Ymddiriedolaeth GIG Prifysgol Felindre
Velindre University NHS Trust

Ref: (IG 16)

ARTIFICIAL INTELLIGENCE (AI) GOVERNANCE POLICY

Executive Sponsor & Function:	Executive Director of Finance
Document Author:	Head of Information Governance
Approved by:	Quality, Safety and Performance Committee
Approval Date:	12th March 2026
Date of Equality Impact Assessment:	15th January 2026
Equality Impact Assessment Outcome:	Approved
Review Date:	March 2027
Version:	1

Contents **Page**

1. INTRODUCTION

In the rapidly evolving field of healthcare, the integration of artificial intelligence (AI) technologies has the potential to revolutionise services, streamline administrative processes, and enhance overall operational efficiency. Velindre University NHS Trust (the Trust) recognises the importance of adopting AI technologies while ensuring their lawful, ethical and responsible use.

The Welsh Government commissioned a survey to "*assess the effective adoption of AI across NHS Wales*" this Policy is one result of output recommended by the Survey, which includes the following:

- The adoption of a national AI strategy across NHS Wales to include principles, vision and risk appetite
- A national AI governance Policy
- A national AI ethics framework

The three outputs above would in due course be endorsed by the Welsh Government to assist NHS bodies in their journey.

The Information Governance landscape in Health and Social Care in Wales is under review with the imminent establishment of a new Welsh Government led Strategic IG Group to sit under the Digital, Data and Technologies (DDaT) (Standards) Board, the Group will be strategic in focus and will endorse all-Wales policies such as a National AI Policy.

In the interim, whilst the governance arrangements of the new Strategic IG Group are being set up, and in order to facilitate good governance and mitigate risk it is vital that the Trust has in place an AI Policy pending a future all-Wales AI Policy. This AI policy serves as a guiding framework to ensure the appropriate deployment, management, and oversight of AI systems across the Trust.

2. POLICY STATEMENT

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. The Trust recognises 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', service users, donors' and staff rights, and maintains the trust and confidence of our patients, donors, staff, and stakeholders.

This policy outlines key principles and procedures that must be adhered to when utilising AI technologies within the Trust. It addresses critical aspects such as data privacy, algorithm transparency, accountability, and ongoing monitoring of AI systems. By implementing these guidelines, the aim is to foster a culture of responsible and ethical AI use, where the benefits of AI are harnessed while minimising risks and misuse.

It is important to note that this AI policy is not exhaustive and will be adapted and updated periodically as technology advances, regulatory requirements evolve, and best practices

in AI governance emerge. The Trust is committed to staying at the forefront of responsible AI implementation to ensure the ethical and effective use of AI technologies.

3. SCOPE OF POLICY

All staff are required to comply with this policy. The term "staff" includes permanent, temporary, contracted and voluntary staff of the Trust, including Independent Members and those with honorary contracts who have access to and create officially recorded information. 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 could result in disciplinary action which may include dismissal.

4. AIMS AND OBJECTIVES

The aims and objectives of this policy are to ensure that there is guidance available for staff on the development, implementation, and monitoring of AI systems to protect personal and commercially sensitive data, uphold ethical standards, and mitigate potential risks whilst enabling staff and services to improve from new technologies.

5. RESPONSIBILITIES

In order that the deployment and use of AI meet legal and ethical standards, individuals in existing posts are required to provide technical and practical advice and guidance prior to and during the use of products and services using AI:

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.
- Review and approve Data Protection Impact Assessments (DPIAs) for all AI projects (including those who may have an element of AI as part of their objectives).
- Act as the AI Officer as set out in Section 4(1) of the AI (Regulation) Bill and in the Subsequent AI (Regulation) Act when it receives Royal Assent.
- Act as a member of the virtual panel assessing the use of AI tools within the Trust

Caldicott Guardian (CG):

- Ensure data is processed in accordance with the Caldicott Principles.
- Ensure confidential patient and donor information is processed legally, ethically and appropriately.
- Provide advice and guidance to staff on the implementation of AI in relation to clinical systems.

