South East Coast Ambulance Service
NHS Foundation Trust

Trust Headquarters
Nexus House
4 Gatwick Road
Crawley
West Sussex
RH10 9BG

Tel: 0300 123 0999
www.secamb.nhs.uk

19th December 2025
Internal Ref: 251110
Email:

Dear ,

The trust acknowledges receipt of your Freedom of Information Act 2000 (FOIA) request, referenced above. Please ensure you quote this number in any future correspondence.

Please accept the Trust's apologies for the delay and inconvenience you have experienced regarding your FOIA request.

FOI Request

You asked us:

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.

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.

Formal Response

The Trust confirms it holds / confirms it holds part of / does not hold the information you have requested.

1. Governance framework — The framework used for cybersecurity governance (e.g. NCSC CAF, DSPT, ISO 27001) and the year of its latest board approval - NCSC CAF, DSPT, 2025

Trust response: The Trust completes an annual CAF/DSPT which is used to measure compliance with cyber security and data protection legislation. It does not hold ISO27001 accreditation.

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).

Trust response: National Cyber Security Centre (NCSC) assured board training is completed every 2 years. This was completed in March 2023 and is currently being progressed for 2025.

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).

Trust response: Audit progress updates are provided to the Risk & Audit Committee by our internal auditors and latest update to Risk & Audit Committee was in November 2025.

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

> **Trust response:** Trust response: Head of Information Security and Business Continuity - CDIO – CEO- 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.

Trust response: Yes, CAF DSPT self-assessment, CAF DSPT independent validation, independent audit, or security testing (e.g. penetration test), Annually

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).

Trust response: We have an ongoing Cyber Improvement Programme, which is a major contributor to the Cyber Remediation Programme.

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

Trust response: The Trust has 3 sub-groups relating to data protection, information security and data quality. These groups meet monthly and report directly into the Information Governance Group (IGG). The IGG is held bi-monthly and is responsible for data protection and cyber security compliance.

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).

Trust response: The Trust is a member of locality-based information governance groups and the National Ambulance Information Governance Group. It is also a member of the AACE Cyber Security subgroup and Regional CIS.

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

Trust response: National Cyber Security Centre (NCSC) assured board training is completed every 2 years. This was completed in March 2023 and is currently being progressed for 2025.

In addition to this, board members complete mandatory Data Protection and Cyber Security Awareness training on an annual basis as part of the Trusts CAF/DSPT requirements.

Next steps

Please note you will be able to source a lot of information which is made available on our website.

Should you be dissatisfied with our response then in the first instance please contact Richard Banks, Head of Corporate Governance, via the following email address: FOI@secamb.nhs.uk

You can ask us to review our original response. If you would like us to carry out an internal review, please let us know within 40 working days of you receiving our original response. This review will be conducted by an individual who was not directly involved in reviewing the original response, ordinarily, the Trust Data Protection Officer.
We will endeavour to complete this request within 20 working days.

Should you remain dissatisfied then you can contact the Information Commissioner's Office (ICO). Complaints to the ICO should be made within six weeks of receiving the outcome of an internal review. The easiest way to lodge a complaint is through their website: www.ico.org.uk/foicomplaints.

Alternatively, the ICO's postal address is:
Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, SK9 5AF.

Yours sincerely,

Freedom of Information Coordinator
South East Coast Ambulance Service NHS Foundation Trust