

Artificial Intelligence (AI) Governance Policy

Version No.2 : August 2025

First Issued: July 2024
Review date: August 2026

Contents

(For quick access to a specific heading - **press CTRL and click your mouse** to follow the link for the below options)

1.	INTRODUCTION.....	3
2.	PURPOSE	3
3.	SCOPE	3
4.	DEFINITIONS	4
5.	RESPONSIBILITIES.....	6
6.	POLICY STATEMENT.....	8
7.	PROCEDURE.....	8
8.	MONITORING AND REVIEW	12
9.	REFERENCES.....	13
10.	ASSOCIATED POLICIES & PROCEDURES <i>(To include but not limited to)</i>	13
11.	AUTHOR	13
12.	APPENDICES.....	13
13.	EQUALITY & DIVERSITY IMPACT ASSESSMENT	15
14.	DOCUMENT CONTROL	16

1. INTRODUCTION

In the rapidly evolving field of healthcare, the integration of artificial intelligence (AI) technologies has the potential to revolutionise patient care, streamline administrative processes, and enhance overall operational efficiency. East Coast Community Healthcare (ECCH) recognises the importance of adopting AI technologies while ensuring their ethical and responsible use. This AI policy serves as a guiding framework to ensure the appropriate deployment, management, and oversight of AI systems across ECCH.

2. PURPOSE

The purpose of this policy is to establish clear guidelines for the development, implementation, and monitoring of AI systems to protect personal data, uphold ethical standards, and mitigate potential risks. We recognise that AI systems, including machine learning algorithms and natural language processing, can contribute significantly to research, improving healthcare outcomes and resource allocation. However, it is imperative to ensure that AI technologies are used in a manner that aligns with legal requirements, respects patients' rights, and maintains the trust and confidence of our patients, staff, and stakeholders. This policy outlines key principles and procedures that must be adhered to when utilising AI technologies within ECCH. It addresses critical aspects such as data privacy, algorithm transparency, accountability, and ongoing monitoring of AI systems. By implementing these guidelines, we aim to foster a culture of responsible AI use, where the benefits of AI are harnessed while minimising potential risks.

It is important to note that this AI policy is not exhaustive and may need to be adapted and updated periodically as technology advances, regulatory requirements evolve, and best practices in AI governance emerge. ECCH are committed to staying at the forefront of responsible AI implementation to ensure the ethical and effective use of AI technologies.

3. SCOPE

The policy applies to ECCH and all its employees and must be followed by all those who work for the organisation, including those on temporary or honorary contracts or secondment. It applies to all departments and services that utilise AI irrespective of their scale or scope. It applies to both internally developed AI systems and those procured from external vendors.

Non-compliance with this policy will result in disciplinary action which may include dismissal.

4. DEFINITIONS

The following definitions are intended to provide a brief explanation of the various terms used within this policy.

Term	Definition
Artificial Intelligence (AI) and Generative Artificial Intelligence	The theory and development of computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages. For example: a language translator will, when using AI, produce an output which is naturally spoken or written and indistinguishable from someone who speaks it as a first language. Generative AI is a subset of AI referring to an intelligent machine that can learn from inputted data or its knowledge and by looking for apparent commonalities in the data produces new linked or completely unique information or data.
Data Protection Impact Assessments -	A Data Protection Impact Assessment (DPIA) is a process to help identify and minimise the data protection risks of a project. ECCH requires that DPIAs are considered and where necessary completed in full for any new data processing activities, new systems, services, and commissioning activities. The Quality Impact Assessment Group will review and approve DPIAs and advise of requirements and recommended actions as necessary.
Digital Technology Assessment Criteria (DTAC) -	Developed by the NHS, the DTAC is an assessment criterion required for the commissioning of digital health technologies across the NHS and social care services. The DTAC includes criteria covering clinical safety, data protection, technical security, interoperability, plus usability and accessibility. For your digital health product to pass the DTAC, you need to