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.
- Act as a member of the virtual panel assessing the use of AI tools within the Trust,

Chief Clinical Information Officers:

- Assess the clinical safety risks associated with AI systems used in clinical settings.
- Collaborate with and support the Caldicott Guardian in their role of safeguarding the confidentiality of patient information.
- Collaborate with relevant stakeholders to establish safety protocols and guidelines for AI implementation.
- Monitor and evaluate the performance and safety of AI systems used in clinical settings.
- Investigate and address any incidents or concerns related to the clinical safety of AI systems.
- Act as a member of the virtual panel assessing the use of AI tools within the Trust.

Chief Digital Officer:

- Monitor the deployment and use of AI systems across the Trust.
- Ensure data is processed in accordance with Legislation with regards to Cyber security and resilience.
- Provide the ability to monitor the employment and use of AI Systems across the Trust
- Ensure information is processed securely.
- Provide advice and guidance to staff on the implementation of AI.

Digital & Data and Insights Staff:

- Assist in the implementation, integration, and maintenance of AI systems.
- Ensure the proper configuration, security, and compatibility of AI systems in line with all relevant policies.
- Collaborate with vendors and other stakeholders to address technical issues and provide technical support for AI systems as required.

Finance & Procurement Teams:

- Finance and Procurement Teams have an obligation to make the Information Governance Team aware of any requests to implement AI software.
- Requests for AI solutions will be assessed and authorised by the Information Governance and digital Teams. A Data Protection Impact Assessment MUST be completed prior to implementation; this is a legal requirement for AI.

Research, Development and Innovation (RD&I)

- Assist researchers by signposting them to the correct Health Research Authority (HRA) guidance and advising them on how to apply for ethics approval.

- Refer to Good Machine Learning Practice (GMLP) and 10 guiding principles as developed by the US Food and Drug Agency (FDA), Medicines and Healthcare Products Regulatory Agency (MHRA) and Health Canada.

Employees & Authorised Users:

- Develop and Utilise AI systems in accordance with established guidelines and protocols.
- Utilise AI technology in accordance with established professional standards (e.g. GPhC Standards)
- 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.
- Familiarise themselves with and adhere to the Trust's Information Governance and Security policies, protocols and guidelines.
- Report any concerns or issues related to the AI systems to the DPO.

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. DEFINITIONS

The following definitions are useful when describing AI and subsets of AI:

Artificial Intelligence:

The development of computer systems capable of performing tasks that typically require human intelligence, such as reasoning, learning, decision-making and perception. AI encompasses a wide range of technologies, including machine learning, deep learning and natural language processing

Machine Learning:

Machine learning is the subset of artificial intelligence (AI) focused on algorithms that can "learn" the patterns of training data and, subsequently, make accurate *inferences* about new data. This pattern recognition ability enables machine learning models to make decisions or predictions without explicit, hard-coded instructions.

Deep Learning:

Deep learning is a subset of machine learning driven by multilayered neural networks whose design is inspired by the structure of the human brain.

Natural Language Processing:

Natural language processing (NLP) is a subfield of computer science and artificial intelligence (AI) that uses machine learning to enable computers to understand and communicate with human language.

Generative AI

Generative AI, sometimes called *gen AI,* is artificial intelligence (AI) that can create original content such as text, images, video, audio or software code in response to a user's prompt or request.

Agentic AI:

Agentic AI is an artificial intelligence system that can accomplish a specific goal with limited supervision. It consists of AI agents—machine learning models that mimic human decision-making to solve problems in real time. In a multiagent system, each agent performs a specific subtask required to reach the goal and their efforts are coordinated through AI orchestration.

AI Systems – An AI System is defined as a machine based system that can infer outputs from inputs to generate predictions, content, recommendations or decisions. It operates independently, processing data and detecting patterns, and learns from new data to adjust its outputs. These systems are capable of performing tasks that typically require human intelligence, such as reasoning, learning and perception. Additionally, AI systems can be developed in software or hardware to solves tasks requiring human like cognition and communication. They operate autonomously and adapt after deployment.

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 utilising Data Protection by Design and by Default. The Trust requires that DPIAs are considered and where necessary completed in full for any new data processing activities, new systems, services, and commissioning activities. The Information Governance (IG) Team will review and approve DPIAs and advise of requirements and recommended actions as necessary.

