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

25 February 2019

ID Number – FOI 6890

Title: Cyber Security

Trust Response:

Question:	Trust Response:
1. Are you aware of the Minimum Cyber Security Standard, published 25th June 2018? a. Yes b. No	a. Yes.
2. What is your annual dedicated budget for cybersecurity (including personnel and technology)? 3. Approximately how many cyber-attacks (of any kind) have you experienced in your organisation in these 12-month periods? 4. Which of the following attack / cybersecurity threat types have been detected by your organisation? [Select all that apply] 5. Which of the following form part of your cybersecurity defence technology strategy? [Select all that apply] 6. Which of these obstacles has your organisation experienced in maintaining or improving IT security? [Select all that apply]	We are unable to provide the information in response to above questions as these fall 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.