	meet all requirements in each of the areas.
Machine Learning –	is a sub-field of AI. It is the use and development of computer systems that are able to learn and adapt without following explicit instructions, by using algorithms and statistical models to analyse and draw inferences from patterns in data. Machine learning algorithms are trained on data sets to create models that enable machines to perform tasks that would otherwise only be possible for humans. These tasks include categorizing images, analysing data, predicting price fluctuations etc.
Natural Language Processing –	refers to the branch of computer science/ AI concerned with giving computers the ability to understand text and spoken words in much the same way human beings can.
Processing -	in relation to information or data means; obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, which may include adaptation or alteration of the information; retrieval, or use of the information or data; disclosure of the information or data by transmission, dissemination or otherwise making available, or alignment, combination, blocking, erasure or destruction of the information or data. In summary anything you do with data is “processing”.
Robotic Process Automation (RPA)	- is a form of business process automation that uses automation technologies to mimic back-office tasks of human workers, such as extracting data, filling in forms, moving files, etc. By deploying scripts that emulate human processes, RPA tools autonomously execute various activities and transactions across unrelated software systems. This form of automation uses rule-based software to

	<p>perform business process activities at a high volume, freeing up human resources to prioritize more complex tasks. While RPA is sometimes mistaken for artificial intelligence (AI), the two are distinctly different, RPA is process driven, whereas AI is data driven. RPA bots can only follow the processes defined by an end user, while AI bots use machine learning to recognise patterns in data and learn over time, RPA and AI can complement each other well.</p>
--	---

5. RESPONSIBILITIES

- **Chief Executive of ECCH** – Overall responsibility for the enforcement of this policy lies with the Chief Executive of ECCH
- **Data Protection Officer (DPO):**
 - Oversee and ensure compliance with data protection regulations and best practice associated with AI.
 - Provide guidance on data privacy related to AI systems.
 - Coordinate the review & approval of Data Protection Impact Assessments (DPIAs) for AI projects via the Quality Impact Assessment (QIA) Group.
 - Serve as the point of contact for data subjects and supervisory authorities regarding data protection concerns related to AI.
- **Associate Director ICT & Digital Health:**
 - Review and approve Data Protection Impact Assessments for all AI projects via the QIA Group.
 - Serve as a point of contact for staff with queries or concerns relating to AI.
 - Provide guidance relating to data protection and AI.
 - Ensure the implementation of AI is in line with data protection legislation.
- **Caldicott Guardian (CG):**
 - Ensure data is processed in accordance with the Caldicott Principles
 - Ensure confidential patient information is processed legally, ethically and appropriately.
 - Provide advice and guidance to staff on the implementation of AI.
- **Senior Information Risk Owner (SIRO):**

- Take responsibility for the overall governance and management of information risks associated with AI systems.
 - Ensure that appropriate risk management processes, controls, and policies are in place.
 - Collaborate with other stakeholders to address potential risks and mitigate any adverse impacts arising from AI implementation.
 - Provide oversight and strategic direction to ensure the responsible use of AI technologies.
- **Clinical Safety Officer:**
 - Assess the safety risks associated with AI systems used in clinical settings.
 - Collaborate with relevant stakeholders to establish safety protocols and guidelines for AI implementation.
 - Monitor and evaluate the performance and safety of AI systems.
 - Investigate and address any incidents or concerns related to the clinical safety of AI systems.
- **IT /Technical & Business Intelligence Staff:**
 - Assist in the implementation, integration, and maintenance of AI systems.
 - Ensure the proper configuration, security, and compatibility of AI systems with existing IT infrastructure.
 - Collaborate with vendors and other stakeholders to address technical issues and provide technical support for AI systems as required.
- **Transformation, Finance & Procurement Teams**
 - Finance & Procurement Teams have an obligation to make the Associate Director ICT & Digital Health: aware of any requests to implement AI software.
 - Requests for AI solutions will be assessed and authorised by the Information Governance and IT Teams. A Data Protection Impact Assessment **MUST** be completed prior to implementation; this is a legal requirement for AI.
- **Research and Development Team within the Innovation, Research and Improvement System (IRIS):**
 - Assist researchers by signposting them to the correct Health Research Authority (HRA) guidance and advising them on how to apply for ethics approval.

