight**
- **Health Trust Europe**
- **NHS Shared Business Service (NHS SBS)**
- **NHS North of England Commercial Procurement Collaborative (NOE CPC)**
- **East of England NHS Collaborative Procurement Hub (EOE CPC)**
- **London Procurement Partnership (LPP)**
- **NHS Supply Chain (NHS SC)**
- **Eastern Shires Purchasing Organisation (ESPO)**
- **Yorkshire Purchasing Organisation (YPO)**
- **Countess of Chester Health COCH**
- **QE Facilities**
- **Everything ICT**
- **North East Procurement Organisation (NEPO)**
- **Crown Commercial Service (CCS)**

2) Are there any favored frameworks you tend to use?

- **NHS North of England Commercial Procurement Collaborative (NOE CPC)**
- **NHS Supply Chain (NHS SC)**
- **NHS Shared Business Service (NHS SBS)**

3) Who is the decision maker for IT Purchasing?

- **IT Asset Control, IT Contracts & Purchasing Staff**
- **Head of ICT**

4) Who is your mobile phone provider?

Vodafone, EE, O2

5) How many mobile devices, (laptops, mobiles, tablets do you have?

Mobiles - 800

6) What Mobile Device Management Solution are you using and when is the renewal date?

*** see below**

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

*** see below**

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

*** see below**

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

*** see below**

10) What are you using for instant messaging?

*** see below**

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

*** see below**

12) What email exchange server are you running? Cloud or on premise?

*** see below**

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

*** see below**

14) What endpoint detection & response solution do you currently use?

*** see below**

15) Do you have an incident response team within your IT department?

*** see below**

16) Who Currently provides services described below:

*** see below**

a) Assurance Services

- Pen Testing
- Breach Simulation
- Adversarial Attack

b) Breach Management

- Compromise Assessments
- Incident Response
- Digital Forensics

c) Strategic Services

- Maturity Reviews
- Policy/procedure Reviews

d) Framework Reviews

*** The DBTH NHSFT considers that the disclosure of this information will compromise the Trust's security.**

Please note that all information related to the security processes involved in protecting the Trust's data systems is considered exempt from disclosure under FOIA s.24(1) (Safeguarding National Security). If disclosed, such information could be used to identify ways in which our computer systems could be breached. Patient data as well as other confidential information could therefore be accessed or

compromised. The Trust has a duty to protect such information under GDPR and the Data Protection Act 2018.

As part of the Critical National Infrastructure for the NHS, the Trust has a duty to protect the integrity of our systems. The disclosure of the information requested could expose weaknesses in our systems and lead to breaches, making the UK or its citizens, in this case our patients, more vulnerable to security threats. The release of such information is therefore exempt under FOIA s.24(1) (Safeguarding National Security).

Section 24 is a qualified exemption, therefore the public interest in withholding the information should outweigh the public interest in its disclosure. The Trust has applied the public interest test and believes that disclosure of this information could lead to breaches in Trust security and is therefore a reasonable

threat to the confidential patient data held on our systems. There is a strong public interest in protecting the confidentiality of patient data and of ensuring that healthcare services can be provided to the public without increasing the possibility of attack by hackers or malware, or of putting personal or other information held on these systems at risk of corruption or subject to illegal access. For these reasons, the Trust has decided that it is in the public interest to withhold this information at this time.

Additionally, the information is also being withheld by the Trust for organisational security reasons; and we consider that the information which has been withheld is also exempt from disclosure under section 31(1)(a) of the Freedom of Information Act.

The relevant parts of the ICO guidance on S.31 are described as follows:

31.(1) Information is exempt if its disclosure under this Act would, or would be likely to, prejudice -

(a) the prevention or detection of crime.

As Section 31 is subject to the prejudice test the Trust reasoning for its use is to withhold information that would make anyone, including the public authority itself, more vulnerable to crime for example, by disclosing its own security procedures.

It is the view of our Digital Transformation function that the disclosure of the information requested would prejudice our ability to resist any future cyber and related attacks, etc. on our systems.

In view of the above, the Trust exempts the supply of the information requested.