Torbay and South Devon
NHS Foundation Trust

Acceptable Use of Artificial Intelligence (AI) Technologies Policy

Document Information

This is a controlled document. It should not be altered in any way without the express permission of the author or their representative. On receipt of a new version, please destroy all previous versions.

Date of Issue:	**January 2026**	**Next Review Date:**	April 2026
Version:	1	Last Review Date:	
Lead Author	Technologies Research Programme Manager		
Contributors	Director of Digital Innovation Information Governance Officer		
Reviewed By	IM&T Group		
Director Responsible	Director of Corporate Governance and Trust Secretary		

Approval Route:

Approval Information	**Details**
Approved By:	IM&T Group
Date Approved:	December 2025

Links or overlaps with other policies:

- Information Governance Policies
- Appropriate Policy Document for Special Category Data
- Health Adult Social Care Records Policies Procedures and Guidance
- Information Asset Management Policy, Procedure and Guidance
- Information Management and Technology Security Policy
- IT Asset Lifecycle Policy
- Network User Security Operating Policy
- Retention Destruction of Corporate Records Policy

We are committed to preventing discrimination, valuing diversity and achieving equality of opportunity. No person (staff, patient or public) will receive less favourable treatment on the grounds of the nine protected characteristics (as governed by the Equality Act 2010): Sexual Orientation; Gender; Age; Gender Reassignment; Pregnancy and Maternity; Disability; Religion or Belief; Race; Marriage and Civil Partnership. In addition to these nine, the Trust will not discriminate on the grounds of domestic circumstances, social-economic status, political affiliation or trade union membership.

We are committed to ensuring all services, policies, projects and strategies undergo equality analysis. For more information about equality analysis and Equality Impact Assessments please refer to the Equality and Diversity Policy.

This policy is an evolving document. It will undergo changes with newer updates. Please ensure that you are referring to the most up to date version of this document.

Contents

1. Executive Summary

1.1. Artificial Intelligence (AI) presents both opportunities and risks for the Trust. When applied responsibly, AI can improve patient care, streamline operational processes, and support staff. However, without governance and oversight, AI may cause harm, introduce bias, or undermine public trust.

1.2. This policy sets out a clear and proportionate framework for how AI will be identified, assessed, adopted, monitored, and decommissioned within the Trust. It ensures compliance with UK law, international standards, and NHS values. The policy applies to all staff, contractors, vendors, and partners. All AI systems must be registered on the Information Asset Register (IAR), evaluated proportionately, and overseen by the Trust's Governance Groups.

1.3. The Trust commits to five core principles - Safety, Transparency, Fairness, Accountability, and Contestability. These principles will guide all AI adoption decisions in the Trust

2. Introduction & Context

2.1. AI technologies continue to evolve rapidly. They range from machine-learning models that predict patient risk of deterioration, to natural-language processing tools that summarise medical notes, and robotic-process-automation (RPA) systems that streamline repetitive administrative tasks. Generative AI platforms such as Microsoft Copilot are being explored within the Trust for non-clinical productivity use cases.

2.2. Other third-party generative AI tools are currently not approved, pending further cybersecurity and governance review**.** Given this landscape, the Trust recognises the need for:

- A balanced approach that encourages innovation while managing risks
- A governance framework that ensures transparency, fairness, and accountability.
- Alignment with national and international guidance (Please refer to Appendix E for more information

2.3. Our approach puts emphasis on the Trust's commitment to user-led adoption, where staff and patient groups will be actively involved in evaluating and shaping how AI is used.

3. Scope

3.1. This policy applies to all AI activities within the Trust, including but not limited to.

- **Clinical applications** - diagnostic support, triage tools, predictive analytics for deterioration, personalised care recommendations.

- **Operational applications -** workforce scheduling, bed management, demand forecasting, process automation.
- **Research applications -** model development, analysis of large datasets, collaborations with academia and industry.
- E**ducational applications -** simulation training, digital literacy tools, and staff development platforms.

3.2. This policy applies to.
- All staff (clinical and non-clinical), contractors, volunteers, and third-party vendors engaged in AI activities.
- To all systems procured, developed, or adopted by the Trust that involve AI.
- To all data (clinical, operational, or research) used for training, validating, or deploying AI models.