- **End-Users:**
 - Utilise AI systems in accordance with established guidelines and protocols.
 - Provide feedback and insights on the effectiveness, usability, and impact of AI technologies.
 - Report any incidents or concerns related to AI system performance or safety.
- **Employees & Authorised users:**
 - Familiarise themselves with and adhere to ECCH's Information Governance & Security policies, protocols and guidelines.
 - Report any concerns or issues related to the AI systems to the ICT helpdesk.

It is important to note that these roles and responsibilities may vary, collaboration and clear communication among these roles are essential for the successful and responsible use of AI.

6. **POLICY STATEMENT**

ECCH is committed to the use of technology to support organisational function and to make efficiency savings but only where the risk can be controlled or mitigated effectively.

7. **PROCEDURE**

Defining the purpose and identifying a legal basis for the use of AI:

Generative artificial intelligence can be used in many ways to enhance the work of ECCH.

It is important that the purpose and use of AI is clearly defined and agreed, including why AI is being used and what value it will bring to the organisation. You must also determine if a legal basis for the use of data is required before any data is processed. Where possible any data should be anonymous so a legal basis would not be required. However, it is important that data and use cases are carefully assessed to determine if individuals can be identified using the contents of the information even if common identifiers such as name, address and phone number are removed. The combined details of a local area, a rare disease and a very young age may enable a patient to be identified. In such cases you would need to treat this as personal data and therefore identify a legal basis for the processing along with meeting the requirements of the common law duty of confidentiality.

The above requirements also apply to data used to test and develop AI systems even if there is no outcome or decision for an individual, this is because you are processing data by using it to train AI models or algorithms.

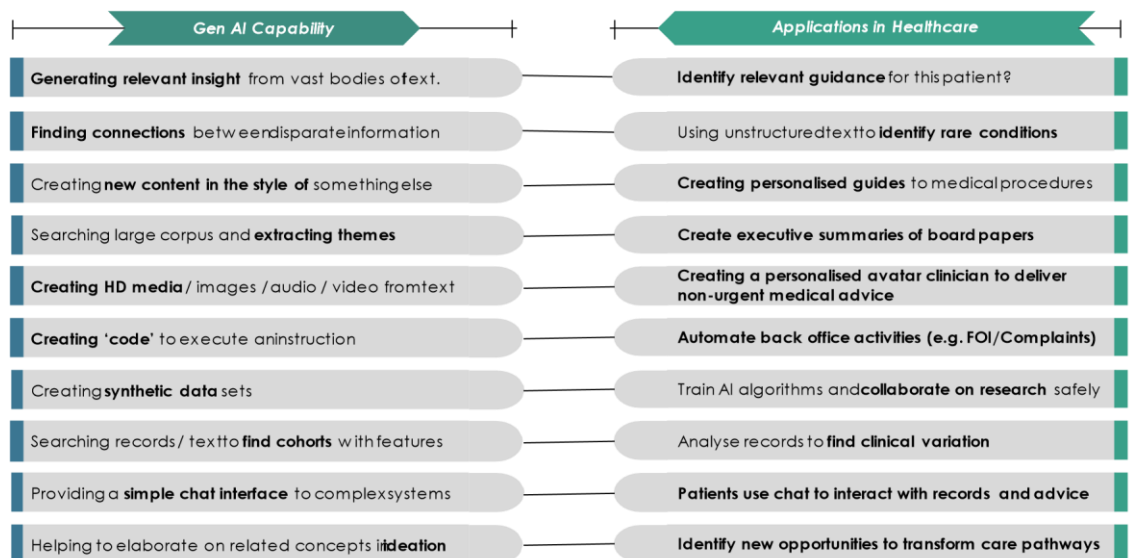
In general, AI can be used in healthcare in three ways:

- AI specifically for use in healthcare settings,
- AI for population or health research,
- Freely or commercially available 'generic' AI.

