

Artificial Intelligence (AI) Policy

V1.0

September 2026

Summary

Artificial Intelligence (AI) will play a transformative role in acute care over the next decade, enabling smarter, faster, and more personalised healthcare delivery. AI-driven tools will support clinicians through advanced decision support, predictive analytics, and real-time risk stratification, helping to identify deterioration earlier and optimise treatment pathways. Whilst the benefits of AI are clear, it also brings with it significant challenges and considerations and will require strong governance and clear guidance to embed responsibly, ensuring adherence to regulations, alignment to ethical standards and ensuring patient trust.

This policy provides Royal Cornwall Hospitals NHS Trust (RCHT) with an enabling framework for the safe, responsible use of Artificial Intelligence (AI) across both clinical and non-clinical settings to improve patient care, staff experience and organisational effectiveness. It supports innovation while maintaining essential controls for clinical safety, information governance, cyber security, equality and legal compliance (including the Data Protection Act 2018, Equality Act 2010, and NHS clinical risk standards DCB0129/DCB0160).

This policy has two purposes: (1) staff guidance for approved AI tools currently available and (2) governance arrangements for future AI systems. It is recognised that the AI landscape is changing quickly and this policy will therefore develop over time.

For everyday business and administrative productivity tasks, staff should use **NHS- and Trust-approved AI tools when undertaking Trust activities**, including **Microsoft M365 Copilot within NHS.net Connect (NHS Enterprise protections)**, signed in with their **NHS.net Connect account**. Personal Microsoft M365 Copilot access via a personal Microsoft account and other consumer or public AI services may be used for personal purposes. They should not be used to process, create, analyse or store confidential Trust information, patient information, staff information, or non-public NHS information. Where AI tools are being used in support of Trust activities, staff are expected to use NHS- and Trust-approved AI tools.

Other AI solutions should only be sought where approved NHS options are not available and appropriate Trust assessment and approval has been completed. Governance scales with risk: the AI Group provides final approval for Trust-wide AI systems and agents intended for broad use, while Microsoft M365 Copilot personal agents used by individuals remain the user's responsibility within this policy's guardrails. This policy aligns with NHS.net Connect acceptable use for Microsoft M365 Copilot, including use for work via NHS.net Connect accounts and devices, transparency when sharing AI-assisted content, verification of outputs, and use for clinical administration but not clinical decision-making.

Data Protection Act 2018 (UK GDPR): AI use must have a valid lawful basis for processing personal data and must follow Trust Information Governance requirements, including transparency, data minimisation, appropriate access controls and retention. Information Governance must be engaged early. For departments or categories of use, lawful-basis and DPIA coverage may initially be framed broadly at an early stage and then refined as use cases and risks become clearer. If you are unsure, seek advice from the Information Governance Team and refer to the Management of Information, Records and Data Quality Policy.

Information Governance Team: rch-tr.infogov@nhs.net

EVERYONE needs to read pages 3 and 4.

If you have specific questions or are unsure about your responsibilities, please consult the full policy for more detail.

What is this about?

This Artificial Intelligence (AI) Policy explains how Royal Cornwall Hospitals NHS Trust (RCHT) uses AI safely, responsibly and proportionately. It supports innovation while protecting patients, colleagues, confidential information and the Trust.

This policy has two purposes: (1) staff guidance for approved AI tools currently available and (2) governance arrangements for future AI systems. It is recognised that the AI landscape is changing quickly and this policy will therefore develop over time.

This policy distinguishes between general-purpose AI tools (such as Microsoft M365 Copilot), which must not be used for clinical decision-making, and purpose-built clinical AI systems, which may be considered through the governance routes described in this policy.

Why does it matter to me?

AI can help staff draft, summarise, organise information and improve productivity, but it must be used within clear guardrails. Staff remain responsible for checking outputs, protecting confidential information and using only approved tools for Trust work.

How does this support patient care?

Responsible AI use supports patient care by helping teams work more effectively while maintaining safety, confidentiality and professional judgement. By following the policy, we help ensure:

- AI is used to support, not replace, human judgement.
- Clinical decisions remain with appropriately qualified staff and established clinical processes.
- Patient, staff and confidential information is handled lawfully and securely.
- Higher-risk AI use is assessed through the correct governance route before wider deployment.

What we ask of you

Every member of staff has a role to play. Please:

- Use Microsoft M365 Copilot within NHS.net Connect for approved business and administrative tasks.
- Do not use personal or public AI tools for Trust work unless formally assessed and approved.
- Check AI outputs carefully before using or sharing them.
- Protect patient-identifiable, staff-identifiable and confidential Trust information.

- Escalate higher-risk, Trust-wide, clinical, supplier or automation use cases through the policy route.

AI can help us work better, but it does not remove professional accountability. Use approved tools, protect information, check outputs and escalate risk early.		
Topic	☑ Do	✗ Don't
Use approved AI tools	Use Microsoft M365 Copilot within NHS.net Connect, signed in with your NHS account, for approved business and administrative tasks. Use AI to support drafting, summarising, organising information and administrative productivity where it is appropriate and within policy. Check and apply professional judgement to any AI output before using, sharing or relying on it.	DON'T use personal Microsoft accounts, consumer AI or public AI services for Trust work unless formally assessed and approved. DON'T enter or upload the following into public AI tools: Patient-identifiable data. Confidential clinical or operational data. NHS documents which are not already publicly available. DON'T use AI to make clinical decisions or direct patient care. DON'T rely on AI outputs without checking accuracy, context, bias and suitability.
Protect confidential information.	Only use data you are authorised to access and apply data minimisation.	DON'T enter patient-identifiable, staff-identifiable or otherwise confidential Trust information unless the use has been approved and any required DPIA is in place.
Be transparent about AI use.	Tell people when AI has helped create content where this is relevant, and inform meeting participants when AI transcription or recording features are enabled.	DON'T use AI in a way that misrepresents facts, authorship, decisions or professional judgement.
Keep clinical decision-making separate.	Use AI only to support clinical administration where approved; clinical decisions must remain with qualified staff and established clinical processes. Escalate any AI use that could influence direct care, clinical workflows or patient outcomes.	DON'T use Microsoft M365 Copilot or any AI tool to make clinical decisions, diagnose, prescribe, triage or direct patient care.

Topic	☑ Do	✗ Don't
Escalate higher-risk AI.	Seek approval early for new tools, new suppliers, Trust-wide agents, automation at scale or uses that may affect individuals. Use the interim escalation process until the AI Group is established.	DON'T deploy new AI tools, agents, supplier products or automation at scale without the required governance, assurance and approval.
Report AI concerns and incidents.	Stop and escalate suspected data leakage, unsafe outputs, bias, cyber security concerns or unknown AI agents joining or transcribing meetings.	DON'T ignore or try to manage AI-related security, safety or information governance incidents yourself.

Table of Contents

Summary	2
1. Introduction.....	8
2. Purpose of this Policy/Procedure	8
3. Scope.....	8
4. Definitions/Glossary	8
5. Ownership and Responsibilities	9
5.1. Ownership	9
5.2. Responsibilities	9
5.3. Lead executive.....	9
5.4. Responsible reporting group	9
5.5. Lead professional	10
5.6. Role of the AI Group.....	10
5.7. Role of the Managers	10
5.8. Role of Individual Staff.....	10
6. Standards and Practice.....	11
7. Dissemination and Implementation	20
8. Monitoring compliance and effectiveness	20
9. Updating and Review	21
10. Equality and Diversity	21
Appendix 1. Governance Information	22
Appendix 2. Quality and Equality Impact Assessment (QEIA) Form	25
Appendix 3. AI implementation checklist / lifecycle requirements	26
Appendix 4. AI implementation form – Pilot.....	30
Appendix 5. AI implementation form – Full implementation.....	32
Appendix 6. AI annual review form	34
Supporting document: Terms of Reference - AI Group.....	36
Supporting document: Role profile - Departmental AI Champions.....	40

Data Protection Legislation

The Trust must comply with the UK GDPR, Data Protection Act 2018, and Data (Use and Access) Act 2025 by ensuring all personal data is processed lawfully, fairly, transparently, and for a defined purpose.