3.3. For clarity, this policy excludes purely deterministic, rules-based systems that do not learn or adapt over time.

4. Definitions

4.1. For clarity, the policy defines AI broadly to cover-
- **Machine Learning (ML)** algorithms that learn from data to make predictions or classifications (e.g., readmission risk).
- **Deep Learning** multi-layer neural networks, often used in imaging or speech tasks.
- **Natural Language Processing (NLP)** systems that analyse or generate human language (e.g., summarising clinical notes, chatbots for patient queries).
- **Generative AI** systems that create text, images, video, or audio (e.g., large language models).
- **Robotic Process Automation (RPA)** automation of repetitive, rule-based tasks (e.g., appointment booking, data entry).
- **Predictive Analytics** identifying trends and forecasting outcomes (e.g., falls risk).

4.2. Additional terms can be found in Appendix B – Glossary

5. Principles

The Trust's adoption of AI is guided by five core principles, consistent with the UK's pro-innovation framework.

5.1. Safety, Security & Robustness

5.1.1. AI must always be safe for patients, staff, and the organisation. Safety extends beyond technical performance to include clinical, data protection, and cyber security assurance.

Systems must undergo rigorous pre-deployment testing, resilience checks, and cyber security reviews.

5.1.2. Clinical AI must comply with DCB 0129/0160 and, where applicable, Medicines and Healthcare products Regulatory Agency (MHRA) requirements for Artificial Intelligence as a Medical Device (AIaMD), including conformity assessment and post-market surveillance.

5.1.3. All AI systems must also ensure data security and lawful processing in line with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Data (Use and Access) Act 2025.

5.1.4. Systems should be demonstrably robust under different conditions, resilient to misuse or adversarial inputs, and supported by documented safety and privacy risk assessments.

5.2. Transparency & Explainability

5.2.1. All data subjects must know when AI is being used. Systems must be transparent about their use, purpose, and limitations. Where models are not inherently explainable, additional documentation must be provided. Plain-language explanations must be available for varied AI literacy levels.

5.2.2. Where appropriate, there must be an opportunity for persons to opt out of AI processing of personal data, with the risks explained.

5.3. Fairness

5.3.1. AI must not discriminate. Models must be tested against representative datasets and monitored for bias throughout their lifecycle. Equality Impact Assessments (EIAs) (please refer to Appendix 2) are mandatory for all AI systems that could affect patients or staff.

5.3.2. AI must not be used to make decisions which impact the rights and freedoms of any person. This includes any systems which influence people's decisions or exploit their vulnerabilities, evaluate or classify people based on social behaviour or traits, and systems that predict a person's risk of committing a crime.

5.4. Accountability & Governance

5.4.1. Each AI system must have an Information Asset Owner (IAO) responsible for compliance, monitoring, and reporting. The IAO must be appropriately qualified and able to make decisions on the safe use of the tool which they own.

5.4.2. Oversight is provided by the Operational Information Governance Group.

5.5. Contestability & Redress

5.5.1. Data subjects must be able to challenge AI-supported decisions. Human override must always be possible. Complaints and incidents relating to AI must be captured via Datix and reviewed by the Operational Information Governance Group.

6. Roles & Responsibilities

Following are key responsibilities for individuals:

6.1. All Staff- Must use AI responsibly ensuring to not use a tool for a purpose beyond its approved scope, complete all mandatory and statutory training, and report concerns / incidents regarding AI use.

6.2. Information Governance (IG)- ensure data protection compliance, approve DPIAs and provide recommendations relating to the use of AI technologies.

6.3. Digital Futures Team - provide innovation support, horizon scanning, pilots, AI Training Hub, and is responsible for strategic alignment of AI use within the Trust across the ICS.

6.4. Cyber Security - Ensures all vulnerability assessments, threat modelling, and secure integrations when AI is deployed.

6.5. Clinical Safety Officer – Ensures all clinical safety assurances (DCB 0129/0160, AIDRS, MHRA AIaMD) are completed and ratified.

6.6. Caldicott Guardian – Provides recommendation regarding the safe use of AI to oversight of patient-identifiable data.

6.7. Senior Information Risk Officer (SIRO) - Holds responsibility for all information assets controlled by the Trust and is responsible for making risk-based decisions regarding high-risk deployments, based on the recommendations of the DPO and Information Governance Team.

6.8. Procurement Team/Lead - Are responsible for assuring all AI procurements meet regulatory standards and include appropriate contractual clauses based on value and risk.

