FOI REF: 26/220

East Sussex Healthcare NHS Trust

3rd June 2026

Eastbourne District General Hospital
Kings Drive
Eastbourne
East Sussex
BN21 2UD

Tel: 0300 131 4500
Website: www.esht.nhs.uk

Further to your recent request for information made under the Freedom of Information Act (FOIA) 2000, I now set out our answers to your specific questions, and any clarifications sought and provided, as follows:

1) What is the name of your organisation?

East Sussex Healthcare NHS Trust.

2) Within which Nation do you report (England, Scotland, Wales, Northern Ireland)?

England.

3) To which ICS / ICB (or alternative) do you report / belong? (if this is in the process of changing please give the name of the new organisation as you will be of 1 May 2026)

NHS Surrey and Sussex ICB.

4) Does your senior leadership team have live access to updates regarding the Trust corporate plan?

The Trust's integrated delivery plan and supporting numerical plans are shared by email and Teams, with monitoring and updates through the Trust's governance arrangements.

5) Are you able to provide live reporting regarding shared projects / risks to your local ICB / ICS / appropriate alternative body?

No, East Sussex Healthcare NHS Trust does not have a shared project management tool across the ICB / ICS which the Trust can access.

6) What is your latest NHS Digital Maturity Score?

I can confirm that we hold the information requested above. However, the information is exempt from disclosure under Section 21 of the Freedom of Information Act 2000. This is because the information is accessible to you, as it is already in the public domain and can be accessed by the following link:

25/494 – East Sussex Healthcare NHS Trust

This is an absolute exemption and there is, therefore, no requirement to consider the public interest.

Please note that the Digital Maturity Score provided in Freedom of Information request 25/494 is the most recent one available. The Trust has not yet completed the 2026 Digital Maturity Assessment.

7) What software do you use for the management of Projects?

Under Section 31(1)(a) of the Freedom of Information Act (FOIA), the Trust can confirm that it holds information relevant to your request, however, we are unable to disclose it for the reasons explained below.

Historically, we would disclose information relevant to the Trust's IT systems, infrastructure and software as part of our transparency agenda under the terms of the Freedom of Information Act (FOIA). However, in light of the recent cyber-attacks on NHS hospitals and the serious impact these have had on patient services and the loss of patient data, we are having to reconsider this approach. Please see several links to news articles about these recent cyber incidents provided below for your information.

- *NHS England — London » Synnovis Ransomware Cyber-Attack*
- *NHS England confirm patient data stolen in cyber attack - BBC News*
- *Merseyside: Three more hospitals hit by cyber attack - BBC News*

As a result of these attacks, thousands of hospital and GP appointments were disrupted, operations were cancelled, and confidential patient data was stolen which included patient names, dates of birth, NHS numbers and descriptions of blood tests.

When we respond to a Freedom of Information request, we are unable to establish the intent behind the request. Disclosure under the FOIA involves the release of information to the world at large, free from any duty of confidence. Providing information about our systems or security measures to one person is the same as publishing it for everyone. While most people are honest and have no intention of misusing information to cause damage, there are criminals who look for opportunities to exploit system weaknesses for financial gain or to cause disruption.

In the context of the FOIA, the term ''public interest'' does not refer to the private or commercial interests of a requestor; its meaning is for the "public good". The Trust receives a significant number of requests each year regarding our IT systems, infrastructure and cyber security measures. Most of these requests are commercially driven and serve no direct public interest. Information relevant to our IT portfolio is often requested by consultancy companies who then pass on this information to their client base. Many of these requests are submitted through the FOI portal whatdotheyknow.com who publish our responses, making this information available to an even wider audience.

As a large NHS Trust we hold extensive personal data relevant to our patients and staff, much of which is considered very sensitive. A lot of this information is held electronically

on various administration and clinical systems. We have a duty under the Data Protection Act 2018 and the UK GDPR to protect this personal information and take all necessary steps to ensure this data is kept safe. This means not disclosing information that could allow criminals to gain unlawful access to our systems and infrastructure. The Trust can be heavily fined should it be found to have acted in a negligent way which results in a personal data breach. We need to demonstrate that we comply with our legal obligations under data protection and freedom of information legislation, but we must be careful that too much transparency does not result in harm to our patients or staff, or cause disruption to our services.