Before processing personal data, an appropriate Article 6 UK GDPR lawful basis must be identified and recorded. Where special category data is involved, a relevant Article 9 condition must also be documented.

All staff, contractors, students, volunteers, agency workers, and third parties working on behalf of the Trust are responsible for complying with data protection legislation.

Further guidance is available in the Trust's Information Use Framework and Information Governance policies. Advice can also be obtained from the Information Governance Team.

Royal Cornwall Hospital Trust rch-tr.infogov@nhs.net

1. Introduction

AI is becoming a core capability in modern healthcare. Used well, it can reduce administrative burden, improve access to knowledge, and support service improvement. RCHT will adopt AI in a practical, staff-led way that protects patients, colleagues and the Trust, the wider Cornwall and Isles of Scilly ICS and the NHS in general.

2. Purpose of this Policy/Procedure

- 2.1. This policy sets out how RCHT enables responsible AI use: tools (NHS-approved tools such as Microsoft M365 Copilot when undertaking Trust activities), safe handling of Trust information, and proportionate governance for higher-risk or Trust-wide deployments for Trust activities.
- 2.2. This is the Trust's first AI Policy and supersedes earlier internal AI guidance where it exists. The policy is designed to be used alongside supporting guidance, training and standard operating procedures as these are developed.

3. Scope

- 3.1. Who / what this policy applies to: This policy applies to all staff and anyone working on behalf of RCHT, and to any AI used for Trust work in either a clinical or non-clinical setting across all RCHT sites and services.
- 3.2. Out of scope: This policy complements (and does not replace) existing Trust policies on information governance, IT cyber security, records, procurement, clinical risk, and HR. Personal AI agents are not in the scope of the AI Group but must still comply with this policy. Personal use of consumer and public AI services outside Trust activities is outside the scope of this policy.

4. Definitions/Glossary

- **Artificial intelligence (AI):** technology that performs tasks normally requiring human intelligence (including generative AI).
- **Generative AI:** AI that generates content (for example text) from prompts.
- **Microsoft 365 Copilot:** An AI based tool that is used at the Trust within the NHS Enterprise Data Protection environment. This is powered by a large language model but is not in itself an AI model.
- **Large Language Model (LLM):** An AI model trained on large volumes of text to generate or interpret language. ChatGPT is an example of an application that uses a large language model.
- **AI agent:** a configured AI capability that supports a defined task/workflow using approved instructions and knowledge sources.
- **Personal agent:** an agent used by an individual for their own Trust related activity that is contained within the NHS-approved AI solution (Microsoft M365 Copilot at the time of this version).

- **Trust-wide agent / widely used AI:** AI intended for broad or repeated use that requires formal assurance and AI Group approval before deployment at scale.
- **User:** anyone using an AI tool or system for Trust work.
- **DPIA:** Data Protection Impact Assessment.
- **IG:** Information Governance.
- **Other consumer or public AI services** - such as ChatGPT.
- **Human in the loop:** a human reviewing AI outputs.
- **Automated decision making:** an AI process that does not have a human in the loop review.
- **Ambient scribing:** automated scribing or transcription of conversations.
- **Clinical AI / AI as a Medical Device:** AI that is used for clinical purposes.
- **Non-clinical AI:** AI for business and administrative purposes.

5. Ownership and Responsibilities

5.1. Ownership

The board-level executive responsible for this policy is the Chief Finance Officer (CFO). The CFO sponsors this policy and is accountable for ensuring that AI use in RCHT is appropriately governed, delivers value, and remains safe, ethical and compliant.

5.2. Responsibilities

This policy applies to both clinical and non-clinical AI use. Clinical AI requires clinical governance, information governance, cyber security, procurement, clinical safety oversight and appropriate Caldicott Guardian involvement where relevant. Non-clinical AI should follow CITS, Information Governance, cyber security and procurement routes. The approval pathways for each are set out in this policy so staff can identify the correct route and controls for their use case.

5.3. Lead executive

Chief Finance Officer (CFO) accountable executive for AI governance and this policy.

5.4. Responsible reporting group

- Until established, AI governance will be managed through existing Trust routes coordinated by the Digital Health Group, with escalation to the policy owner for executive decision where required.
- Once established, the AI Group will maintain overall oversight of Trust-wide AI, set policy, receive escalations where required, and carry out annual reviews.

5.5. Lead professional

- Information Governance (including the Data Protection Officer) provides advice on lawful and fair processing, DPIAs and information-handling requirements.
- Cornwall IT Services (CITS) provides technical leadership, configuration, platform assurance and delivery support.
- CITS provides cyber security assurance and incident response where AI is implicated.
- Clinical Safety Officer/CCIO provides clinical safety oversight for use cases that could influence patient care.

5.6. Role of the AI Group

- Set and oversee Trust-wide AI governance expectations, aligned to Trust Standing Orders, Standing Financial Instructions, the Scheme of Delegation, and relevant national guidance and best practice.
- Monitor approvals and make decisions on Trust-wide AI systems, AI agents and automation at scale where policy, risk, contention or uncertainty requires AI Group input.
- Confirm that required assurance is complete (proportionate to risk), including IG/DPIA, cyber security, clinical safety (where applicable), procurement/supplier assurance, and operational readiness.
- Seek any information it requires within its remit from any member of staff; all staff must cooperate with requests made by the AI Group.
- Commission reports, data or specialist advice from Trust teams or external partners as required to discharge its responsibilities.
- Establish and oversee task and finish groups to support delivery of Trust-wide AI priorities and hold them accountable for performance against agreed plans and milestones.

5.7. Role of the Managers

- Ensure staff understand key guardrails (confidentiality, verification, transparency) and use approved tools for NHS activities (Microsoft M365 Copilot).
- Escalate proposed Trust-wide uses or higher-risk use cases through the interim process or (once established) the AI governance groups.

5.8. Role of Individual Staff

- For everyday business and administrative productivity tasks (for example drafting, summarising and meeting notes), use Microsoft M365 Copilot within NHS.net Connect (NHS Enterprise protections), signed in with your NHS account.

- Personal Microsoft M365 Copilot access via a personal Microsoft account and other consumer or public AI services may be used for personal purposes. They should not be used to process, create, analyse or store confidential Trust information, patient information, staff information, or non-public NHS information. Where AI tools are being used in support of Trust activities, staff are expected to use NHS- and Trust-approved AI tools.
- Protect confidentiality and privacy: only use data you are authorised to access, apply data minimisation, and do not enter patient-identifiable, staff-identifiable, or otherwise confidential Trust information unless that has been approved.
- Verify AI outputs before use or sharing; you remain accountable for accuracy, appropriateness and safety of any AI-assisted content.
- Do not use AI for clinical decision-making or to direct patient care; AI may support clinical administration and drafting, but decisions must rely on appropriate professional judgement and established clinical processes.
- Be transparent when sharing AI-assisted content and inform participants when enabling transcription/recording/AI meeting features where applicable. Label AI-assisted content clearly on documents. Only Microsoft M365 within NHS.net Connect should be used to record or transcribe meetings.
- Stop and escalate concerns (for example suspected data leakage, unsafe outputs affecting decisions, bias/discrimination risks, or cyber security concerns) via existing incident routes and notify Information Governance and CITS as required. Escalate if an unknown AI agent connects to or transcribes a meeting.
- Escalate any products that you are aware have now introduced AI to ensure they have had the appropriate governance approvals.
- Seek approval early for Trust-wide use, automation at scale, new tools/suppliers, or use cases that may influence patient care or decisions about individuals (follow the interim escalation process in section 6).
- Keep appropriate records where AI outputs contribute to the clinical or corporate record, in line with Trust records management requirements.
- Stay updated with policies on AI and data protection (acceptable use).