7. Governance Framework

7.1. To ensure consistency, transparency, and compliance with national guidance, all proposed AI systems must follow the Trust's Regulatory Onboarding Pathway**.**

7.1.1. This pathway provides a structured sequence of steps from idea to deployment, reflecting the requirements of NHS England, the AI and Digital Regulations Service

(AIDRS), the Medicines and Healthcare products Regulatory Agency (MHRA), and the Trust's internal governance framework.

7.1.2. All AI activities must align with applicable legislation, regulations, and recognised standards. A summary of essential legal requirements and recommended good-practice frameworks (including GDPR, DUAA 2025, MHRA AIaMD, DTAC, ISO/IEC 42001, and the EU AI Act) is provided in **Appendix E.** A full overview of the required stages, actions, and outputs is provided in **Appendix G: Regulatory Onboarding Pathway**.

7.1.3. Before initiating either pathway, proposers must check the AI classification through the AI and Digital Regulations Service (AIDRS) the national guidance portal jointly operated by MHRA, NICE, CQC, and HRA. AIDRS helps determine if the proposed system qualifies as a **medical device**, **research tool**, or **non-clinical digital innovation**, ensuring the correct governance route is followed.

7.1.4. All AI systems must first be checked through the **AI and Digital Regulations Service (AIDRS)** to determine regulatory classification. Systems identified as **AI as a Medical Device (AIaMD)** under MHRA oversight will automatically follow Pathway B (Clinical AI) and comply with MHRA requirements for CE/UKCA marking and post-market surveillance.

7.2. AI Impact Assessment (AIIA)

7.2.1. All AI systems, irrespective of risk level, must undergo an AI Impact Assessment (AIIA) as part of the proportionality review.

7.2.2. The AIIA evaluates ethical, societal, legal, and organisational implications and ensures compliance with the UK Government's AI regulatory principles, NHS England's AI Assurance framework, and ISO/IEC 42001 requirements for responsible AI management.

7.2.3. The AIIA complements the Data Protection Impact Assessment (DPIA), Equality Impact Assessment (EIA) (Appendix 2), and Risk Assessment (Appendix C), and must be completed before pilot or deployment.

7.2.4. (See Appendix 3 – AI Impact Assessment Template.)

7.3. Dual Pathways for Approval

The Trust applies a risk-based dual pathway for approval.

7.3.1 Pathway A (Non-clinical / Non-patient data AI):

a. A proposal will be made and scoped by the Digital Futures Team

b. If accepted this proposal will form an IT Project reviewed at the IT Projects Meeting and prioritised according to the IT Projects Prioritisation Policy

c. The project will be reviewed by Information Governance & Cyber Security, with completion of a Data Protection Impact Assessment & Cyber Security documentation.

d. Once completed the IG and Cyber Security will make a recommendation at the Operational Information Governance Group. If accepted as 'low' or 'medium' risk, this will be fed to the SIRO through routine decision-making channels.

e. If the project recommendation is to not adopt, or the project deemed a 'high' risk to the rights and freedoms of data subjects'; SIRO approval will be sought through the Governance Delivery Group.

f. A Technical Design Authority meeting may be stood up to approve any technical integrations before deployment.

g. Once deployed the asset will be registered on the Trust's Information Asset Register.

7.3.2 Pathway B (Clinical AI / Patient data AI):

a. A proposal will be made and scoped by the Digital Futures Team

b. If accepted this proposal will form an IT Project reviewed at the IT Projects Meeting and prioritised according to the IT Projects Prioritisation Policy

c. The project will be reviewed by Information Governance & Cyber Security, with completion of a Data Protection Impact Assessment & Cyber Security documentation.

d. The project will be reviewed by the Chief Clinical Information Officer and Medical Device Safety Officer.

e. Once completed the IG and Cyber Security will make a recommendation at the Operational Information Governance Group. If accepted as 'low' or 'medium' risk, this will be fed to the SIRO and Caldicott Guardian through routine decision-making channels.

f. If the project recommendation is to not adopt, or the project deemed a 'high risk to the rights and freedoms of data subjects'; SIRO approval will be sought through the Governance Delivery Group.

g. A Technical Design Authority meeting may be stood up to approve any technical integrations before deployment.

h. Once deployed the asset will be registered on the Trust's Information Asset Register.

7.4 Lifecycle Governance

7.4.1 For effective oversight of AI throughout its full lifecycle, governance will operate through **stage-based controls** and **continuous assurance cycles**. These stages ensure that all AI systems are designed, deployed, monitored, and retired safely, in alignment with NHS, UK, and international regulatory standards.

