Maidstone and Tunbridge Wells NHS Trust

Ref: FOI/GS/ID 9669

Please reply to:
FOI Administrator
Trust Management
Maidstone Hospital
Hermitage Lane
Maidstone, Kent
ME16 9QQ
Email: mtw-tr.foiadmin@nhs.net
www.mtw.nhs.uk

16 January 2025

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 Web Filtering and Security Awareness Training.

You asked: All questions are shown as received by the Trust.
Please could you provide the following information:
General:
** Number of Sites*
** Number of Employees*
** Number of IT Staff*
** Annual IT Budget*

Web Security
1. Who is the provide of your current web security solution?
2. Does your current web security provide you visibility in to cloud and/or business application usage?
3. When is the contract up for renewal?
4. Typically, what is the chosen duration of these contracts 12, 24, or 36 Months?
5. Name and contact details of the person responsible?
6. Current annual spend for this contract?
7. Current number of licenses for this contract?
8. Did you purchase via a reseller, or partner (if yes, please specify who e.g. Phoenix, Softcat etc.)?
9. Are you planning on assigning specific budgets for securing web security in 2024?
10. Do you procure this technology through the G-Cloud framework (if not, how do you procure & plan to procure email security in the future?)

Security Awareness Training
1. Do you current undertake cyber security awareness training with your staff?
2. Who is your current Security Awareness Training provider?
3. When is the contract up for renewal?
4. Typically, what is the chosen duration of these contracts 12, 24, or 36 Months?
5. Name and contact details of the person responsible?
6. Current annual spend for this contract?
7. Current number of licenses for this contract?
8. Did you purchase via a reseller, or partner (if yes, please specify who e.g. Phoenix, Softcat etc.)?
9. Are you planning on assigning specific budgets for Security Awareness Training in 2024?
10. Do you procure this technology through the G-Cloud framework (if not, how do you procure & plan to procure email security in the future?)

Trust response:
General:
* Number of Sites – please see https://www.mtw.nhs.uk/about-us/
* Number of Employees – please see https://www.mtw.nhs.uk/about-us/
* Number of IT Staff – Please see https://www.mtw.nhs.uk/wp-content/uploads/2024/10/Digital-Support-Services_mtw-structure-October-2024_FOI.pdf
* Annual IT Budget – 2024/25 £14,275,251
The Trust has a dedicated Cyber Security team and has purchased and installed many different solutions to help protect us against cyber threats.

Following the Synnovis cyber-attack on the NHS, the Trust has taken the decision to not release information relating to its Cyber security.

The Trust can neither confirm nor deny whether information is held under section 31(3) of the FOIA. The full wording of section 31 can be found here: http://www.legislation.gov.uk/ukpga/2000/36/section/31

S31(3) of the FOIA allows a public authority to neither confirm nor deny whether it holds information where such confirmation would be likely to prejudice any of the matters outlined in section 31(1). This includes information the disclosure of which would or would be likely to prejudice the prevention or detection of crime.

As section 31(3) is a qualified exemption, it is subject to a public interest test for determining whether the public interest lies in confirming whether the information is held or not.

The Trust recognises that answering the request would promote openness and transparency with regards to the Trust's software systems.

Cyber-attacks, which may amount to criminal offences for example under the Computer Misuse Act 1990 or the Data Protection Act 2018, are rated as a Tier 1 threat by the UK Government. The Trust like any organisation may be

subject to cyber-attacks and, since it holds large amounts of sensitive, personal and confidential information, maintaining the security of this information is extremely important.

In this context, the Trust considers that confirming or denying whether the requested information is held would provide information about the Trust's systems and its resilience to cyber-attacks. There is a very strong public interest in preventing the Trust's information systems from being subject to cyber-attacks. Confirming or denying the type of information requested would be likely to prejudice the prevention of cybercrime, and this is not in the public interest.