6. Standards and Practice

- 6.1. This section sets out the practical standards and behaviours that enable staff to use AI confidently, while protecting patients, colleagues, and the Trust. The intention is to create clear, usable guardrails: where AI adds value, we want teams to use it; where AI creates unacceptable risk, we want teams to stop, escalate, and seek advice.
- 6.2. How to use this section: controls are risk-based. Everyday productivity use (for example drafting and summarising with Microsoft M365 Copilot) should be simple and supported. As impact increases (for example automation at scale or anything that could influence patient care), additional assurance and approvals apply.

Practical application of this policy

- 6.3. Most staff will only use approved AI tools for routine business and administrative activities. For these uses, staff should follow the user guidance and key guardrails set out in the summary and "Do / Don't" sections of this policy. The more detailed governance requirements described later in this section primarily apply to higher-risk use cases, including new AI tools, clinical AI, Trust-wide deployments, automation at scale, and uses that may influence decisions about individuals or patient care.

AI risk

- 6.4. The level of risk associated with AI use is not determined solely by the activity being performed (for example drafting, summarising, analysing or transcription). Risk also depends on the nature of the information being processed, the potential impact of errors, the individuals affected, and the extent to which outputs may influence decisions or actions.
- 6.5. For example, summarising a routine administrative meeting may represent a relatively low-risk use case, whereas summarising information relating to patient care, safeguarding, complaints, workforce matters or significant organisational decisions may present a higher level of risk. In these situations, users should exercise additional caution and ensure outputs are thoroughly reviewed and verified against source information.
- 6.6. Users should remain aware that AI systems may introduce inaccuracies, omissions, altered emphasis, or unintended changes in meaning, even where outputs appear plausible and professionally presented. The sensitivity of the information and the consequences of error should therefore always be considered when determining the level of assurance, review and governance required.

Human Review and Professional Judgement

- 6.7. AI outputs must always be subject to meaningful human review before they are relied upon, shared, recorded, or used to support decisions. Human review is an important control but should not be regarded as a guarantee that errors, omissions, or unintended changes in meaning will always be detected.
- 6.8. AI systems may generate outputs that appear plausible, professionally written and factually correct while still containing inaccuracies, missing context, altered emphasis, or bias. Users should therefore exercise professional judgement and consider whether the output accurately reflects the source information, intended meaning and organisational context.
- 6.9. Particular care should be taken when using AI to draft, summarise or analyse information relating to patient care, safeguarding, complaints, investigations, workforce matters, legal proceedings, or significant organisational decisions.
- 6.10. Users remain accountable for the accuracy, appropriateness, and consequences of any AI-assisted content. Responsibility for decisions remains with the individual or team using the output and cannot be delegated to an AI system.

6.11. What AI can be used for

- At the date of this policy the only Trust approved AI solution for business administration and general use is Microsoft M365 Copilot. AI solutions for other purposes (such as clinical AI solutions) are subject to the guidelines set out as part of their approval or pilot.
- Any other clinical or non-clinical solution must be subject to approval in accordance with the process set out in this policy.

6.12. General-purpose AI versus Clinical AI

- This policy distinguishes between:
 - General-purpose AI tools (such as Microsoft M365 Copilot), which may be used for approved business, administrative and clinical administration activities but must not be used to make clinical decisions, diagnose, prescribe, triage or direct patient care.
 - Purpose-built clinical AI systems, which may support clinical decision-making or patient care where they have completed the appropriate clinical safety, information governance, procurement, regulatory and governance requirements described in this policy.

6.13. Microsoft M365 Copilot acceptable use

- Use Microsoft M365 Copilot within NHS.net Connect using your NHS account (managed devices where possible).
- Personal Microsoft M365 Copilot access via a personal Microsoft account and other consumer or public AI services may be used for personal purposes. They should not be used to process, create, analyse or store confidential Trust information, patient information, staff information, or non-public NHS information. Where AI tools are being used in support of Trust activities, staff are expected to use NHS- and Trust-approved AI tools.
- Microsoft M365 Copilot is provided for use across NHS.net and the rules relating to your use of NHS.net Connect also apply to your use of Microsoft M365 Copilot, such as the rules relating to the use of sensitive information.
- Microsoft M365 Copilot can be used for all administrative and business support purposes, including those involving sensitive information, such as clinical administration activities with sensitive information.
- If you intend to use sensitive data (including personally identifiable data or pseudonymised data) you must complete a DPIA to set out the reason for the usage. You are expected to only use data that you would have access to in your normal course of work and any variations from this should be clearly documented. Until a DPIA is approved, please use pseudonymised data unless you have access to that data as a normal course of your work. For new projects departmental heads are required to discuss data protection issues with teams so that are aware of how AI can and can't be used.

- Microsoft M365 Copilot can access all information you have permission to view within your NHS.net Connect account, except for documents which have been classified and labelled as 'Official Sensitive'. It is therefore important that you ensure your documents are classified and labelled in accordance with your organisation's data classification requirements. As Microsoft M365 Copilot can access all information which you have permission to view, it is important to ensure that you only have access to data and files necessary for your role.
- When enabling Microsoft M365 Copilot in a Microsoft Teams meeting, you should inform participants (verbally or via the meeting chat) and allow them to opt out if needed. Transparency builds trust and avoids misunderstandings that could upset colleagues inside or outside the organisation.

6.14. In all cases, users remain accountable for checking outputs are accurate, appropriate, and safe.

- Drafting and improving documents and communications (with human review).
- Summarising and organising information you are permitted to access (then confirming against the source).
- Supporting service improvement, readability and translation of non-confidential content, and personal productivity (personal agents) using approved tools and trusted knowledge sources for NHS activities.

6.15. Where Microsoft M365 Copilot must not be used

- Microsoft M365 Copilot must not be used to make clinical decisions or in relation to any activity requiring clinical judgement.
- Creating or using AI outputs in ways that are deceptive or that misrepresent facts, authorship or decisions.
- Automated decision-making that has legal or similarly significant effects on patients or staff without the safeguards required by law and Trust governance (including the right to human review where applicable).

6.16. Uses of AI for clinical and non-clinical purposes should follow the AI implementation checklist at [Appendix 3](#). The AI Group will coordinate intake, triage, and assurance through its clinical and non-clinical routes, approve cases where appropriate, maintain overall oversight, set policy, receive escalations where required, and carry out annual reviews. This covers:

- Use case and data sources: document the purpose of the AI tool, system or process, the intended users, the decisions or tasks it supports, and the data sources to be used.
- Clinical safety applicability: Where the AI could influence direct care, clinical safety assurance must be completed in line with DCB0160 and relevant clinical governance, and suppliers must provide evidence aligned with DCB0129 where applicable.