7.5 Evaluation of AI Systems

7.5.1 The Trust requires that all AI systems undergo structured evaluation before they are approved for use. Evaluation ensures that systems are safe, fair, effective, and appropriate for the Trust's local context. This applies equally to **third-party AI products** and to **in-house developed systems**, although the type of evidence required may differ.

7.5.2 Appendix 1 contains the standardised evaluation checklist that must be completed before any AI system can be approved. This checklist provides a consistent structure to capture evidence, assess risks, and document decisions.

7.6 Foundation Models & Generative AI - Use-Case Card Approach

7.6.1 The Trust currently permits the use of **Microsoft Copilot** as its approved generative AI platform. All other third-party generative AI tools are **not authorised for use** within the Trust environment currently pending further evaluation of cybersecurity, data protection, and safety implications.

8. Data Protection & Privacy

8.1 AI systems must comply with UK GDPR, DPA 2018, and the DUAA 2025. This is assessed through a Data Protection Impact Assessment and the AI Impact Assessment.

8.2 Please refer to the Information Governance Policy for further information.

9. Risk Management

9.1. AI systems bring distinct risks that must be actively identified, assessed, and managed throughout their lifecycle. The Trust's approach combines the categorical framework of the EU AI Act (risk tiers) with the context-specific proportionality principle from the UK pro-innovation framework.

9.2. Risk Categories

9.2.1. Risks are grouped into six categories to support consistent assessment:

a. **Clinical Risk-** Potential for incorrect diagnoses, unsafe treatment recommendations, or inappropriate triage that could harm patients.

b. **Technical Risk-** Failures in system design, downtime, poor integration, adversarial attacks, or cybersecurity vulnerabilities.

c. **Data Risk-** Use of incomplete, biased, or poor-quality data; inappropriate processing of patient identifiable data (PID); or breaches of privacy.

d. **Ethical Risk-** Risks of discrimination, opacity, exclusion of vulnerable groups, or erosion of trust in clinicians and services.

e. **Operational Risk-** Disruption to workflows, over-reliance by staff on AI recommendations, or resource inefficiency caused by faulty outputs.

f. **Legal/Regulatory Risk-** Breaches of data protection law, medical device regulation, or failure to comply with Trust governance policies.

9.2.2. These categories provide the foundation for risk assessments recorded in DPIAs, AI Impact Assessments, and safety cases.

9.3. Mitigation Measures

9.3.1. For each risk category, appropriate mitigation strategies are required. Key measures include:

a. **Testing & Validation-** Pre-deployment testing against local anonymised or synthetic datasets, with results benchmarked against clinical standards.

b. **Bias Audits-** Evaluation of performance across age, gender, ethnicity, and other protected characteristics; use of Equality Impact Assessments.

c. **Monitoring & Audit-** Continuous monitoring of outputs, error rates, and drift; annual audits for all AI systems, with quarterly dashboards for high-risk systems.

d. **User Training-** Mandatory Level 1 Training via Digital Passport for all staff on AI capabilities, limitations, and safe use; scenario-based training for high-risk applications.

e. **Human Oversight-** Clinicians remain responsible for decisions; human-in-the-loop checks are required for all high-risk or clinical AI systems.

f. **Fallback Procedures-** Clear manual workflows must remain available in case of AI failure; "safe to fail" design is a mandatory principle.

g. **Transparency Tools-** Documentation such as model cards, factsheets, and explainability features must accompany AI systems to support informed use.

10. Incident and Policy Breach Management

10.1. All AI-related incidents must be reported on the Trust's Incident Risk Management System (Datix), investigated, and acted upon with the same rigour as any clinical and IT safety incidents.

10.2. Policy breach management

10.2.1. A breach of this AI Policy occurs when staff, contractors, or vendors:

a. Use AI systems without following the Trust's governance pathways (approval, DPIA, safety case, IAR registration).

b. Input patient-identifiable or sensitive staff data into unapproved AI systems.

c. Rely on AI outputs without required human oversight or against clinical safety guidance.

d. Circumvent monitoring, audit, or reporting processes (e.g. failing to log incidents via Datix).

e. Fail to complete mandatory AI training (Level 1 Digital Passport).

f. Misuse AI tools (including Microsoft Copilot or generative AI) in ways that are discriminatory, unsafe, reputationally damaging, or contrary to Trust values.

g. Deploy or procure AI systems without Procurement, IG, or Operational Information Governance Group involvement.

h. Breaches may include deployment of an AI as a Medical Device (AIaMD) without satisfying MHRA medical device obligations, misreporting or failing to monitor AIaMD post-market performance, or not engaging with regulatory reporting requirements.

