St Helens and Knowsley Teaching Hospitals NHS Trust

Ref no:	079250517
From:	Press
Date:	25/05/17
Subject:	Computer Security

REQUEST

1) Do you deal with computer security in-house or do you use a contractor?

(2) If you use a contractor what is the name of the company?

(3) How much do you pay the contractor?

(4) Who is your Head of IT or equivalent role who has responsibility for making systems secure?

(5) How much is your Head of IT paid?

(6) How many devices did you have running:

a) Windows XP

b) Windows Vista

c) Windows 7

d) Windows 8

(7) On which date was the trust informed of the patch for MS-17-010 which protects against the Wannacry exploit?

8) How many of computers running each of the operating systems above were not patched for MS-17-010 which would have protected against Wannacry? Please give a separate answer for each operating system.

(9) When do you think you will have phased out all unsupported systems?

(10) How many bed days does the trust estimate have been lost as a result of ransomware attacks in the past three years?

If this email address processes FOIs for more than one trust/health board please provide the info for each one.

RESPONSE

The Trust must do its utmost to protect patient and staff information.

Patient information and staff information are the foundations upon which healthcare is built, and the Trust have a clear responsibility to safeguard this information to ensure we are able to provide the necessary care to our service users.

To provide the requested information above would highlight any vulnerability, should any such vulnerability exist (within hardware or software or architecture or Vendor, etc.), within our IT infrastructure which could be exploited for the purposes of ransomware, other malware, or to withhold/disrupt IT functionality within the Trust.

This information relating to the cyber security agenda is likely to assist criminal offenders thereby seriously threatening the effective delivery of healthcare by the Trust. The act of gathering information as requested, in the hacking arena is known as foot-printing and our network architecture is closely protected to at least NHS protect if not NHS Confidential. Therefore:

Our patients (and staff) must have confidence that their very sensitive personal data will be held securely.

They (patients & staff) must have confidence that we'll be able to provide the services they need.

Therefore, providing the specific requested information would put their confidence at risk.

Furthermore, loss of patient and staff data by such an attack would massively impact upon our ability to provide effective healthcare to our service users.

And therefore, this would be extremely harmful to the public & the services the Trust provides.

Therefore in accordance with Section 31 of the Freedom of Information Act the Trust will not be releasing the requested information as this would prejudice our ability to resist cyber-attacks.