How these should be used in health and care settings is outlined below.

Developing Artificial Intelligence Products for Healthcare

The NHS's AI and Digital Regulations Service is an AI regulation service for people who develop or plan to use AI or a digital technology in health and social care. It brings together regulations, guidance and resources for digital healthcare technologies. The service is comprised of four partners; National Institute for Health & Care Excellence (NICE), Medicines and Healthcare products Regulatory Service (MHRA), Health Research Authority (HRA) and Care Quality Commission (CQC). You can contact this service at: [About the AI and Digital Regulations Service - AI regulation service - NHS \(innovation.nhs.uk\)](https://innovation.nhs.uk)



Agilisys • DATA & DECISION

Using AI for Research

Health Research Authority (HRA) approval is required for research studies that take place in the NHS in England. The 'HRA AI and Digital Regulations Service' can provide guidance for NHS AI adopters, and digital health innovators.

Review by an NHS Research Ethics Committee (REC) is required, as well as an assessment of regulatory compliance and related matters undertaken by dedicated HRA staff.

If you are planning to develop an AI research programme within the NHS, the Research and Development Support Services team within the Innovation, Research and Improvement System (IRIS) will be able to provide advice and guidance on how to apply for research ethics and approvals via the Health Research Authority.

Freely Available Artificial Intelligence Apps and Services

AI is a feature of many applications currently used by staff including Apps within MS Teams. It is important to use AI appropriately and responsibly to ensure that it does not compromise personal data, business sensitive information, violate policies, or pose a risk to patient safety or our network integrity. ECCH recommends caution when using freely available AI software such as Chat GPT. Although it can be used in the same way you might use different sources to kickstart a research project or better understand what people are saying about a topic, it should not be used as your primary source for information because it can produce inaccurate, biased or false information.

The UK's National Cyber Security Council (NCSC) states that you should not enter sensitive information (such as personal details or company intellectual property) into chatbots, and not to perform queries that could be problematic if made public (for example sharing your secrets and asking ChatGPT to solve a personal dilemma).

If using publicly available AI then you must follow the following basic rules:

- No personal data should be used in these apps or services.
- No business sensitive data should be used in these apps or services.
- These apps must only be used for non-clinical purposes.
- You must inform the Information Governance team where you intend to use these services for routine working.
- You must be aware of any copyright and intellectual property considerations when using generative AI.
- Users should be aware of any potential ethical considerations when using these products. Including the potential to propagate biased, discriminatory, or harmful content.
- Be aware that you will need to verify any output of these products to ensure accuracy.
- AI software used for work purposes should only be accessed via corporate devices.
- As per the ICT Policy you must not install any software without explicit permission from IT. Additionally downloading commercial software is not permitted without a license, in this case please refer to procuring AI products.

When procuring and implementing artificial intelligence products or systems that include AI features you must:

