FOI 0368/2025 Response

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

DSPT-CAF was submitted in June 2025 and is regularly reviewed and discussed at BSMHFT's Information Governance Steering Group (IGSG) meeting, which reports into a sub-committee of the board.

Please note that for IGSG, Caldicott Guardian is the Chair, and the Senior Information Risk Owner (SIRO) is Deputy Chair.

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).

The board receive and review quarterly reports for cyber security governance as part of an overall ICT review.

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).

Most recent review was completed in August 2025.

4. **Reporting line — The current reporting structure for cybersecurity governance (e.g. CISO → CIO → Board).**

Reporting line:

Head of IT – Chief Information Office (CIO) – Senior Information Risk Owner (SIRO) - 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.

Internal annual audit of the DSPT-CAF.

ICT pentest assessment.

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).

4

7. Internal coordination — Whether a steering group, programme office, or committee coordinates concurrent cybersecurity initiatives within the Trust, and its reporting level (executive/board).

We have an Information Security Assurance Group (ISAG) committee which oversee cybersecurity initiatives at managerial level.

ISAG report into Information Governance steering Group (IGSG).

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 is a member of regional Integrated care systems (ICSs) group, which includes cybersecurity, co-ordination and sharing mechanism.

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

All staff members' including Board members are mandated to complete an annual Information Governance training.

The training is provided by NHSE – eLearning for healthcare, and covers cyber security.