- Information governance and DPIA: Where personal data is processed, Information Governance must be engaged early. DPIAs and lawful-basis considerations may be framed broadly at an early stage for departments or categories of use and then refined as use cases and risks become clearer. Ensure transparency, data minimisation, access control and retention requirements are met.
- Automated decision-making safeguards: Where AI meaningfully influences decisions about individuals, ensure safeguards are in place, including meaningful human review, transparency about AI involvement, and routes for challenge/contestability as required.
- Supplier and product assurance: AI considerations must be identified and addressed explicitly at the procurement stage from the outset, including where suppliers describe functionality as automation, decision support or similar terms rather than AI. Third-party AI-enabled products must be assessed through procurement, Information Governance and CITS routes, proportionate to risk, with any required NHS assurance expectations (including Digital Technology Assessment Criteria (DTAC) where applicable) and clear contractual terms for data use, security and accountability completed before purchase or deployment. This applies to both procured and free products.
- Cyber Security: Implement proportionate technical controls (least-privilege access, secure configuration, and protection against common AI risks such as prompt injection and data leakage in integrated workflows).
- Testing and quality assurance: Validate outputs for accuracy, bias/fairness risks, and operational reliability before go-live; define acceptance criteria; test against representative scenarios.
- Change control: Material changes must be risk-assessed and may require re-approval. This includes new data sources, new integrations, expanded scope, new users, model or configuration changes, and the introduction of AI functionality into an existing system. The Trust should maintain a proportionate process that supports timely decisions on change requests and new use cases, with lighter-touch routes for low-risk pilots or minor changes within approved guardrails.
- Monitoring: Define how performance, safety incidents, and unexpected behaviour will be monitored (including feedback routes), and how the Trust will respond (rollback/disable, fixes, communications).
- Records and retention: ensure prompts, outputs and decisions that form part of the clinical or corporate record are handled in line with Trust records management requirements.

6.17. AI lifecycle requirements

- All AI tools, systems and processes approved through this policy will be subject to an annual review starting 12 months after sign-off with an option to bring forward the review at any point given the rapid pace of change in relation to AI. Annual reviews will be carried out by the AI Group.
- The lifecycle requirements are summarised at [Appendix 3](#).

- The annual review form is shown at [Appendix 6](#).

6.18. The AI Group will hold a register of Trust-wide AI tools, systems and processes that have been approved or escalated to the AI Group for decision. This will include a named owner, purpose, data sources, supplier, approvals, and review date.

6.19. Interim escalation and decision process (until AI governance groups are established).

- Immediate safety / incident escalation: if there is suspected data leakage, unsafe outputs affecting decisions, or cyber compromise, stop use and report via existing incident and information security routes, and notify the IG Team, Clinical Governance, Clinical Safety and CITS without delay.
- Submit proposal for triage: email the Information Governance Team (rch-tr.infogov@nhs.net) with owner, purpose, intended users (individual/department/Trust-wide), data involved, proposed tool/supplier, and whether it could influence patient care or decisions about individuals.
- Interim triage: IG will coordinate triage with CITS (and clinical safety where relevant) to agree assurance needed (for example DPIA, clinical safety, procurement/DTAC, cyber security review) and confirm decision route.
- Decision route: low-risk departmental use within approved tools may proceed once controls are confirmed; Trust-wide, high-risk, new supplier, or automation-at-scale proposals must be escalated for executive decision via the policy owner and existing governance routes, with advice recorded. Approval processes should be as quick and easy as possible while remaining safe and defensible, with a deliberately lighter-touch approach for time-limited pilots, low-risk exploratory use, and minor changes within approved guardrails.
- Record and review: the Digital Health Group will maintain an interim Trust AI register/log of proposals and decisions (owner, purpose, tool, data, approvals, review date) until the AI Group is established.

6.20. Example use cases

- Examples of appropriate AI use cases include:
 - Reporting and analysis.
 - Productivity and administrative support.
 - Summarisation and meeting support.
 - Scribing and documentation support.
 - Workflow support and automation.
 - Data science and research.
 - Clinical applications.

6.21. Incident management and reporting

AI-related incidents and near misses must be reported and managed through existing Trust incident and information security reporting routes, with escalation to IG, CITS, clinical safety and clinical governance as appropriate. Examples include: suspected data leakage, inappropriate access, unsafe/incorrect outputs affecting decisions, and failures in configured agents or automation.

6.22. Risk-based assurance (what changes as risk increases)

- Assurance increases with sensitivity, scale and potential impact on patient care or significant decisions. The approval processes are designed to be as quick and easy as possible while remaining safe and defensible, with a deliberately lighter-touch approach for time-limited pilots and low-risk exploratory use within approved guardrails.
- Low risk: everyday Microsoft M365 Copilot drafting and summarising within your access, with verification and transparency.
- Personal data or patient impact: engage IG (DPIA where required) and follow clinical governance/clinical safety where care could be influenced or where the data being used is not normally accessible to individuals in their role.
- New tools or scale: engage Procurement/CITS for assurance and obtain AI Group approval for Trust-wide agents/systems or automation at scale (once the AI Group is established).

6.23. Implementation and dissemination:

Once approved, this policy will be actively communicated through Trust channels with clear staff-facing messages on what has changed, what staff need to do, where approved guidance is located, and how support or approval can be sought. Line managers and Departmental AI Champions will support local adoption. Where new tools or Trust-wide agents are proposed, teams must follow the interim escalation process (or, once established, the AI governance groups) before deployment.

6.24. Related legislation, national and local guidance.

- Data Protection Act 2018 (UK GDPR) lawful basis, transparency, data minimisation, rights and DPIA where required.
- Equality Act 2010 fairness and non-discrimination; consider bias/fairness in testing where relevant.
- NHS clinical safety standards DCB0129/DCB0160 (where applicable).
- NHS and NHS.net Connect acceptable use guidance for Microsoft M365 Copilot (where applicable).
- [Human Rights Act 1998](#).
- [Computer Misuse Act 1990](#).

- [Freedom of Information Act 2000](#).
- [The Environmental Information Regulations 2004](#).
- Confidentiality: NHS Code of Practice - [GOV.UK](#).
- The Caldicott Principles - [GOV.UK](#).
- Data Retention and Information Management Policy – [NHSmail Support](#).
- [Clinical risk management standards - NHS England Digital](#).
- Data (Use and Access) Act 2025.
- [Data \(Use and Access\) Act 2025 | ICO](#).
- Updated DTAC form and guidance (v2 - mandatory 6 April 2026).
- Updated NHS England Digital Technology Assessment Criteria (DTAC) form and guidance - [Innovation Service](#).
- Data protection and automated decision-making.
- Data (Use and Access) Act 2025 - what it means for organisations - ICO. <https://ico.org.uk/about-the-ico/what-we-do/legislation-we-cover/data-use-and-access-act-2025/>.
- Guidance on AI and data protection - ICO. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/>.
- Explaining decisions made with AI - ICO and The Alan Turing Institute. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/explaining-decisions-made-with-artificial-intelligence/>.
- National data opt-out - NHS England. <https://digital.nhs.uk/services/national-data-opt-out>.
- Clinical safety and medical device.
- Clinical risk management standards (DCB0129 and DCB0160) - NHS England. <https://digital.nhs.uk/services/clinical-safety/clinical-risk-management-standards>.
- Software and Artificial Intelligence (AI) as a Medical Device - MHRA / GOV.UK. <https://www.gov.uk/government/publications/software-and-artificial-intelligence-ai-as-a-medical-device>.
- Yellow Card - reporting for medical devices - MHRA. <https://yellowcard.mhra.gov.uk/>.
- NHS assurance, security and procurement.

