Mersey and West Lancashire Teaching Hospitals NHS Trust

Ref. No:	FOI2275
Date:	08/01/2025
Subject:	Information on NHS cyber governance and board oversight (2018–2024)

REQUEST & RESPONSE

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

1. The framework used for cyber security governance (e.g. NCSC CAF, DSPT, ISO 27001) and the year of its most recent board approval.

   MWL follows the DSPT framework which is aligned to CAF. Previously it was aligned to Cyber Essentials.

2. How often the board or an executive committee formally reviews cyber security or cyber resilience.

   Cyber reports are written and presented to the Executive Committee and the Trust Board monthly. In addition, there is an annual report to both as part of the Trust's annual Data Security and Protection Toolkit submission (CAF)

3. The title and month/year of the most recent board or committee paper relating to cyber resilience.

   Cyber Report – Execs. January 2026

4. The reporting line for cyber security governance (e.g. CISO → CIO → Board).
   IT Security Manager > Director of Informatics / Senior Information Risk Owner

5. Whether external assurance (e.g. CAF self-assessment, DSPT validation, independent audit or security testing) has been undertaken, and the type and frequency only.
   DSPT Audit (CAF aligned), evidence items reviewed by external auditor. This takes place annually, over several months.

6. The approximate number of concurrent cyber security improvement initiatives typically active in a year, and whether this has been increasing, decreasing or stable.

Full service improvement plan is devised and reviewed on a yearly basis, there were 4 key initiatives on this years plan.

7. Whether a steering group or committee coordinates cyber security initiatives internally, and its reporting level.

There is a bi-weekly cyber security meeting attended by members of various sub team leads. An action tracker is managed and fed into monthly CA meetings that has senior members of IT as members. Evidence from these meetings is used to support DSPT submission.

8. Whether the Trust participates in cross-Trust or regional cyber-governance coordination mechanisms, and at what level.

   There are bi-weekly core cyber group meetings at regional level.

9. Whether board-level cyber security training or workshops have been held since 2018, and in which years.

   Cyber Essentials training has been completed by Board annually.

No technical details, vulnerabilities or sensitive operational information are requested