10.3. **Any breach must be reported to IG as soon as it is identified.**

11. AI Innovation & Adoption

11.1. The Trust recognises that innovation is essential for improving services and patient outcomes, but we must ensure that adoption is safe, ethical, and evidence based. The aim

is to support creativity and experimentation while ensuring that systems are only scaled once there is evidence that they can deliver value and align with the Trust's principles.

12. AI Training

12.1. The Trust will establish an AI Training & Literacy Hub to support staff in improving their AI competency, and understand practices for safe, ethical and responsible use of AI.

a. Level 1 – Awareness (all staff): AI basics, risks, and reporting.

b. Level 2 – Practitioner (clinical/operational users): explainability, oversight, safe use.

c. Level 3 – Advanced (developers/leaders/governance): lifecycle management, evaluation, regulation.

12.2. Level 1 training is mandatory via the Digital Passport. Level 2 and 3 training is not mandatory but encouraged for safe use of AI.

12.3. Awareness modules will be available to all staff, but completion will only be mandatory for those directly involved in the development, procurement, governance, or use of AI systems. Practitioner and advanced training will be targeted at relevant clinical, operational, digital, and governance roles.

12.4. Training content will align with national NHS AI literacy initiatives and be updated as guidance evolves.

12.5. Learners will receive CPD-accredited certificates at each level to encourage completion and support professional development portfolios.

13. Monitoring, Review & Improvement

13.1. The Trust adopts a structured approach that combines governance oversight, quarterly reporting, annual audits, and focus on continuous improvement activities.

13.2. Oversight and Escalation

13.2.1. **Operational Information Governance Group-** Meets to review new proposals, monitor the performance of live systems, and oversee incidents. It acts as the primary forum for escalation of risks, safety concerns, or ethical issues.

13.2.2. **Escalation process -** Incidents or risks identified through Datix, audits, or user feedback are escalated to the Operational Information Governance Group. Where significant, they are further escalated to SIRO.

14. Reporting and Accountability

14.1. **Quarterly Reports -** The **Operational Information Governance** Group will provide quarterly updates to the Governance Delivery Group and the Trust Executive. These reports will summarise AI adoption, performance metrics, incidents, mitigations, and emerging risks.

14.2. **Transparency -** Summary information about AI systems in use (purpose, safeguards, and oversight arrangements) will be made publicly available where appropriate, to maintain patient and public trust.

14.3. **AI Register (Public Transparency Record)** - The Trust will maintain an AI Register listing all AI systems approved for use or under evaluation. The Register provides a public-facing summary of each system's purpose, data use, risk classification, and responsible owner, supporting accountability and public trust. It complements the Information Asset Register (IAR) and is maintained by the Digital Futures Team. A summary will be published on the Trust website and updated at least annually or whenever new AI systems are approved.

14.4. Audits and Reviews

14.4.1. **Annual Audit -** All AI systems must undergo an annual review covering accuracy, safety, fairness, bias, transparency, and patient/staff acceptability.

14.4.2. **Independent Assurance -** Where appropriate, external audits or third-party assurance will be sought for critical AI systems.

15. Policy Review

15.1. The AI Policy itself will be reviewed by the Operational Information Governance Group on an annual basis**,** or sooner if prompted by significant changes in law, standards, or NHS guidance.

15.2. Updates will be shared with staff through internal communications and integrated into the AI Training & Literacy Hub to ensure learner awareness of changes.

16. Appendices for additional information

Guidance:
- Appendix A: RACI Matrix
- Appendix B: Glossary
- Appendix C: Risk domains and template
- Appendix D: Decommissioning Flow
- Appendix E: Alignment with Legislation, Standards and Frameworks
- Appendix F: Use-case Examples
- Appendix G: Regulatory Onboarding Pathway

Supporting Documents
- Appendix 1: Evaluation Checklist
- Appendix 2: Equality Impact Assessment template
- Appendix 3: AI Impact Assessment (AIIA)
- Appendix 4: AI Triage Form
- Appendix 5: Document Checklist for AI Systems