- Digital Technology Assessment Criteria (DTAC) - NHS England Transformation Directorate. <https://transform.england.nhs.uk/key-tools-and-info/digital-technology-assessment-criteria-dtac/>.
- AI and Digital Regulations Service (AIDRS) - live navigator - NHS England. <https://www.digitalregulations.innovation.nhs.uk/>.
- CAF-aligned Data Security and Protection Toolkit (DSPT) - NHS England. <https://transform.england.nhs.uk/information-governance/caf-aligned-dspt-evolution-of-our-assurance-model/>.
- Generative AI and ambient scribing.
- Guidance on the use of AI-enabled ambient scribing products - NHS England. <https://www.england.nhs.uk/long-read/guidance-on-the-use-of-ai-enabled-ambient-scribing-products-in-health-and-care-settings/>.
- Ambient Voice Technology (AVT) Self-Certified Supplier Registry - NHS England. <https://digital.nhs.uk/services/ambient-scribing/ambient-voice-technology-self-certified-supplier-registry>.
- AI governance principles and equality.
- Implementing the UK's AI regulatory principles (the five principles) - DSIT / GOV.UK. <https://www.gov.uk/government/publications/implementing-the-uks-ai-regulatory-principles-initial-guidance-for-regulators>.

6.25. Associated Trust policies and documents

Sponsor to populate with relevant RCHT policies and documents (for example: Information Governance and data protection policies, records management, IT and cyber security policies, procurement and supplier assurance, clinical risk and safety governance, incident reporting, Acceptable Use Policy, IT Security Policy, Collaboration (Email, Chat and Instant Messaging) Policy).

6.26. Training requirements

Training and support should be staged and role appropriate. Initial support should cover access to approved AI tools and the basics of using AI properly and safely. Core training should cover safe prompting, verification, confidentiality, transparency and the human-in-the-loop principle. Enhanced training should be provided for applications such as Excel which will use significant data and require more oversight than other applications, as well as staff designing agents, automation or Trust-wide deployments, including risk assessment, DPIA and clinical safety pathways, testing, monitoring and incident reporting. Queries should be escalated via line management, Information Governance or CITS as appropriate.

7. Dissemination and Implementation

- 7.1. This policy will be implemented through publication on the RCHT Document Library and active communication through Trust channels. Staff-facing communications should clearly explain what has changed, what staff need to do, where approved guidance is located, and how support or approval can be sought. Line managers are responsible for reinforcing the key guardrails: use approved tools, protect confidential information, verify outputs, and be transparent when sharing AI-assisted content.
- 7.2. Until the AI Group is established, proposals for Trust-wide or higher-risk AI will be managed using the interim escalation and decision process in section 6, coordinated by Information Governance and CITS with escalation to the policy owner where executive decisions are required. Supporting materials (for example FAQs, prompt guidance, and simple intake and testing checklists) will be developed and maintained by CITS and Information Governance.
- 7.3. Where helpful, RCHT will consider collaboration and alignment with partner organisations, including CFT, particularly where staff, systems, governance arrangements, or learning are shared.

8. Monitoring compliance and effectiveness

Information Category	Detail of process and methodology for monitoring compliance
Element to be monitored	Compliance with AI guardrails (use of approved tools, handling of confidential data, verification and transparency) and compliance with lifecycle requirements for Trust-wide/higher-risk AI (register, DPIA/clinical safety/cyber security/testing/monitoring).
Lead	Policy owner (CFO) supported by Information Governance, CITS; once established, the AI Group will provide oversight.
Tool	Trust AI register/log; DPIA records; cyber security assurance records; clinical safety documentation where applicable; incident reporting; periodic sampling/audit of Trust-wide deployments.
Frequency	At least annually, and by exception following significant incidents or major Trust-wide AI changes/rollouts.
Reporting arrangements	Reporting through existing Trust governance routes (Information Governance Group, cyber security governance and relevant clinical governance). Once established, reporting via AI Group (and by exception to ELT/committees as agreed).
Acting on recommendations and Lead(s)	Actions assigned to IG/CITS/clinical safety owners as appropriate; escalated to policy owner for resolution and resource decisions.
Change in practice and lessons to be shared	Lessons learned shared via CITS and governance communications; policy and supporting SOPs/guidance updated where required.

9. Updating and Review

This policy will be reviewed at least annually, and earlier where there are material changes to NHS guidance, law or regulation, or significant changes to the Trust's AI capability or risk profile. Approved tools and their associated risks should also be reviewed regularly to confirm ongoing fitness for purpose, safety, security, and compliance. Significant revisions will follow the Trust's standard consultation, approval, and dissemination processes. Minor updates (for example organisational title changes) may be approved by the accountable executive and re-published.

10. Equality and Diversity

10.1. RCHT is committed to equality, diversity, and inclusion. AI must be used in ways that are fair, transparent, and non-discriminatory. Where Trust-wide or higher-risk AI is proposed, the risk assessment and testing approach should consider potential bias, accessibility and differential impacts, and any concerns should be escalated via the interim process (or the AI Group once established).

10.2. This document complies with the Royal Cornwall Hospitals NHS Trust service Equality and Diversity statement which can be found in the [Equality Diversity and Inclusion Policy](#) or the [Equality and Diversity website](#).

10.3. Quality and Equality Impact Assessment (QEIA)

The QEIA process allows RCHT to monitor the impact of changes to its policies and services, ensuring that nobody is unduly disadvantaged. The Quality and Equality Impact Assessment (QEIA) Form is available via the link in [Appendix 2](#).

Appendix 1. Governance Information

Information Category	Detailed Information
Document Title:	AI (Artificial Intelligence) Policy V1.0
This document replaces (exact title of previous version):	None
Date Issued/Approved:	3 September 2026
Date Valid From:	September 2026
Date Valid To:	September 2027
Author/Owner:	Adam Wheeldon – Associate Director of Finance
Contact details:	Adam.wheeldon@nhs.net
Brief summary of contents:	This policy has two purposes: (1) staff guidance for approved AI tools currently available and (2) governance arrangements for future AI systems. This policy sets out RCHT's approach to the safe, responsible and proportionate use of artificial intelligence across clinical and non-clinical settings. It describes approved AI use, Microsoft M365 Copilot acceptable use, information governance and data protection requirements, clinical safety controls, cyber security, procurement and supplier assurance, escalation and approval routes, monitoring, incident reporting, training, and lifecycle requirements for pilots, full implementation and annual review.
Suggested Keywords:	Artificial Intelligence; AI; Generative AI; Microsoft M365 Copilot; NHS.net Connect; AI governance; AI Group; AI agents; clinical AI; non-clinical AI; automation; information governance; DPIA; data protection; cyber security; clinical safety; DCB0129; DCB0160; DTAC; procurement; supplier assurance; records management; incident reporting; AI annual review.
Target Audience:	RCHT: Yes CFT: No CIOS ICB: No
Executive Director responsible for Policy:	Chief Finance Officer

Information Category	Detailed Information
Approval route for consultation and ratification:	Executive Directors support. Staff Side support. Executive Leadership Team support. Audit and Risk Assurance Committee support. Trust Board Approval.
Manager confirming approval processes:	Adam Wheeldon – Associate Director of Finance
Name of Governance Lead confirming consultation and ratification:	Adam Wheeldon – Associate Director of Finance
Links to key external standards:	None required
Related Documents:	Management of Information, Records and Data Quality Policy; Information Governance and data protection policies; Data Protection Impact Assessment guidance; IT Security Policy; Acceptable Use Policy; Collaboration, Email, Chat and Instant Messaging Policy; Incident Reporting Policy; Procurement and supplier assurance procedures; Clinical Risk Management / Clinical Safety Policy; Records Management Policy; Quality and Equality Impact Assessment guidance; AI implementation checklist and lifecycle requirements; AI implementation forms for pilot and full implementation; AI annual review form; Terms of Reference for the AI Group; Departmental AI Champions role profile.
Training Need Identified:	No
Publication Location (refer to Policy on Policies – Approvals and Ratification):	Internet and Intranet
Document Library Folder/Sub Folder:	Finance / Finance General

Version Control Table

Date	Version Number	Summary of Changes	Changes Made by
July 2026	V1.0	New document.	Adam Wheeldon, Associate Director of Finance

All or part of this document can be released under the Freedom of Information Act 2000.