- Engage with the organisational transformation and procurement processes and associated governance.
- Engage with the Data Protection Officer, IT/ Technical & Business Intelligence Teams.
- You are **legally required** to complete a Data Protection Impact Assessment (DPIA), the service area and the supplier must engage with this process. DPIA's must be undertaken via QUEST within the Project Module – Assessments - DPIA [Create](#). ECCH's DPIA contains a set of specific AI questions which must be answered for the DPIA to be approved as shown at [appendix 1](#).
- You must consider the risks and practical steps to reduce these risks that are documented in the ICO's AI Toolkit [AI and data protection risk toolkit | ICO](#)
- If the AI is associated with healthcare provision (such as image reading) a Digital Technology Assessment Criteria must be completed.
- As part of the DPIA and DTAC processes any associated biases or ethical concerns must be documented and addressed; potential societal impact and ethical implications of AI deployments should be carefully assessed and mitigated.
- If the AI is associated with research, you must obtain approval from the Health Research Authority (HRA).
- The Clinical Safety Officer and the Medical Device Safety Officer - MDSO (if developing a medical device) must be consulted throughout procurement and implementation. If you require an MDSO this role will be sourced from an external organisation.
- You must adhere to the conditions set out in [Article 22](#) of the UK General Data Protection Regulation in relation to automated individual decision making, including profiling. – Individuals have the right not to be subject to automated decision making.
- **ALL AI outcomes or outputs must be reviewed by a human. You cannot rely solely on the use of AI for decision making, there must be substantial involvement from an appropriately qualified human.**
- There must be an agreed process to flag any concerns regarding the output of any AI products.
- If there are concerns which have led to an incident this must be reported as per the Incident Reporting Policy.
- Incident response plans should be established to handle security incidents, including data breaches, unauthorised access, and system failures.
- Use of AI must be transparent to staff and patients ensuring they understand where it is being used and how it may impact their employment, work or care. The logic behind it must be explainable.

- Data must be collected and processed in a lawful and ethical manner, with appropriate consent and anonymisation measures in place.
- Data access and sharing must be strictly controlled, and data must be stored securely throughout its lifecycle.
- You should conduct patient and public engagement activities that include determining if individuals support the use of data for your intended purpose, or if they have any concerns on how their data will be used.
- If the use of AI involves service change, then prior to the implementation of any AI programme, formal consultation must take place with employees and their trade union representatives in accordance with the organisational change policy.
- You must be assured that any product mitigates against bias and discrimination.
- AI systems should be continuously monitored for suspicious activities, anomalies, and potential security breaches.

7 Consultation

All stakeholders such as ECCH's SIRO/DPO, Executive lead and IT Lead, Research & Development Team, transformation, Business Intelligence and IT involved in developing, implementing, managing, and monitoring artificial intelligence have been engaged in the development of this policy.

8 Training

Staff involved in the implementation of AI will require training. This will be addressed as and when required with the level of training dependent on the level of involvement.

Additionally, staff will be reminded of the governance implications of using AI via staff briefings, newsletters etc.

8. MONITORING AND REVIEW

Adherence to this policy will be monitored through staff awareness and completion of data protection impact assessments, spot-checks and audits. This will be monitored by the ECCH Information Governance Team.

This policy will be reviewed every year. Earlier review may be required in response to exceptional circumstances, organisational change, or relevant changes in legislation/guidance.

The policy will be disseminated by being made available on the ECCHO intranet and highlighted to staff through staff communications, and by managers.

Breaches of this policy may be investigated and may result in the matter being treated as a disciplinary offence under ECCH's disciplinary procedure.

9. REFERENCES

- Information Commissioner's Office – Artificial Intelligence Toolkit and associated documentation
- Gartner Workshop – Create a robust AI strategy
- NHS England
- Health Research Authority
- GOV.UK Understanding Artificial Intelligence Ethics & Safety
- UK General Data Protection Regulation
- Data Protection Act 2018
- The Common Law Duty of Confidentiality
- Privacy and Electronic Communications Regulations
- Confidentiality: NHS Code of Practice (Department of Health)
- Human Rights Act 2000
- Caldicott Principles

10. ASSOCIATED POLICIES & PROCEDURES *(To include but not limited to)*

- IT Security Policy
- Data Protection Impact Assessment Procedure
- Subject Access Request Policy
- Information Governance Policy & Staff Handbook
- Confidentiality Policy
- Disciplinary Policy

11. AUTHOR

Head of Corporate Governance and Risk Management / Data Protection Officer -
August 2025

12. APPENDICES

Appendix 1 – Data Protection Impact Assessment -AI Questions

Link to QUEST DPIA form –

<https://ecch.inphase.com/Questionnaire/Create?name=DPIA&m=46>

DPIA

New



What is a DPIA?

