

Approval & Use of Artificial Intelligence (AI)

Policy

This document can only be considered current when viewed via the current document directories / systems. If this document is printed or saved to another location, you are advised to check that the version you use remains current and valid, with reference to the 'review due' date.

Version	2.0	Issue Date	13/11/2025	Next Review	13/11/2026
Author(s) Name(s) & Job Title(s)		Andy Mayne Chief Scientist for Data, Operational Research and Artificial Intelligence			
Owner Name(s) & Job Title(s)		David Shannon Director of Strategic Development			
Approved By		Data Security & Protection Group			
Approval date		13/11/2025			
Colleagues / Groups Consulted		AI Ethics Committee Data Security & Protection Group			

Contents

1	Introduction.....	3
2	What is Artificial Intelligence.....	3
3	Roles and Responsibilities	4
4	Scope	5
5	Equality & Inclusion	5
6	General Risks and Mitigations	6
6.1	Prevention of Bias and Discrimination.....	7
6.2	Responsibility & Liability.....	8
6.3	Misinformation	9
6.4	Surveillance.....	9
6.5	Cybersecurity.....	10
6.6	Copyright and Intellectual Property	11
6.7	Transparency.....	11
7	Specific Applications of AI	12
7.1	Communications and public facing media.....	12
7.1.1	Generating Creative Media.....	12
7.1.2	Preventing loss of Originality / Creativity / Quality	12
7.1.3	Referencing when AI has been used.....	12
7.1.4	Use of existing creative media.....	13
7.1.5	Editing media	13
7.2	Recruitment.....	13
7.2.7	Generative AI within Search Engines	14
7.3	Clinical Applications	16
7.4	Data Science, Analytics and Research.....	19
7.5	General	20
7.6	Third party applications	21
8	Legal regulations for AI.....	21
9	Restricted Practices	22
10	Procurement of products containing AI	23
11	References.....	24
12	Monitoring.....	26

1 Introduction

This policy outlines the operational guidelines to safely integrate Artificial Intelligence (AI) within Somerset NHS Foundation Trust. The implementation of AI has the potential to revolutionise patient care, optimise operational efficiency, and drive groundbreaking research. However, as with any innovative technology, this must be delivered with a balanced approach between fostering innovation and our ethical and legal responsibilities.

2 What is Artificial Intelligence

- 2.1 AI is the development of computer systems to mimic tasks that would normally require human levels of intelligence. Most commonly, these tasks use machine learning algorithms to recognise patterns, solve complex problems, understand natural languages, and make decisions. It can also refer to the use of robotics in automating tasks that would normally be performed by a human.

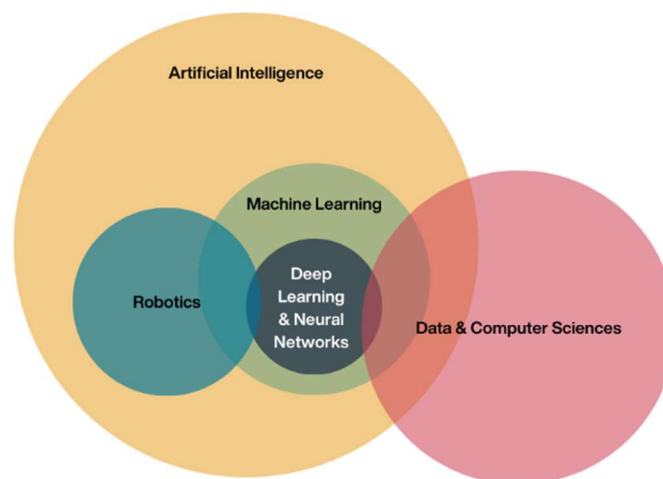


Fig. 1 – Interrelationships of AI terminology

- 2.2 There are three categories that AI models can be grouped into.

Narrow	General	Super
An AI model that specialises in one area and can solve one problem to the standard of a human.	An AI model that is considered as smart as a human across a broad range of tasks.	An AI model that is considered to surpass human intelligence in almost all tasks.

- 2.3 It is important to note that as of 2025, even the best and most complex AI models (Gemini, Grok, ChatGPT etc.) do not surpass narrow AI. However, we must ensure protections are in place for future developments.
- 2.4 AI can be further broken down by the learning methodology used on the training data.

Supervised	Unsupervised	Reinforcement
Where the model is told what the outputs should be	Where the model does not have defined outputs and is looking for patterns	Iteratively learn from mistakes to train model.
Examples Regression Classification Time Series Forecasting	Examples Anomaly Detection Clustering	Examples Playing games Learning to walk

- 2.5 For the purposes of this policy, AI is defined as software that utilise Machine Learning, Deep Learning, Robotics and Neural Networks. The study of these areas come under the umbrella of Computer, Decision and Data Sciences.