All Policies, Strategies and Operating Procedures, including Business Plans, are to be kept for the lifetime of the organisation plus six years.

This document is only valid on the day of printing.

Controlled Document.

This document has been created following the Royal Cornwall Hospitals NHS Trust [The Policy on Policies \(Development and Management of Knowledge Procedural and Web Documents Policy\)](#). It should not be altered in any way without the express permission of the author or their Line Manager.

Appendix 2. Quality and Equality Impact Assessment (QEIA) Form

The QEIA process allows RCHT to monitor the impact of changes to its policies and services, ensuring that nobody is unduly disadvantaged.

Please ensure you have completed a Quality and Equality Impact Assessment (QEIA) using this link to complete the form:

[E11 QEIA Policy](#)

For guidance, please see the [QEIA Essentials – Quick Reference Guide](#) or contact as required below:

Equality, Diversity and Inclusion guidance, please contact: rcht.inclusion@nhs.net

Quality Governance guidance, please contact Jillian Tozer: jillian.tozer3@nhs.net

Appendix 3. AI implementation checklist / lifecycle requirements

Completion of the checklist will enable the five UK AI principles to be confirmed (safety / robustness; transparency and explainability; fairness; accountability; contestability).

Process	Use of NHS-approved AI tools for business and administration purposes (Microsoft M365 Copilot)	Pilot	Full implementation	Annual review
AI tool, system or process name	Complete name.	Complete name.	Complete name.	Confirm the approved tool, system or process remains the same, or describe any changes.
Owner	Complete name.	Complete name.	Complete name.	Confirm the current business owner and whether ownership has changed.
Use case and data sources to be used	Use within approved Microsoft M365 Copilot scope for business and administrative purposes.	Assess the use case, intended users, expected benefits, and the data sources to be used.	Confirm the approved use case, operational scope, intended users, and the data sources to be used.	Confirm the use case remains appropriate and that the data sources in use remain accurate and appropriate.
Clinical safety applicability	Not applicable unless the use could influence direct care.	Identify the Clinical Safety Officer lead where applicable. Document against DCB clinical safety standards. Clinical safety assurance must be completed in line with DCB0160 and relevant clinical governance, and suppliers must provide evidence aligned with	Identify the Clinical Safety Officer lead where applicable. Confirm clinical safety evidence, DCB0160 / DCB0129 position, and any medical device considerations.	Confirm clinical safety standards continue to be met and record any updated clinical safety considerations.

Process	Use of NHS-approved AI tools for business and administration purposes (Microsoft M365 Copilot)	Pilot	Full implementation	Annual review
		DCB0129 where applicable.		
Information governance and DPIA	Follow approved Copilot arrangements. Complete a departmental DPIA where personal or confidential data is used, and consider any sharing agreements.	Complete DPIA requirements, consider any sharing agreements, and record the approval route.	Confirm the completed DPIA, lawful basis, transparency arrangements, sharing agreements, and approval status.	Review the DPIA and resubmit if appropriate. Confirm whether any new processing or sharing arrangements have been introduced.
Automated decision-making safeguards	Not applicable.	Where AI meaningfully influences decisions about individuals, document safeguards including meaningful human review, transparency about AI involvement, and routes for challenge or contestability.	Where AI meaningfully influences decisions about individuals, confirm safeguards including meaningful human review, transparency about AI involvement, and routes for challenge or contestability.	Provide an assessment of any changes in arrangements since implementation.
Supplier and product assurance	Not applicable.	Provide supplier name, product details, licensing or pilot arrangement, contract dates if applicable, and any known upgrade or scalability considerations.	Provide supplier and product details, contract and licensing arrangements, support model, and upgrade notification arrangements, including where AI functionality is described using other terms such as automation or decision support.	Provide any updates on supplier performance, contract changes, licensing, service support, upgrades, or new AI-related functionality introduced in the past 12 months.

Process	Use of NHS-approved AI tools for business and administration purposes (Microsoft M365 Copilot)	Pilot	Full implementation	Annual review
Cyber Security	Not applicable beyond approved platform controls.	Conduct a preliminary digital security assessment against DSPT and cyber security requirements.	Conduct a full digital security assessment against DSPT and cyber security requirements.	Provide an update on any digital security issues, incidents, reassessments, or mitigation changes arising in the past 12 months.
Testing and quality assurance	Not applicable.	Document how testing will be carried out and how quality assurance will be obtained as part of the pilot.	Validate outputs for accuracy, fairness, and operational reliability before go-live; define acceptance criteria; and test against representative scenarios.	Provide an update on how testing, monitoring, and output validation continue to confirm accuracy, fairness, and operational reliability.
Approval	Not applicable.	Approval through the AI Group (AIG) .	Approval through the AI Group (AIG) .	Annual review submitted to the AI Group (AIG) .
Monitoring	Not applicable.	Set out how the pilot will be monitored, including feedback, incidents, benefits, and review points.	Define how performance, incidents, feedback, unexpected behaviour, and benefits will be monitored, including rollback or disable arrangements if required.	Confirm monitoring outcomes, incidents, feedback, benefits, and actions taken during the review period.
Records and retention	Follow Trust records management requirements where prompts, outputs, or decisions form part of the clinical or corporate record.	Ensure prompts, outputs, and decisions that form part of the clinical or corporate record are handled in line with Trust records	Ensure prompts, outputs, and decisions that form part of the clinical or corporate record are handled in line with Trust records	Confirm records and retention arrangements remain compliant with Trust requirements.

Process	Use of NHS-approved AI tools for business and administration purposes (Microsoft M365 Copilot)	Pilot	Full implementation	Annual review
		management requirements.	management requirements.	

Appendix 4. AI implementation form – Pilot

Governance route: This form supports review and approval by the **AI Group (AIG)**.

Category	Information
AI tool, system or process name	Click or tap here to enter the full name.
Business owner	Click or tap here to enter the name, role and department.
Clinical or non-clinical use	Click or tap here to describe whether this pilot is clinical, non-clinical, or mixed, and where it will be used.
Pilot purpose and use case	Click or tap here to describe the problem being addressed, intended users, expected benefits, and the decisions or tasks the AI will support.
Data sources to be used	Click or tap here to list the data sources, systems, and information types the pilot will access or process.
Clinical safety applicability	Click or tap here to confirm whether the pilot could influence direct care, clinical workflows, or patient outcomes. If yes, name the Clinical Safety Officer lead and outline the planned DCB0160 / DCB0129 approach.
Information governance and DPIA	Click or tap here to confirm whether personal data is involved, whether a DPIA is required, any data-sharing considerations, and the planned approval route.
Automated decision-making safeguards	Click or tap here to explain whether the AI will meaningfully influence decisions about individuals and, if so, how meaningful human review, transparency, and challenge routes will be maintained.
Supplier and product details	Click or tap here to provide the supplier name, product name, licensing or pilot arrangement, contract dates if applicable, and any known upgrade or scalability considerations.
Cyber Security assessment	Click or tap here to summarise the preliminary digital security assessment, including DSPT / cyber security considerations and any identified risks or mitigations.
Testing and quality assurance plan	Click or tap here to describe how testing will be carried out during the pilot, including accuracy checks, fairness considerations, operational reliability, and acceptance criteria.
Records and retention	Click or tap here to explain how prompts, outputs and decisions that form part of the clinical or corporate record will be handled in line with Trust records management requirements.