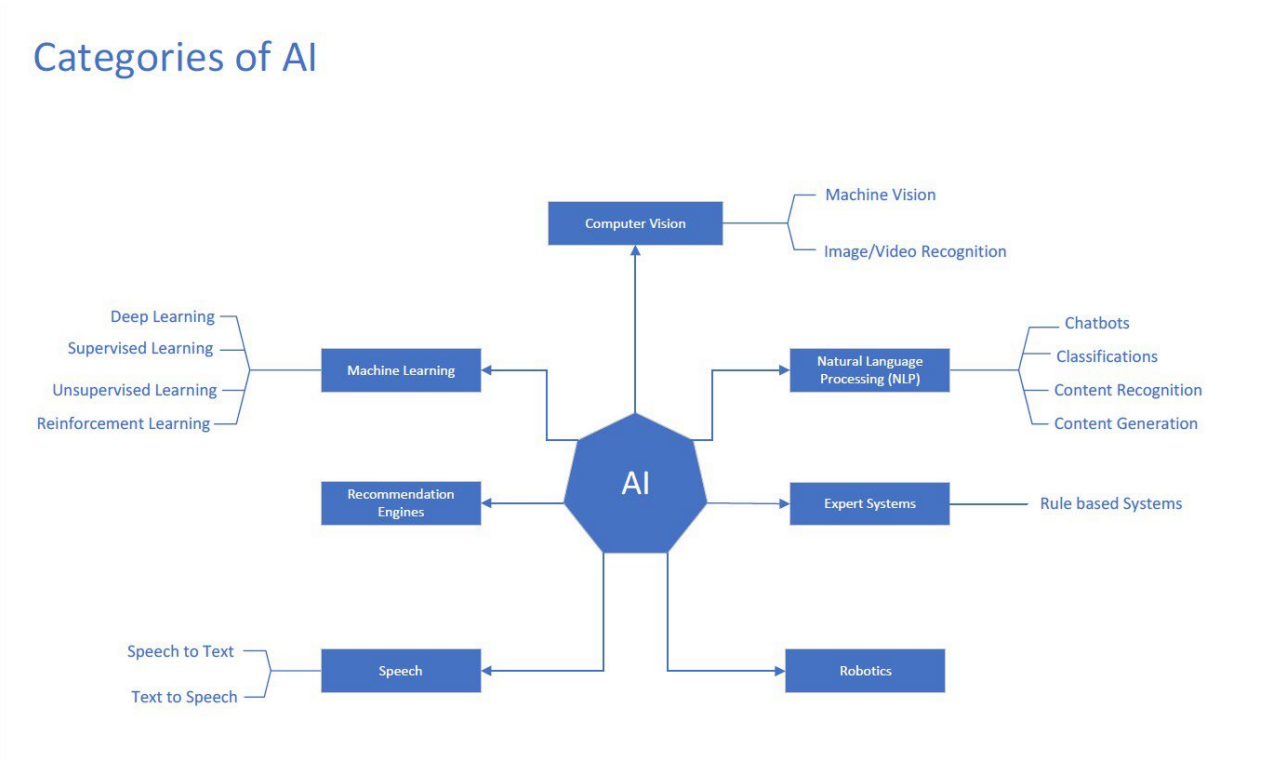
Digital Technology Assessment Criteria (DTAC) – Developed by the NHS in England, the DTAC is an assessment criterion required for the commissioning of digital health technologies across the NHS and social care services. The DTAC includes criteria covering clinical safety, data protection, technical security, 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.

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 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.

The Schematic below sets out the interconnected relationship of differing sub-categories of AI and where AI fits in the domain of data science:



Sensitive Data – Any personal data that is defined as sensitive under the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018, including but not limited to:

- Patient identifiable data (e.g., names, dates of birth, addresses).
- Medical records and health information.
- Financial and payment information.
- Any other information that is deemed sensitive by NHS Wales organisations.

Personal data is defined in UK GDPR Article 4(1) as:

> "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*";

Special Category Personal Data is defined in UK GDPR Article 9(1) as:

> "*data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*"

7. IMPLEMENTATION/POLICY COMPLIANCE

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

Artificial Intelligence can be used in many ways to enhance the work of the Trust. 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. Such purpose and use must be set out formally within the DPIA process which is already set in law under Article 35 UK GDPR.

