The Dudley Group NHS Foundation Trust

Date: 11/10/2017

FREEDOM OF INFORMATION REQUEST FOI/013687 - Security on mobile device estates'.

In light of an increasing cyber-security threat I am carrying out some research relating to the level of security currently used by NHS Trusts on mobile device estates. Please could I ask you to respond to this Freedom Of Information request on behalf of your Trust?

Freedom of Information request 013687

Exemption 43 (2) applied given the organisation considers this level of information commercially sensitive from an information security perspective.
The public interest test set out in section 2(2)(b) supports application of exemption 43 (2) given there is a greater public interest in maintaining the exemption 43 (2) outweighing the public interest in disclosure in order to protect public and public services against cyber security threats.

Question		Response
1/	Are your mobile devices enabled for corporate email?	Yes
	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)?	Exemption 43
	If you answered Yes to Question 2, please move straight to Question 6	
3/	Which Mobile Device Management solution(s) do you use?	Exemption 43
4/	How many MDM licences do you currently have?	Exemption 43
5/	When are your Mobile Device Management licences valid until?	One of purchase NA
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?	Exemption 43
7/	Do you manage your MDM solution in-house or use a third party managed service?	Exemption 43
8/	If third party managed, which organisation manages your Mobile Device Management solution for you?	NA

9/	Do you use any form of Endpoint Threat Prevention on your mobile devices to flag potential cyber risks proactively?	Exemption 43
	If you answered No to Question 9, please move straight to Question 14	
10/	Which Endpoint Threat Prevention solution(s) do you use?	Exemption 43
11/	If you use Endpoint Threat Prevention solution(s), which of these security risks are detected:	Exemption 43
	Distributed Denial of Service	Exemption 43
	Suspicious Domain	Exemption 43
	Digital Identity Monitoring	Exemption 43
	Information Leaks	Exemption 43
	Credential Theft	Exemption 43
	Phishing	Exemption 43
	Malware	Exemption 43
	Suspicious Mobile Apps	Exemption 43
12/	How many endpoint threat protection licences do you have?	Exemption 43
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?	Exemption 43
15/	Are you currently able to restrict access to certain websites across your entire mobile device estate?	Exemption 43
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?	Exemption 43
17/	Is the data wipe auditable?	Yes
18/	Are you currently operating your mobile devices in compliance with the General Data Protection Regulation (GDPR), enforceable from May 2018?	Yes
19/	How do you currently dispose of a device which is no longer to be used?	Exemption 43
20/	Is your device disposal fully auditable?	Yes