Dear Freedom of Information Officer,

I am writing to you to request the following information about your NHS Trust under section 1(1) of the Freedom of Information Act 2000:

1. What was the total number of cyber attack incidents that have been recorded in your trust in the past

24 months?

I confirm that The Walton Centre NHS Foundation Trust holds the information you have requested. However, I am unable to provide you with that information as I consider that the following exemptions apply to it:

**Section 31 (1a) – The prevention or detection of crime**

This information is exempt from disclosure under Section 31 (1a) of the Freedom of Information Act 2000 (FOIA). We consider that if the data you have requested were to be combined with other information which may be available in the public domain, there would likely to be an increased risk of a cyber-security attack upon the Trust. As part of the Critical National Infrastructure for the NHS, the Trust has a duty to protect the integrity of our systems.  The disclosure of the information requested could expose weaknesses in our systems and lead to breaches, making the UK or its citizens, in this case our patients, more vulnerable to security threat.

**Public Interest Test**

To use this exception we are required to undertake a public interest test. The matters which were considered in applying the public interest test are as follows:

**Factors in favour of disclosure:**

* Disclosure of the data supports the general public interest in the transparency, accountability and general understanding of the delivery of public services.

**Factors in favour of withholding:**

* Breaches in Trust security and is therefore a reasonable threat to the confidential patient data held on our systems.
* Temporary or long term lack of availability of IT systems
* Corruption/loss of patient data which would prevent or interrupt provision of patient care.

There is a strong public interest in protecting the confidentiality of patient data and of ensuring that healthcare services can be provided to the public without increasing the possibility of attack by hackers or malware, or of putting personal or other information held on these systems at risk of corruption or subject to illegal access. For these reasons, the Trust has decided that it is in the public interest to withhold this information at this time.

This response therefore acts as a refusal notice under section 17 of the FOIA.

2. What is the classification of your policy regarding breach response? – Same as above

3. Of the devices running Windows operating systems, what is the number and percentage of devices

running Windows 11, Windows 10, Windows 7, Windows XP? - Same as above

4. What are the top 20 cyber security risks in your Trust, and how are they managed? - Same as above

5. Do you continue to use the Unified Cyber Risk Framework, is so how many risks are still identified/managed. - Same as above

6. What is your Patch Management Cycle and how is it implemented on old Operating systems (e.g., for   
Windows , Windows XP)? - Same as above

7. What is your current status on unpatched Operating Systems? - Same as above

8. Of the devices running Windows Servers operating systems, what is the number and percentage of

devices running Windows 2000, Windows 2003, Windows 2008, Windows 2012, Windows 2016, Windows 2019, Windows 2022? - Same as above

9. Has your Trust signed up to and implemented the NHS Secure Boundary managed service to strengthen cyber resilience? If so, how many cyber security threats has the NHS Secure Boundary detected within your NHS Trust since its implementation? - Same as above

10. Does your Trust hold a cyber insurance policy? If so: - Same as above

1. What is the name of the provider;
2. How much does the service cost; and
3. By how much has the price of the service increased year-to-year over the last three years?

11. When did the current Board last receive a briefing on cybersecurity threats within healthcare, and when did they last participate in cyber security training? How frequently, if at all, do these briefings and trainings occur, and are they carried out by cyber security technology professionals? - Same as above

12. Has your NHS Trust completed a Connection Agreement to use the Health and Social Care Network (HSCN)? If so, did you pass, and is there a copy of the code of connection? - Same as above

13. Have there been any incidents of staff members or personnel within your Trust being let go due to issues surrounding cyber security governance? - Same as above

1. How many open vacancies for cyber security positions are there within your Trust, and is their hour capacity affected by a shortage of qualified applicants? - Same as above
2. Are there mandatory minimum training requirements for those transferred internally to work in cybersecurity within your Trust, and if so, how often is the training updated and revised to reflect the evolving nature of the industry? - Same as above
3. How much money is spent by your Trust per year on public relations related to cyber attacks? What percentage of your overall budget does this amount to? - Same as above
4. Does your Trust have a Chief Information Risk Officer? If so, who do they report to? - Same as above
5. When was the last time your Trust underwent a security audit? At what frequency do these audits occur? - Same as above
6. What is your strategy to ensure security in cloud computing? - Same as above
7. Do you purchase additional / enhanced support from a Supplier for end-of-life software (Operating Systems / Applications)? If so, what are the associated costs per year per Operating System / Application, and the total spend for enhanced support? - Same as above