Category	Information
Pilot timescale	Click or tap here to enter the planned start date, end date and review point.
Workforce Implications	Click or tap here to confirm that the organisational change process will be followed if the AI project will have an impact on workforce.
Approval	Click or tap here to record the AI Group (AIG) decision, date, conditions of approval, and named approver.

Appendix 5. AI implementation form – Full implementation

Governance route: This form supports review and approval by the **AI Group (AIG)**.

Category	Information
AI tool, system or process name	Click or tap here to enter the full name.
Business owner	Click or tap here to enter the name, role and department.
Clinical or non-clinical use	Click or tap here to describe whether the implementation is clinical, non-clinical, or mixed, and where it will be used.
Use case and operational scope	Click or tap here to describe the approved use case, intended users, service areas, expected benefits, and any limits on use.
Data sources to be used	Click or tap here to list the data sources, systems, and information types the implementation will access or process.
Clinical safety assurance	Click or tap here to identify the Clinical Safety Officer lead, summarise the DCB0160 / DCB0129 evidence, and note any medical device or regulatory considerations if applicable.
Information governance and DPIA	Click or tap here to summarise the completed DPIA, lawful basis, transparency arrangements, data-sharing agreements, and approval status.
Automated decision-making safeguards	Click or tap here to explain how meaningful human review, transparency, and challenge routes are maintained where the AI influences decisions about individuals.
Supplier and product assurance	Click or tap here to provide supplier and product details, contract and licensing arrangements, service support model, upgrade notification arrangements, and how AI-related functionality is identified if described using other terms such as automation or decision support.
Cyber Security assessment	Click or tap here to summarise the full digital security assessment, cyber security review outcome, key risks, and agreed mitigations.
Testing and quality assurance	Click or tap here to confirm how outputs were validated for accuracy, fairness, and operational reliability, including representative scenarios, acceptance criteria, and any residual limitations.

Category	Information
Training, communications and support	Click or tap here to describe user training, staff communications, local guidance, support arrangements, and escalation routes.
Monitoring arrangements	Click or tap here to describe how performance, incidents, feedback, unexpected behaviour, and benefits will be monitored, including rollback or disable arrangements if required.
Records and retention	Click or tap here to explain how prompts, outputs and decisions that form part of the clinical or corporate record will be handled in line with Trust records management requirements.
Workforce Implications	Click or tap here to confirm that the organisational change process will be followed if the AI project will have an impact on workforce.
Approval	Click or tap here to record the AI Group (AIG) decision, approval date, conditions, go-live date, and named approver.

Appendix 6. AI annual review form

Category	Information
AI tool, system or process name	Click or tap here to enter the full name.
Business owner	Click or tap here to enter the name, role and department.
Date of last approval / review	Click or tap here to enter the most recent approval or review date.
Clinical or non-clinical use	Click or tap here to confirm whether the current use remains clinical, non-clinical, or mixed, and whether the scope has changed.
Use case review	Click or tap here to confirm that the use case remains appropriate, proportionate, and within the originally approved scope, or describe any changes.
Data sources review	Click or tap here to confirm whether the data sources in use remain accurate and appropriate, and whether any new data sources or integrations have been introduced.
Clinical safety review	Click or tap here to confirm whether clinical safety standards continue to be met, summarise any new safety issues, and record any updated DCB0160 / DCB0129 considerations if applicable.
Information governance and DPIA review	Click or tap here to confirm whether the DPIA remains current, whether any new processing or sharing arrangements have been introduced, and whether resubmission is required.
Automated decision-making safeguards review	Click or tap here to confirm whether arrangements for meaningful human review, transparency, and challenge remain effective, and describe any changes since implementation.
Supplier and contract review	Click or tap here to provide any relevant updates on supplier performance, contract changes, licensing, service support, upgrades, or new AI-related functionality introduced in the past 12 months.
Cyber Security review	Click or tap here to summarise any digital security issues, incidents, reassessments, or mitigation updates arising in the past 12 months.

Category	Information
Testing, accuracy and quality review	Click or tap here to explain how ongoing testing, monitoring, and output validation have confirmed accuracy, fairness, and operational reliability over the review period.
Monitoring and incidents	Click or tap here to summarise performance, benefits, user feedback, incidents, near misses, unexpected behaviour, and actions taken.
Records and retention review	Click or tap here to confirm whether prompts, outputs and decisions that form part of the clinical or corporate record continue to be handled in line with Trust records management requirements.
Outcome of annual review	Click or tap here to record the recommendation: continue unchanged, continue with actions, pause pending actions, or retire.
Submission and sign-off	Click or tap here to record the date submitted to the AI Group (AIG), the review decision, actions required, action owner, and next review date.

The sections that follow are not part of the policy but may be useful for the application of it.

Supporting document: Terms of Reference - AI Group

1. Constitution

1.1. The AI Group (AIG) operates under the authority of the Executive Leadership Team to provide multidisciplinary oversight of AI deployments, set Trust-wide AI policy and governance expectations, receive escalations where required, and carry out annual reviews.

1.2. The AI Group has no delegated powers other than those specified in these Terms of Reference and the Trust Scheme of Delegation.

2. Authority

2.1. The AI Group is authorised by the Executive Leadership Team to:

- Set and oversee Trust-wide AI governance expectations, aligned to Trust Standing Orders, Standing Financial Instructions, the Scheme of Delegation, and relevant national guidance and best practice.
- Monitor approvals and make decisions on Trust-wide AI systems, AI agents and automation at scale where policy, risk, contention or uncertainty requires AI Group input.
- Confirm that required assurance is complete (proportionate to risk), including IG/DPIA, cyber security, clinical safety (where applicable), procurement/supplier assurance, and operational readiness.
- Seek any information it requires within its remit from any member of staff; all staff must cooperate with requests made by the AI Group.
- Commission reports, data or specialist advice from Trust teams or external partners as required to discharge its responsibilities.
- Establish and oversee task and finish groups to support delivery of Trust-wide AI priorities and hold them accountable for performance against agreed plans and milestones.

3. Purpose

3.1. The purpose of the AI Group is to maintain overall oversight of Trust-wide AI, set policy, provide strategic assurance and decision-making, receive escalations where required, and carry out annual reviews so that AI is adopted safely, lawfully, ethically and with clear accountability.

3.2. The Group shall:

- Provide the Trust-wide route for oversight, escalation, annual review and policy-setting for AI systems and agents, including clinical and non-clinical routes as set out in this policy.
- Set expectations for risk-based assurance and minimum standards for AI lifecycle controls (register, DPIA/IG, clinical safety where applicable, cyber security, testing, monitoring, change control and records).

- Maintain oversight of the Trust AI register and ensure owners and review dates are in place for Trust-wide AI.
- Review AI-related incidents, near misses and emerging risks/themes, and ensure appropriate actions are taken and learning is shared.
- Oversee benefits measurement for Trust-wide AI deployments and ensure monitoring arrangements are proportionate to risk and value.
- Agree priorities and sequencing for Trust-wide AI delivery (in alignment with Digital Health Group and Trust strategy).
- Receive proposed AI use cases and confirm that each has a named owner, clear purpose and an appropriate route for review.
- Review use cases through either the clinical route or the non-clinical route, drawing in the right assurance input for each.
- Support teams to complete the information needed for review, assurance, pilot or implementation.
- Approve use cases through the agreed clinical and non-clinical routes where assurance is sufficient and escalation is not required.

