

Ref: FOI/GS/ID 8236

**Please reply to:**  
FOI Administrator  
Trust Management  
Maidstone Hospital  
Hermitage Lane  
Maidstone, Kent  
ME16 9QQ  
Email: [mtw-tr.foiadmin@nhs.net](mailto:mtw-tr.foiadmin@nhs.net)  
[www.mtw.nhs.uk](http://www.mtw.nhs.uk)

08 June 2023

## **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 Cyber security.

*You asked: All questions are shown as received by the Trust.*

- 1. For each year (2020 – 2022), please confirm how many cyberattacks your Trust has suffered?*
- 2. For each year (2020 – 2022), please confirm how many cyberattacks have resulted in the halting of or delay in delivery of care or services to patients?*
- For each year (2020-2022), please confirm:*
- 3. The GBP (£) value of budget allocated to cybersecurity*
- 4. What percentage of the Trust's entire budget for the financial year was spent on cybersecurity?*
- 5. How many times in the last 12 months have you audited your third-party suppliers' cybersecurity measures?*

Trust response:

1. Zero
2. Zero
- 3, 4 & 5.

The trust has applied Section 31 (1)(a) of the FOI Act (Law Enforcement) to the remaining questions as providing this information could compromise the security of the Trust's network / data and might materially cover activity which forms part of ongoing criminal investigations

The information which has been withheld is exempt from disclosure under section 31(1)(a) of the Freedom of Information Act. The relevant parts of the ICO guidance on the subject (<https://ico.org.uk/media/for-organisations/documents/1207/law-enforcement-foi-section-31.pdf>) run as follows:

31.(1) Information is exempt if its disclosure under this Act would, or would be likely to, prejudice - (a) the prevention or detection of crime. It could be used to withhold information that would make anyone, including the public authority itself, more vulnerable to crime for example, by disclosing its own security procedures. It is the view of this trust's Information security function that disclosure of the information above would prejudice our ability to resist cyber-attacks, etc. on our systems.

The Trust has a dedicated Cyber Security team and has purchased and installed many different solutions to help protect us against cyber threats. However, we will not be publicising or sharing the details of these products, solutions or vendors because we believe that in doing so, we put our self at risk.

We will also not be publishing details around any system be it hardware or software that is either end of life or is coming to end of life as we believe that publishing this information also puts the trust at risk. This would include but is not limited to items such as "does the trust have any machines running an out of date operating system or unsupported hardware".