Maidstone and Tunbridge Wells NHS Trust

Ref: FOI/GS/ID 4283

Please reply to:
FOI Administrator
Trust Management
Maidstone Hospital
Hermitage Lane
Maidstone
Kent
ME16 9QQ
Email: mtw-tr.foiadmin@nhs.net

30 November 2017

Freedom of Information Act 2000

I am writing in response to your request for information made under the Freedom of Information Act 2000 in relation to security on mobile devices.

1/ Are your mobile devices enabled for corporate email?
If you answered No to Question 1, please move straight to Question 3
2/ Is corporate email delivered to your devices purely using Microsoft Exchange ActiveSync (with no other Mobile Device Management solution used)?
If you answered Yes to Question 2, please move straight to Question 6
3/ Which Mobile Device Management solution(s) do you use?
4/ How many MDM licences do you currently have?
5/ When are your Mobile Device Management licences valid until?
6/ If a user accidentally breaks their mobile device, how many days does it currently take to get a fully working replacement device to them?
7/ Do you manage your MDM solution in-house or use a third party managed service?
8/ If third party managed, which organisation manages your Mobile Device Management solution for you?
9/ Do you use any form of Endpoint Threat Prevention on your mobile devices to flag potential cyber risks proactively?
If you answered No to Question 9, please move straight to Question 14
10/ Which Endpoint Threat Prevention solution(s) do you use?
11/ 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
12/ How many endpoint threat protection licences do you have?
13/ When are your Endpoint Threat Protection licences valid until?
14/ 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?
15/ Are you currently able to restrict access to certain websites across your entire mobile device estate?
16/ 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?
17/ Is the data wipe auditable?
18/ Are you currently operating your mobile devices in compliance with the General Data Protection Regulation (GDPR), enforceable from May 2018?
19/ How do you currently dispose of a device which is no longer to be used?
20/ Is your device disposal fully auditable?

1/ Yes
2/ No
3/ Airwatch
4/ 1200
5/ Block Solutions Expires Mar 2018,
6/ 20 days
7/ 3rd party
8/ Block Solutions
9/ No
If you answered No to Question 9, please move straight to Question 14
14/ Yes
15/ Yes
16/ Both
17/ Yes
18/ Yes
19/ 3rd party destruction of the device
20/ Yes