NHS
Blood and Transplant

Board Meeting in Public

Tuesday, 01 December 2026

Title of Paper	Confidentiality & Data Protection Policy (POL2/8)	**Agenda No.**	4.1
Nature of Paper	☒ Official	☐ Official Sensitive	
Author(s)	Andrew O'Connor, Interim Chief Information Security Officer		
Lead Executive	Rebecca Tinker, Chief Digital & Information Officer		
Non-Executive Director Sponsor	Ian Murphy, NED, ARGC Chair		
Presenter(s) at Meeting	Rebecca Tinker, Chief Digital & Information Officer		
Presented for	☒ Approval ☐ Information ☐ Assurance ☐ Update		
Is there a plan to communicate this to the organisation?	☒ Yes ☐ No ☐ Yet to be determined		

Executive Summary

The Board is asked to approve Version 8 of the Confidentiality and Data Protection Policy (POL2/8) following review and endorsement by the Audit, Risk and Governance Committee (ARGC).

This scheduled revision updates NHSBT's core data governance framework to ensure formal alignment with the Data (Use and Access) Act 2025 (DUAA) and establishes new organisational controls for emerging technologies.

Key enhancements include a mandatory governance framework for Artificial Intelligence (AI) deployments, perimeter privacy controls regarding wearable recording devices (smart glasses), formal SIRO oversight for management access to employee mailboxes, and statutory updates reflecting the transition to the Information Commission.

Previously Considered by

- **ARGC (October 2026):** Reviewed and endorsed for Board approval, recommending explicit reference to the UK Algorithmic Transparency Recording Standard (ATRS) for algorithmic decision-making tools, which has now been incorporated.
- **Information Governance Committee (IGC) (6 October 2026):** Reviewed and endorsed, updates and changes.

Recommendation

Board is asked to:

- **Approve** Version 8 of the Confidentiality and Data Protection Policy (POL2/8) for immediate operational adoption.
- **Note** that operational protocols for wearable technology and algorithmic decision-making will remain under review as statutory codes of practice are published by the Information Commission during 2027.

Risk(s) identified (Link to Board Assurance Framework Risks)

Linked to Board Assurance Framework (BAF): P-09 (Regulatory Compliance)

Strategic Objective(s) this paper relates to:

☐ Modernising One NHSBT ☐ Optimising Donor Experience and Meeting Demand
☐ Campaigning & Identity ☒ Data, AI and Interoperability ☐ New Treatments

Appendices:	Appendix 1: Draft Confidentiality and Data Protection Policy (POL2/8) with Tracked Changes

1. Purpose & Strategic Context

This paper presents **Version 8 of the Confidentiality and Data Protection Policy (POL2)** to the Audit, Risk and Governance Committee for formal approval. POL2 defines NHSBT's technical and organisational framework for safeguarding donor, patient, and colleague data across all directorates.

This scheduled update addresses four core operational and regulatory drivers:

1. **Statutory Alignment with DUAA 2025:** Translating primary legislative reforms under the Data (Use and Access) Act 2025 into NHSBT operational standards.
2. **Artificial Intelligence (AI) Governance:** Codifying clear pre-deployment controls, Data Protection Impact Assessment (DPIA) gates, and human oversight safeguards for machine learning and algorithmic tools.
3. **Internal Data Access Controls:** Establishing clear SIRO governance over management requests to access current or former employee email accounts, eliminating historical ambiguity.
4. **Physical & Perimeter Privacy:** Addressing emerging consumer recording hardware (such as smart glasses) within donor sessions, laboratories, and clinical areas following recent positioning from the regulator.

2. Summary of Policy Amendments (Version 8)

Functional Area	Summary of Amendment	Operational & Governance Impact
Legal Status & Scope	Standardised description of NHSBT as an executive arm's length Special Health Authority	Harmonises organisational definitions across all regulatory and commercial documentation.
Management Email Access	Codified strict restrictions on accessing employee and leaver mailboxes.	Prohibits unilateral management access. Routine requests must route through Data Privacy; non-consensual searches mandate formal SIRO sign-off.
Research & Legitimate Interests	Updated UK GDPR Art. 4 scientific research definitions and Recognised Legitimate Interests per DUAA 2025	Streamlines data sharing for public health research and collaborative university studies without individual legitimate interest assessments.
International Data Transfers	Adopted statutory "Data Protection Test" and updated transfer risk assessment terminology.	Ensures cross-border data transfer assessments for research platforms and third-party vendors meet new statutory standards.
Statutory Complaints Handling	Codified mandatory 30-day acknowledgment requirement for data protection complaints.	Aligns NHSBT public logging and complaints processes with DUAA standards.

Artificial Intelligence (AI)	Integrated a comprehensive governance framework (mandatory DPIAs, bias mitigation, accuracy, meaningful human oversight under Art. 22/22A, and alignment with the Algorithmic Transparency Recording Standard (ATRS).	Enforces pre-deployment security/privacy screening, mandates formal transparency recording for public-impacting algorithms, and prevents solely automated decisions in clinical triage, organ offering, or staff workflows
Wearable Technologies / Smart Glasses	Established baseline privacy rules regarding recording wearables on NHSBT premises following recent ICO positioning.	Protects donor, patient, and staff confidentiality across donation sessions, laboratories, and clinical facilities.

3. Detailed Operational Implications

- **Governance of Mailbox Investigations (Section 6):**
  Prohibits ad-hoc managerial access to staff or leaver mailboxes. Non-consensual searches now require documented necessity, Data Privacy Team review, and formal authorisation from the Senior Information Risk Owner (SIRO).

- **Artificial Intelligence & Algorithmic Oversight (Section 13):**
  Mandates a completed DPIA (using the regulator's AI Toolkit) before any AI tool is deployed. Crucially, the policy requires demonstrable, meaningful human oversight under DUAA 2025 (UK GDPR Art. 22/22A), preventing solely automated decisions across clinical triage, organ offering algorithms, and workforce processes.

- **Wearable Recording Technologies on Site (Section 14):**
  Establishes perimeter controls across donor centres, mobile sessions, and laboratories to prevent unconsented audio/video recording via consumer devices (e.g., smart glasses), safeguarding donor trust and staff confidentiality.

4. Risk Assessment and BAF Alignment

- **Link to Board Assurance Framework (BAF): P-09 (Regulatory Compliance)**

- **Risk Context:** Failure to maintain policy alignment with DUAA 2025 reforms, revised PECR statutory penalty structures (aligned to UK GDPR maximums of up to 4% global turnover), and evolving AI standards exposes NHSBT to regulatory enforcement, compromised internal audit ratings, and reputational damage.

5. Recommendations

ARGC is asked to:

1. **Approve** Version 8 of the Confidentiality and Data Protection Policy (POL2) for immediate operational adoption.

2. **Note** that operational protocols for wearable technology and algorithmic decision-making have been updated and reflect in the new policy and will remain under review as statutory codes of practice are published by the Information Commission during 2027.