

Ref: FOI/GS/ID 6929

**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)

18 October 2021

## **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 and software systems.

*You asked:*

- 1. In the past three years has your organisation:*
  - a. Had any ransomware incidents? (An incident where an attacker attempted to, or successfully, encrypted a computing device within your organisation with the aim of extorting a payment or action in order to decrypt the device?)*
    - i. If yes, how many?*
  - b. Had any data rendered permanently inaccessible by a ransomware incident (i.e. some data was not able to be restored from back up.)*
  - c. Had any data rendered permanently inaccessible by a systems or equipment failure (i.e. some data was not able to be restored from back up.)*
  - d. Paid a ransom due to a ransomware incident / to obtain a decryption key or tool?*
    - i. If yes was the decryption successful, with all files recovered?*
  - e. Used a free decryption key or tool (e.g. from <https://www.nomoreransom.org/>)?*
    - i. If yes was the decryption successful, with all files recovered?*
  - f. Had a formal policy on ransomware payment?*
    - i. If yes please provide, or link, to all versions relevant to the 3-year period.*
  - g. Held meetings where policy on paying ransomware was discussed?*
  - h. Paid consultancy fees for malware, ransomware, or system intrusion investigation*
    - i. If yes at what cost in each year?*
  - i. Used existing support contracts for malware, ransomware, or system intrusion investigation?*
  - j. Requested central government support for malware, ransomware, or system intrusion investigation?*
  - k. Paid for data recovery services?*

- i. If yes at what cost in each year?*
- l. Used existing contracts for data recovery services?*
- m. Replaced IT infrastructure such as servers that have been compromised by malware?*
- i. If yes at what cost in each year?*
- n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?*
- i. If yes at what cost in each year?*
- o. Lost data due to portable electronic devices being mislaid, lost or destroyed?*
- i. If yes how many incidents in each year?*
- 2. Does your organisation use a cloud based office suite system such as Google Workspace (Formerly G Suite) or Microsoft's Office 365?*
- a. If yes is this system's data independently backed up, separately from that platform's own tools?*
- 3. Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.)*
- a. Mobile devices such as phones and tablet computers*
- b. Desktop and laptop computers*
- c. Virtual desktops*
- d. Servers on premise*
- e. Co-located or hosted servers*
- f. Cloud hosted servers*
- g. Virtual machines*
- h. Data in SaaS applications*
- i. ERP / finance system*
- j. We do not use any offsite back-up systems*
- 4. Are the services in question 3 backed up by a single system or are multiple systems used?*
- 5. Do you have a cloud migration strategy? If so is there specific budget allocated to this?*
- 6. How many Software as a Services (SaaS) applications are in place within your organisation?*
- a. How many have been adopted since January 2020?*

Trust response:

1. The trust has applied Section 31 (1)(a) of the FOI Act (Law Enforcement) to this question as providing this 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 issued a Cyber Security statement which can be found on our website using the following link: <https://www.mtw.nhs.uk/freedom-of-information/>

2. Yes.

2a. The trust has applied Section 31 (1)(a) of the FOI Act (Law Enforcement) to this question as providing this 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 issued a Cyber Security statement which can be found on our website using the following link: <https://www.mtw.nhs.uk/freedom-of-information/>

3. The trust has applied Section 31 (1)(a) of the FOI Act (Law Enforcement) to this question as providing this 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 issued a Cyber Security statement which can be found on our website using the following link: <https://www.mtw.nhs.uk/freedom-of-information/>

4. The trust has applied Section 31 (1)(a) of the FOI Act (Law Enforcement) to this question as providing this 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 issued a Cyber Security statement which can be found on our website using the following link: <https://www.mtw.nhs.uk/freedom-of-information/>

5. No

6. Unknown - we do not distinguish SAAS to software

7. Not known.