ICO definition – 'A DPIA is a process designed to help you systematically analyse, identify, and minimise the data protection risks of a project or plan. It is a key part of your accountability obligations under the UK GDPR, and when done properly helps you assess and demonstrate ho

Show more

Title

Title *

Title

AI

Does this project involve AI? *

Yes

No

Artificial intelligence (AI) is technology that enables computers and machines to simulate human learning, comprehension, problem solving, decision making, creativity and autonomy.

Fairness -Please detail what measures you have taken to ensure that there is equitable treatment of groups or individuals. ? *

Fairness -Please detail what measures you have taken to ensure that there is equitable treatment of groups or individuals.

Robustness - Please detail how the AI process has been reviewed or tested for "Robustness" against the following:
Malicious input: Errors or abnormal input:

Robustness - Please detail how the AI process has been reviewed or tested for "Robustness" against the following: Malicious input: Errors or abnormal input: Availability of the service:

Explainability - Please detail the objective of the AI process and how it is processing information to come to a conclusion in language an individual without technical knowledge can comprehend. *

Explainability - Please detail the objective of the AI process and how it is processing information to come to a conclusion in language an individual without technical knowledge can comprehend.

Transparency - Please detail what information the process is collecting, how and where it is stored, and who has access to the data. ? *

Transparency - Please detail what information the process is collecting, how and where it is stored, and who has access to the data.

Privacy Please - Please detail what privacy protections have been implemented in this AI use case. This might include data minimisation, anonymisation or pseudofiction. *

Privacy Please - Please detail what privacy protections have been implemented in this AI use case. This might include data minimisation, anonymisation or pseudofiction.

13. EQUALITY & DIVERSITY IMPACT ASSESSMENT

In reviewing this policy, the Policy Group considered, as a minimum, the following questions:

- ☐ Are the aims of this policy clear?
- ☐ Are responsibilities clearly identified?
- ☐ Has the policy been reviewed to ascertain any potential discrimination?
- ☐ Are there any specific groups impacted upon?
- ☐ Is this impact positive or negative?
- ☐ Could any impact constitute unlawful discrimination?
- ☐ Are communication proposals adequate?
- ☐ Does training need to be given? If so is this planned?

Adverse impact has been considered for age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion and belief, sex, sexual orientation.

Blank version of the full Equality & Diversity Impact assessment can be found here:

http://eccho/Home/FormsGuidance.aspx?udt_575_param_index=E&udt_575_param_page=2

14. DOCUMENT CONTROL

Version Date	Version No.	Author/ Reviewer	Comments
June 2025	2	Head of Corporate Governance and Risk Management	Details of the QIA Group for DPIA approval. Additional associated policies added. Further DPIA on QUEST details clarified and included appendix 1 to demonstrate DPIA AI questions and included a link direct to the form.

DOCUMENT CONTROL SHEET

Name of Document:	Artificial Intelligence (AI) Governance Policy
Version:	2
File Location / Document Name:	ECCHO
Date Of This Version:	August 2025
Produced By (Designation):	Head of Corporate Governance and Risk Management
Reviewed By:	(appropriate groups/virtually etc)
Synopsis And Outcomes Of Consultation Undertaken:	Changes relating to relevant committees/groups involved in ratification processes.
Synopsis And Outcomes Of Equality and Diversity Impact Assessment:	N/A
Ratified By (Committee): -	IG & Caldicott
Date Ratified:	14/08/2025
Distribute To:	ECCHO
Date Due For Review:	August 2026
Enquiries To:	Head of Corporate Governance and Risk Management

Approved by Appropriate Group/Committee	<input type="checkbox"/> Date: 14/08/2025
--	--