Our Ref: NG/RM/25397
Date: 28th November 2025

Nicola Griffiths
Deputy Director of Governance
North Staffordshire Combined Healthcare NHS Trust
Lawton House
Bellringer Road
Trentham
ST4 8HH

Reception: 0300 123 1535

Dear

Freedom of Information Act Request

I am writing in response to your e-mail of the 8th November 2025**.** Your request has been processed using the Trust's procedures for the disclosure of information under the Freedom of Information Act (2000).

Requested information:
I am an academic researcher at [redacted] studying how NHS Trusts organise and oversee cybersecurity governance and organisational learning.

My current analysis is based mainly on publicly available and published sources (NAO reports, NCSC guidance, parliamentary evidence, etc.).

However, I recognise that such materials may not fully reflect how governance actually operates within individual Trusts.

To ensure that my research findings reflect real-world governance practices rather than policy design alone, I would appreciate your assistance with a small set of factual, non-sensitive governance indicators under the Freedom of Information Act 2000.

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. **The Trust uses the NHS Data Security and Protection Toolkit (DSPT), aligned to the National Cyber Security Centre's Cyber Assessment Framework (CAF) since 2024. ISO 27001 is recognised for suppliers but not adopted internally.**
   Latest Board-level approval: April 2024.

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). **Cyber resilience and governance are reviewed annually as part of DSPT assurance, with additional updates provided to the Board and Audit Committee during the year.**

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). **The latest formal review was documented in the Q2 2025/26 Digital Assurance Report, presented to the Board in September 2025.**

4. Reporting line — The current reporting structure for cybersecurity governance (e.g. CISO → CIO → Board). **Cybersecurity governance is overseen by the Deputy Chief Information Officer and Head of Information Governance/DPO, reporting through the Senior Information Risk Owner (SIRO) to the 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.
    - **DSPT/CAF Independent Audit: Annually (most recent September 2024).**
    - **Penetration Testing: Annually by an independent third party.**
    - **Cyber Essentials: Required for key suppliers.**

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). **Typically, 2–4 initiatives per year, trend increasing due to CAF adoption and ICS-wide cyber strategy.**

7. Internal coordination — Whether a steering group, programme office, or committee coordinates concurrent cybersecurity initiatives within the Trust, and its reporting level (executive/board). **The Data Protection Steering Group (DPSG) coordinates cyber and IG initiatives, reporting at executive level and escalating to the Board via SIRO and Audit Committee.**

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). **The Trust participates in ICS Cyber Security Network and Intelligent Customer Forum (ICF) at regional level. The Trust leverages the regional Security Operations Centre (SOC), managed by Staffordshire and Shropshire Health Informatics Service.**
National engagement with NHS England cyber programmes, NHS Cyber Associates Network (CAN), NCSC advisories/CareCERT.

9. Board learning — Whether board-level training sessions or workshops on cyber resilience have been held since 2018, and in which years. **Board-level cyber resilience training delivered in 2019, and development sessions held in 2024 and 2025.**

If you are dissatisfied with the handling of your request, you have the right to ask for an internal review of the management of your request. Internal review requests should be submitted

within two months of the date of receipt of the response to your original letter and should be addressed to: Dr Buki Adeyemo, Chief Executive, North Staffordshire Combined Healthcare Trust, Trust Headquarters, Lawton House, Bellringer Road, Trentham, ST4 8HH. If you are not content with the outcome of the internal review, you have the right to apply directly to the Information Commissioner for a decision. The Information Commissioner can be contacted at: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Yours sincerely

Nicola Griffiths
Deputy Director of Governance