

Freedom of Information Act Request

Under the Freedom of Information Act, I would like to request the following information:

Please provide information for the period 1 January 2018 – 31 December 2024 (inclusive) or the most recent complete year available.

1. Governance framework — The framework used for cybersecurity governance (e.g. NCSC CAF, DSPT, ISO 27001) and the year of its latest board approval.
2. Board review frequency — How often the board or an executive committee formally reviews cyber resilience or cybersecurity governance (e.g. annually, quarterly, ad hoc).
3. Most recent review — The title and month/year of the latest board or committee paper or report relating to cyber resilience (no internal findings required).
4. Reporting line — The current reporting structure for cybersecurity governance (e.g. CISO → CIO → Board).
5. External assurance — Whether the Trust has undergone external assurance such as CAF self-assessment, DSPT validation, independent audit, or security testing (e.g. penetration test / red-team). If so, please indicate only the type and frequency, not the scope or results.
6. Concurrent improvement programmes — Approximate number of cybersecurity-related improvement programmes or initiatives active concurrently in a typical year (2018–2024) and trend (increasing/decreasing/stable).
7. Internal coordination — Whether a steering group, programme office, or committee coordinates concurrent cybersecurity initiatives within the Trust, and its reporting level (executive/board).
8. Cross-Trust coordination — Whether the Trust participates in structured coordination or information-sharing mechanisms with other NHS Trusts or regional bodies on cyber-resilience governance (e.g. ICS cyber networks), and at what level (regional/national).
9. Board learning — Whether board-level training sessions or workshops on cyber resilience have been held since 2018, and in which years.

After careful consideration, the Trust is unable to disclose the information you have requested.

Your questions relate to the Trust's internal cyber-security governance, reporting structures, assurance mechanisms, board-level processes, audit activity, oversight arrangements, and coordination models. Disclosure of this information would reveal details about how the Trust manages, oversees and structures its cyber-security posture, and could therefore be used to exploit potential vulnerabilities or target specific governance or operational processes.

Accordingly, the information is exempt under Section 31(1)(a) of the Freedom of Information Act 2000, which covers information where disclosure would, or would be likely to, prejudice the prevention or detection of crime. Cyber-attacks and attempts to compromise NHS systems are criminal acts, and releasing information about our cyber-security governance increases the risk of such activity succeeding.

Our Ref: 697
November 2025

We also consider Sections 31(1)(g) and 31(2)(a) to apply, as disclosing the requested information would be likely to prejudice the exercise of functions relating to the protection of the security of electronic systems used for the provision of health services.

Public Interest Test

Although there is a general public interest in transparency about how public sector bodies govern risk, in this instance the public interest in maintaining the exemption outweighs the public interest in disclosure. Revealing internal cyber governance arrangements—including frameworks, reporting routes, review structures, internal or external assurance cycles, and Board or committee oversight—would provide malicious actors with information that could compromise the Trust’s cyber-resilience.

Maintaining the security of our systems, protecting patient data, and safeguarding operational services is firmly in the public interest.

As such, the information is withheld.

If you are not satisfied with the handling of your request, you have the right to request an internal review. Requests for an internal review should be submitted within 40 working days from the date of this response, and should be addressed to d.wraith@nhs.net.

If you remain dissatisfied after the internal review, you have the right to appeal to the Information Commissioner’s Office (ICO). The ICO can be contacted at:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Tel: 0303 123 1113
Website: <https://ico.org.uk/make-a-complaint/>

Our Ref: 697
November 2025