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. The definition of Anonymised data is:

> "*information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable*".

It is therefore, 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.

For example, 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 (see Art 6 UK GDPR) for the processing along with meeting the requirements of the common law duty of confidentiality (CLDC), to meet the requirements of CLDC there MUST be one of the following conditions:

- *A mandatory legal requirement or power that enables the CLDC to be set aside, for example, the Children Act 1989 which requires information to be shared in safeguarding cases, powers for Care Quality Commission inspections, reporting of food poisoning, reporting of infectious diseases such as measles, and the powers given to NHS Digital under section 259 of the Health and Social Care Act 2012.*
- *A court order, where a judge has ordered that specific and relevant information must be provided, and to whom.*
- *An overriding public interest, where it is judged that the benefit of providing the information outweighs the rights to privacy for the patient concerned and the public good of maintaining trust in the confidentiality of the service.*
- *Explicit or implied consent.*
- *Legal support for the use of confidential patient information without consent under the Health Services (Control of Patient Information) Regulations 2002, under section 251 of the NHS Act 2006.*

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:

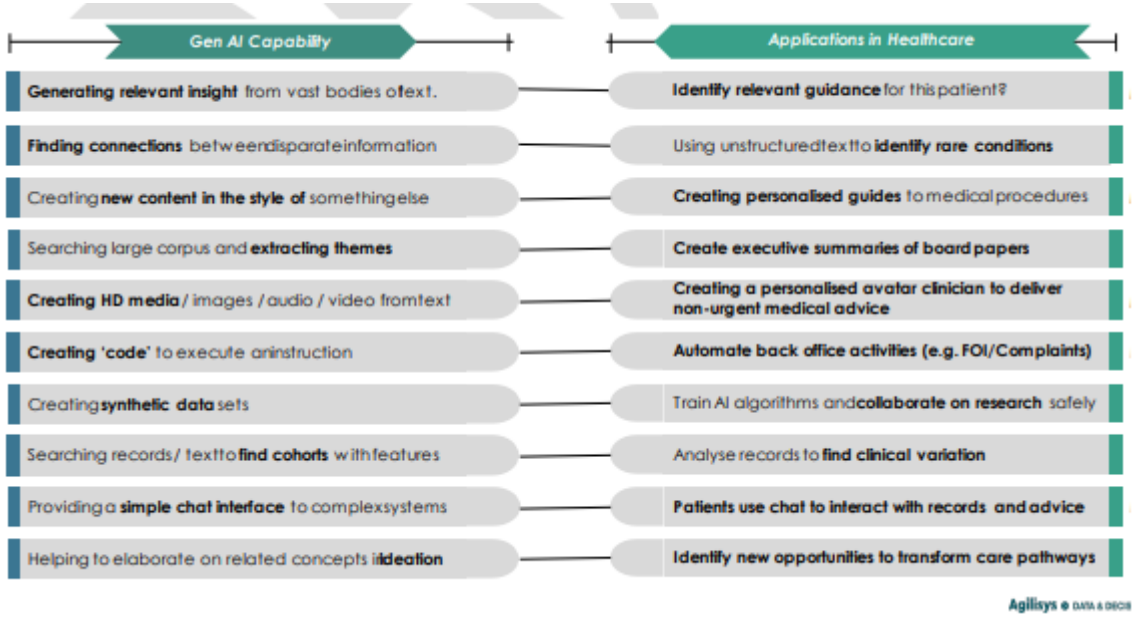
- AI specifically for use in healthcare settings,
- AI for population or health research,
- Freely or commercially available 'generic' AI.

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) {English version of Health Inspectorate Wales}. You can contact this service at:

About the AI and Digital Regulations Service – AI regulation service – NHS (innovation.nhs.uk)



Using AI for Research

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

https://www.digitalregulations.innovation.nhs.uk/

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.

In addition, a useful resource is the UK Government's "*pro-innovation approach to AI*" the link is below:

Pro-Innovation Approach to AI PDF

Public and freely Available Web facing Artificial Intelligence Apps and Services (e.g. Copilot, ChatGPT)

AI is a feature of many applications currently used by staff including Apps within M365 ecosystem. 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 or donor safety, or our network integrity. The Trust **DOES NOT** permit the use of public AI software such as ChatGPT. This is because it can produce inaccurate, biased or false information, it can also be accessed by people outside the NHS and there is a risk that sensitive information may inadvertently become available in the public domain, this would constitute a data breach.

