NHS
Surrey and Borders Partnership
NHS Foundation Trust

Information Governance
18 Mole Business Park
Leatherhead
Surrey KT22 7AD

Tel: 01372 216059
Fax: 01372 217114
Email: IGTeam@sabp.nhs.uk

05 December 2018

ID Number – FOI 6383

Title: Cyber Security – Firewall – Anti-Virus – Microsoft Enterprise

Trust Response:

1. Standard Firewall (Network) - Firewall service protects your corporate Network from unauthorised access and other Internet security threats: 1. Who is the existing supplier for this contract? 2. What does the organisation spend for each of contract? 3. What is the description of the services provided for each contract? Please do not just state firewall. 4. Primary Brand (ONLY APPLIES TO CONTRACT 1&2) 5. What is the expiry date of each contract? 6. What is the start date of each contract? 7. What is the contract duration of contract? 8. The responsible contract officer for each of the contracts above? Full name, job title, contact number and direct email address. 9. Number of License (ONLY APPLIES TO CONTRACT 3)	Refer to Note 1 below.
2. Anti-virus Software Application - Anti-virus software is a program or set of programs that are designed to prevent, search for, detect, and remove software viruses, and other malicious software like worms, trojans, adware, and more 1. Who is the existing supplier for this contract? 2. What does the organisation spend for each of contract? 3. What is the description of the services provided for each contract? Please do not just state firewall. 4. Primary Brand (ONLY APPLIES TO CONTRACT 1&2) 5. What is the expiry date of each contract? 6. What is the start date of each contract? 7. What is the contract duration of contract? 8. The responsible contract officer for each of the contracts above? Full name, job title, contact number and direct email address. 9. Number of License (ONLY APPLIES TO CONTRACT 3)	Refer to Note 1 below.

Question:	Trust Response:
3. Microsoft Enterprise Agreement - is a volume licensing package offered by Microsoft.	
1. Who is the existing supplier for this contract?	1. Bytes Software Series
2. What does the organisation spend for each of contract?	2. £550,000
3. What is the description of the services provided for each contract? Please do not just state firewall.	3. ESA – Full Office 365 Platform
4. Primary Brand (ONLY APPLIES TO CONTRACT 1&2)	4. Not applicable
5. What is the expiry date of each contract?	5. December 2018
6. What is the start date of each contract?	6. January 2018
7. What is the contract duration of contract?	7. One year
8. The responsible contract officer for each of the contracts above? Full name, job title, contact number and direct email address.	8. Procurement@sabp.nhs.uk 0300 55 55 222.
9. Number of License (ONLY APPLIES TO CONTRACT 3)	9. 3500

Note 1: We are unable to provide the information in response to above questions as these falls under exemption:

Section 31(1)(a) – the prevention or detection of crime of the Freedom of Information Act 2000 (FOIA).

We consider this exemption applies, because the release of this information may assist an adversary in carrying out a cyber-attack against us. Section 31(1)(a) is a qualified exemption, and we are therefore required to consider the public interest.

The public interest test considered the following:
• Whilst we acknowledge the public interest in transparency, we are also mindful that there is greater public interest in allowing organisations to operate without threat of attack through the release of information in this manner. Any attack on our IT networks would affect our ability to maintain our services and lead to data breaches.

We are also applying exemption:
Section 40(2) – data protection of the FOIA.

Under the Data Protection Act 1998 (DPA) Principle 7, we are required to have appropriate technical and organisational measures in place against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

We need to consider the public interest when applying the data protection principles.The release of the information may pose a risk to our cyber security and that can lead to a breach of Principle 7 of the DPA. We need to protect the data of the people who use our services and of our employees.