Moreover, under the Network and Information Systems (NIS) Regulations Act 2018, operators of essential services such as NHS organisations like ours have a legal obligation to protect the security of our networks and information systems in order to safeguard our essential services. By releasing information that could increase the likelihood or severity of a cyber-attack, the Trust would fail to meet its security duties as stated in Section 10 of the Network and Information Systems Regulations 2018. Should we not comply with these requirements regulatory action can be taken against the Trust. Further information about the Network and Information Systems (NIS) Regulations Act 2018 can be found here – The Network and Information Systems Regulations 2018: guide for the health sector in England - GOV.UK

Your request asks for specific details regarding our IT systems which, for the reasons explained above, would be inappropriate to release into the public domain. If disclosed, it is possible that patient data as well as other confidential information would be put at risk. Such disclosure could also impact on the security of our systems and result in serious disruption to the health services we deliver to the local community. Section 31(1)(a) of FOIA provides that information is exempt if its disclosure would, or would be likely to, prejudice (a) the prevention or detection of crime. In this case, disclosure would be likely to prejudice the prevention of crime by enabling or encouraging malicious acts which could compromise the Trust's IT systems and infrastructure. The Trust's capacity to defend itself from such acts relates to the purposes of crime prevention and therefore Section 31(a) exemption is applicable in these circumstances. For these reasons, the Trust considers disclosure of the information you are seeking to be exempt under Section 31(1)(a) [*law enforcement*] of the FOIA and the information requested is being withheld in its entirety. The full wording of Section 31 can be found here: Freedom of Information Act 2000

Section 31 is a *qualified* exemption and therefore we must consider the prejudice or harm that may be caused by disclosure of the information you have requested, as well as apply a public interest test that weighs up the factors in maintaining the exemption against those in favour of disclosure.

In considering the prejudice or harm that disclosure may cause, as explained should the Trust release information into the public domain which draws attention to any weaknesses relevant to the security of our systems or those of a supplier, this information could be exploited by individuals with criminal intent. Increasing the likelihood of criminal activity in this way would be irresponsible and could encourage malicious acts which could compromise our IT systems or infrastructure, result in the loss of personal data and/or impact on the delivery of our patient services. We consider these concerns particularly relevant and valid considering the increasing number of cyber incidents affecting NHS systems in recent years and the view by government, the

ICO and NHS leaders that the threat of cyber incidents to the public sector is real and increasing.

- Organisations must do more to combat the growing threat of cyber attacks | ICO

In considering all of these factors, we have concluded that the balance of public interest lies in upholding the exemption and not releasing the information requested. Although disclosure would provide transparency about our software providers and the products used by the Trust, this is outweighed by the harm that could be caused by people who wish to use this information to assess any vulnerabilities in our security measures and consequently use this information for unlawful purposes. Cybercrime can not only lead to major service disruption but can also result in significant financial losses. As a publicly funded organisation, we have a duty for ensuring our public funding is protected and spent responsibly. Moreover, as a public body the Trust must demonstrate that it keeps its confidential data and IT infrastructure safe and complies with relevant legislation, but at the same time we must be vigilant that transparency does not provide an opportunity for individuals to act against the Trust. In considering the impact that recent cyber-attacks have had on NHS services, including the cancellation of thousands of patient appointments and procedures as well as the loss of confidential patient data, we consider the overriding public interest lies in withholding this information. The private or commercial interests of a requester should not outweigh the public interest in protecting the integrity of our systems and continuity of our essential patient services. Although we appreciate there may be legitimate intentions behind requesting this information, we must take a cautious approach to requests of this nature and appreciate your understanding in this matter.

8) Who is responsible for the overall management / reporting of projects?

The Senior Responsible Owner for each project differs depending on what kind of project it is. There's no single person with responsibility for all projects.

9) What software do you use for the management of corporate risks?

Please see the response to question 7.

10) Who is responsible for overall management / reporting of corporate risks to the board?

Richard Milner (Chief of Staff).

11) Is any part of the organisation currently using Microsoft project Online?

No.

12) If yes to the previous question, which teams / departments?

Not applicable.

13) What is your organisation's policy in regards to AI & AI Solutions?

The Trust has a newly formed AI Steering Group which reports into the Digital Transformation and Innovation Steering Group. This group is in the process of ratifying the policy for the approval and use of Artificial Intelligence and will form the main forum for discussion of all AI solutions across the organisation. The policy commits the Trust to safe, fair and ethical use of AI.

I trust this information is helpful in its detail or explanation however, if you are dissatisfied with the response, then you have the right to request an internal review. If you wish to seek an internal review, please write to the Freedom of Information Team at esh-tr.foi@nhs.net quoting the above FOI reference number, within 40 working days. Please note the Trust is not obliged to accept a request for an internal review after this time period.

Yours faithfully

Freedom of Information (FOI) Team
East Sussex Healthcare NHS Trust
0300 131 4716
Core Hours of Business: Monday to Friday 9.00am to 4.00pm