Surrey and Borders Partnership NHS
NHS Foundation Trust

Information Governance
18 Mole Business Park
Leatherhead
Surrey KT22 7AD
Tel: 01372 216059
Fax: 01372 217114
Email: IGTeam@sabp.nhs.uk

4th October 2017
ID Number – FOI 4992
Title: IT Services in the Trust

I refer to your request for information received and acknowledged on 22nd September 2017. I am now in a position to respond to your request; please see our responses below:

Trust Response:

Question	Trust Response
1.Are your mobile devices enabled for corporate email?	Yes
2.If you answered No to Question 1, please move straight to Question 3	
3.Is corporate email delivered to your devices purely using Microsoft Exchange ActiveSync (with no other Mobile Device Management solution used)?	No
4.If you answered Yes to Question 2, please move straight to Question 6	
5.Which Mobile Device Management solution(s) do you use?	BES12
6.How many MDM licences do you currently have?	500 user licences
7.When are your Mobile Device Management licences valid until?	May-19
8.If a user accidentally breaks their mobile device, how many days does it currently take to get a fully working replacement device to them?	20 working days
9.Do you manage your MDM solution in-house or use a third party managed service?	In-house
10.If third party managed, which organisation manages your Mobile Device Management solution for you?	
11.Do you use any form of Endpoint Threat Prevention on your mobile devices to flag potential cyber risks proactively?	Under review

Question	Trust Response
12.If you answered No to Question 9, please move straight to Question 14	
13.Which Endpoint Threat Prevention solution(s) do you use?	
14.If you use Endpoint Threat Prevention solution(s), which of these security risks are detected: Distributed Denial of Service Suspicious Domain Digital Identity Monitoring Information Leaks Credential Theft Phishing Malware Suspicious Mobile Apps	
15.How many endpoint threat protection licences do you have?	
16.When are your Endpoint Threat Protection licences valid until?	
17.Do you allow mobile devices to connect to your corporate network that are more than 2 full releases behind the latest version of the operating system software?	No
18.Are you currently able to restrict access to certain websites across your entire mobile device estate?	Yes
19.If you need to wipe corporate data off a mobile device, what means do you use to wipe a device, either remotely or in hand?	Remotely via MDM controls
20.Is the data wipe auditable?	Yes
21.Are you currently operating your mobile devices in compliance with the General Data Protection Regulation (GDPR), enforceable from May 2018?	In progress
22.How do you currently dispose of a device which is no longer to be used?	Secure asset disposal
23.Is your device disposal fully auditable?	Yes