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

- Engage with the procurement process set out within the Procurement policy.
- Engage via Service Desk
- complete a Data Protection Impact Assessment (DPIA), the service area and the supplier must engage with this process – this is required by law.
- 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 Services Technology Assessment Criteria form and an AI assessment form must be completed.
- As part of the AI assessment form submission any associated biases or ethical concerns must be documented and addressed within the AI Ethics Impact Assessment; potential societal impact and ethical implications of AI deployments should be carefully assessed and mitigated. It is essential that the Trust can be assured that any product mitigates against bias and discrimination.
- If the AI is associated with research, you must obtain approval from Trust's RD&I Team.
- The Chief Clinical Information Officer (if developing a medical device) must be consulted throughout procurement and implementation.
- Welsh Health Circular (WHC) 26/2025 must be consulted when procuring Ambient Voice Technology tools as they are classed as Medical Devices, a DPIA MUST also be completed in compliance with data protection by design and by default.

- 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.
- 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, this requirement will normally be completed by the Clinical Safety process and completion of a DCB0160.
- 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/donors 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.
- When undertaking Research Development and Innovation (RD&I) activities, 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.
- AI systems should be continuously monitored for suspicious activities, anomalies, and potential security breaches in line with stipulations set by the Trust's cyber security team

Copyright Considerations

Velindre University NHS Trust employees using AI technologies must also consider the Copyright and Patents Act 1988 when entering data into these systems, it is important that any information being used or input into an AI tool has the copyright holders permission to do so.

8. EQUALITY IMPACT ASSESSMENT STATEMENT

An EQIA has been completed and its summary is presented at the front of this Policy.

9. REFERENCES

All stakeholders such as the Trust's SIRO/DPO, Executive lead and IG lead, Research, Development and Innovation Team, Procurement Team, Data and Insights and Digital involved in developing, implementing, managing, and monitoring artificial intelligence have been engaged in the development of this policy.

The following References may be useful tools to further understanding of the use of AI:

- Information Commissioner's Office – Artificial Intelligence Toolkit and associated documentation.
- Gartner Workshop – Create a robust AI strategy.
- Governance Mapping for the Effective Adoption of AI across NHS Wales.
- UK Health Research Authority
- GOV.UK - Understanding Artificial Intelligence Ethics & Safety.
- The (retained) EU GDPR 679/2016 (UK General Data Protection Regulations).
- Data Protection Act 2018.
- The Common Law Duty of Confidentiality (CLDC).
- Privacy and Electronic Communications Regulations.
- Confidentiality: NHS Code of Practice (Department of Health).
- Human Rights Act 2000
- Welsh Health Circular 26/2025 – Ambient Voice Technology.
- Caldicott Principles.

10. GETTING HELP

Staff that require assistance should contact the DPO and/or the Chief Digital Officer or a member of their team in the first instance.

11. RELATED POLICIES

- Information Governance Policies.
- Information Security & Supplier Management Policies.
- Data Protection Impact Assessment Procedure.
- Incident Response Plan.
- Information Governance Policy.
- Data Quality Policy.
- Information Security Policy.
- Internet Use Policy.
- Email and Instant Messaging (EIM) Use Policy.
- Safeguarding and Public Protection Policy

12. INFORMATION, INSTRUCTION AND TRAINING

Staff are required to undertake the Information Governance training as part of the statutory/mandatory training. However, staff involved in the implementation of AI will require additional training. This will be addressed as and when required with the level of training dependent on the level of involvement.

Access to Generative AI websites will only be made available to those who have undertaken training. This will be the responsibility of the Cyber Team to provide.

Monitoring Compliance

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 Trust's Information Governance & Cyber Security Teams.

REFERENCES – SPECIFIC APPLICABLE LEGISLATION AND STANDARDS

- UK General Data Protection Regulation
- Data Protection Act 2018
- The Common Law Duty of Confidentiality
- Human Rights Act 1998
- Public Records Act 1958
- Data (Use and Access) Act 2025
- AI Cyber Security Code of Practice