4. Membership

4.1. Core membership should be multidisciplinary and will be confirmed when the Group is established. As a minimum, the AI Group will include representation from:

- Chief Finance Officer (CFO) – Chair.
- Chief Information Officer – Vice Chair.
- Trust AI lead / Trust AI Champions (as nominated by the Chair).
- Head of Information Governance.
- Caldicott Guardian or representative.
- Clinical leadership (e.g., CCIO/Clinical Safety Officer or nominee).
- Cyber security representative (CITS).
- Divisional Director.
- JCNC Representative.
- Medical Devices Representative.

4.2. Where a core member is unable to attend, they may nominate a deputy with sufficient authority and expertise for the agenda, who will count towards quorum.

5. Attendance

5.1. The Group may invite other colleagues or external advisors to attend for specific items (for example: equality and inclusion leads, HR, research governance, legal, suppliers, or service leads).

6. Duties

- **Set and maintain Trust-wide AI policy and governance:** agree and maintain the Trust approach to AI oversight, approval thresholds and minimum assurance artefacts, and ensure alignment to national guidance and internal policies.
- **Approve and review Trust-wide AI:** review proposals and confirm approvals and conditions, including go-live readiness and monitoring arrangements, and carry out annual reviews of approved Trust-wide AI.
- **Oversee assurance and risk:** ensure IG/DPIA, cyber security, clinical safety and procurement assurance are completed proportionately; review incidents and risks and ensure mitigating actions are taken.
- **Oversee delivery and escalations:** receive progress reports and escalations from task and finish groups, and resolve issues or unblock delivery where required.
- **Benefits and learning:** agree benefits measures; review performance and adoption; ensure learning is captured and guidance is updated.

7. Quorum

7.1. The quorum necessary for the transaction of business shall be: (a) the Chair or nominated Vice Chair; and (b) at least two other core members (or nominated deputies), including IG and either Digital or CITS. For clinical AI items, clinical representation (e.g., Clinical Safety Officer/CCIO) should be present.

8. Secretary

8.1. Secretariat support will be provided by an agreed administrative lead (to be confirmed).

9. Frequency of meetings

9.1. The AI Group will meet monthly once established. By exception, urgent decisions may be taken via an extraordinary meeting or e-governance route at the request of the Chair, subject to quorum.

10. Minutes and reporting

10.1. The minutes of all meetings of the AI Group shall be formally recorded. Decisions may also be recorded via the Trust's e-governance route where applicable.

10.2. The AI Group will report by exception to the Executive Leadership Team and to the Audit and Risk Assurance Committee.

11. Performance and evaluation

11.1. The AI Group will review its collective performance and effectiveness at least annually, including whether membership and work plans remain appropriate to the Trust's AI risk profile and priorities.

12. Review

12.1. These Terms of Reference shall be reviewed at least annually and updated to reflect changes in national guidance, Trust governance arrangements, and the Trust's AI maturity. As AI usage in the Trust expands, the AI Group may decide to establish task and finish arrangements to support proposed AI use cases, review them through the appropriate clinical or non-clinical route, and support the safe progression of approved work. Its remit is specifically to cover AI usage, associated assurance and AI-specific approval/escalation routes.

Supporting document: Role profile - Departmental AI Champions

1. Purpose of the role

Departmental AI Champions provide practical, local support to help teams use approved AI safely, confidently and productively. The role is intended to support adoption of the Trust's AI Policy by reinforcing good practice, helping colleagues understand what is and is not permitted, encouraging the use of approved tools such as Microsoft M365 Copilot, and acting as a simple local route for questions, feedback and escalation.

This is a champion role rather than a separate management, digital, information governance or cyber security function. Departmental AI Champions help colleagues apply the policy in day-to-day practice, surface issues early, and support structured learning and continuous improvement within their service or department.

2. Scope

A Departmental AI Champion should normally be a member of staff within the relevant service, division or corporate team who has an interest in digital improvement, good awareness of the Trust AI Policy, and sufficient credibility within the team to support colleagues and promote consistent practice. The role may be held alongside an existing substantive post.

3. Core role

- Promote awareness of the Trust AI Policy, local guidance and approved tools, with a clear emphasis on Microsoft M365 Copilot-first working for appropriate business and administrative use.
- Provide first-line peer support to colleagues on everyday safe use of approved AI tools, including prompting practice, verification of outputs, transparency when sharing AI-assisted content, and protection of confidential information.
- Guide colleagues through an idea or use case explaining how it needs to be approved.
- Encourage consistent use of approved templates, checklists and supporting materials where these exist.
- Surface local issues, barriers, training needs, examples of good practice and potential opportunities for wider learning to the relevant Information Governance, CITS or governance leads.
- Support local communications, demonstrations and practical awareness activity to improve confidence and adoption.
- Promote appropriate record keeping where AI outputs form part of the corporate or clinical record, in line with Trust requirements.
- Escalate suspected incidents, unsafe outputs, data protection concerns, cyber security concerns, bias concerns or unapproved AI use promptly through the appropriate existing routes.

4. What Departmental AI Champions are not responsible for

- They are not the approval authority for new AI tools, Trust-wide AI, higher-risk use cases, clinical AI, or automation at scale.
- They are not expected to provide formal information governance, legal, procurement, cyber security or clinical safety advice.
- They are not accountable for checking or approving colleagues' outputs; responsibility remains with the person creating, using or sharing the content and with the relevant line manager or service lead where applicable.
- They should not create local workarounds that bypass Trust policy, approved tools or established escalation routes.

5. Expected knowledge, skills and behaviours

- Good understanding of the Trust AI Policy and the main guardrails for safe use of approved AI tools.
- Confidence in explaining practical guidance to colleagues in a clear, proportionate and supportive way.
- Awareness of when to stop, seek advice and escalate.
- Commitment to safe, ethical and inclusive use of AI, including awareness of bias, confidentiality and accessibility considerations.
- Strong local relationships and willingness to share learning across teams.

6. Training and support for Departmental AI Champions

Departmental AI Champions should receive proportionate support so that they can perform the role effectively. As a minimum this should include an introduction to the Trust AI Policy, approved tools and acceptable use expectations, practical prompting and verification guidance, information governance and confidentiality guardrails, and how to escalate issues or proposals.

7. Escalation routes

Departmental AI Champions should use the same formal routes as other staff. Immediate concerns relating to suspected data leakage, unsafe outputs affecting decisions, cyber security issues, or other incidents should be escalated through existing Trust incident and information security routes without delay. Questions about lawful basis, confidentiality, DPIA requirements or data use should be directed to the Information Governance Team. Proposed new tools, higher-risk use cases, pilots, automation at scale, or Trust-wide deployments should be directed into the Trust's AI governance and implementation route described in the policy.

8. Indicators of success

- Increased staff confidence in using approved AI appropriately and safely.
- Improved consistency in the use of approved tools and key guardrails.

- Earlier identification and escalation of higher-risk proposals, incidents or non-compliant use.
- Better feedback to central teams on barriers, opportunities, training needs and practical improvements.
- A visible local network of staff who can help embed responsible, proportionate and productive use of AI over time.

9. Review

This supporting document should be reviewed alongside the main AI Policy and updated as the Trust's governance arrangements, approved tools, training offer and local support model develop.