3 Roles and Responsibilities

- 3.1 It is the responsibility of the Data Science & Operational Research team to review this policy if concerns are raised, modern technologies emerge, legal guidance changes and to review and update it before it expires.
- 3.2 For advice and guidance on the safe and ethical use of Artificial Intelligence tools and models, colleagues should contact the Data Science & Operational Research Team on data.science@somersetft.nhs.uk
- 3.3 It is the responsibility of all colleagues at Somerset NHS Foundation Trust including those within its subsidiaries to follow this policy.
- 3.4 It is the responsibility of the Data Security and Protection Group to ensure the compliance with this policy and that any concerns raised by colleagues are reviewed and if required action upon.
- 3.5 It is the responsibility of the AI Ethical Committee to ensure that the use of AI at Somerset NHS Foundation Trust is ethical and used in the best interest of our patients and colleagues.
- 3.6 There are several ways that AI can be used, depending on whether you are using pre created tools, designing your own or if your data is used in the creation of a model. Therefore, within this policy, we will use the following terminology.
- Any user of a working Artificial Intelligence model. Within this policy they are defined as a **“User.”**
 - Somerset NHS Foundation Trust will be defined as either the **“Trust”** or **“Organisation.”**
 - Any Developer or Creator of an Artificial Intelligence model. Within this policy they are defined as a **“Creator or a Developer.”**
 - Any individual whose data is used in the training of an Artificial Intelligence model. Within this policy they are defined as a **“Person.”**
 - Any product or person that is not owned / employed by the Somerset NHS Foundation Trust is referred to as a **“Third Party Supplier.”**

4 Scope

- 4.1 The Scope of this Artificial Intelligence Policy covers all those employed at Somerset NHS Foundation Trust including subsidiary company employees and contractors, any processes using AI, any data for AI (input and output) and any technical systems using AI across all locations.
- 4.2 This policy also covers all applications of Artificial Intelligence across Somerset NHS Foundation Trust including software purchased or developed by the Trust that utilises AI as its primary or any secondary function.

5 Equality & Inclusion

5.1 Commitment to Equality and Inclusion

Somerset NHS Foundation Trust is committed to ensuring that the use of Artificial Intelligence (AI) in our organisation supports equality and inclusion for all individuals. This policy aims to prevent bias and discrimination in AI systems and to promote fairness and transparency in decision-making processes.

5.2 Fair Treatment and Discrimination

AI systems should be designed and implemented in a way that prevents unlawful discrimination based on protected characteristics as defined by the Equality Act 2010. These include age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, and sexual orientation.

5.3 Preventing Bias in AI

- 5.3.1 AI models used or designed by the organisation must be thoroughly tested to ensure they do not introduce or perpetuate bias against any group.
- 5.3.2 Developers and third-party suppliers are required to demonstrate that AI systems are designed using diverse data representative of the population of Somerset, including anyone who receives healthcare but does not reside in Somerset to minimise potential bias.

5.4 Accessibility and Fairness

- 5.4.1 All individuals must have equal access to the services and opportunities provided by AI systems. AI should not create barriers or restrict access based on discriminatory factors.
- 5.4.2 Automated decisions made by AI must be subject to human review unless the standards in 7.3.1 have been met, particularly when they may significantly affect an individual's rights, healthcare, or access to services.

5.5 Transparency and Accountability

- 5.5.1 Somerset NHS Foundation Trust is committed to ensuring transparency in the use of AI systems, and Information Asset Owners must ensure that the Public, Staff and Patients have suitable access to information explaining the models being used and the rationale.

- 5.5.2 Any concerns related to bias, fairness, or discrimination in AI must be reported to the Data Security and Protection Group for review and action.

5.6 Promoting Inclusivity in Development

- 5.6.1 Any AI systems developed at Somerset NHS Foundation Trust should accommodate and reflect the diversity of the communities we serve. Developers and Third parties should prioritise inclusivity in the training and testing phases to ensure equitable outcomes.

6 General Risks and Mitigations

General risks are those that are considered to apply to all forms of AI Trust wide and should be considered in all cases.

- 6.0.1 Any new AI process or system which uses personal data requires a Data Protection Impact Assessment (DPIA) and approval by the Trust's Data Protection Officer (DPO), Senior Information Risk Owner (SIRO) and IT/Cyber Security Lead.
- 6.0.2 All AI software, including web-based products, must be recorded on the information asset register and have a completed DPIA with approval from Information Governance, Cybersecurity, and the Data Science & Operational Research Team before use. A list of Pre-Approved AI software is available on the Artificial Intelligence intranet page.
- 6.0.3 Users should be aware that any AI system with the potential to cause harm to patients, for example (but not limited to): system failures, algorithmic flaws or misuse, must be compliant with the established framework of clinical risk management – DCB 0160 that was incorporated into English law in section 250 of the Health and Social Care Act 2012.
- 6.0.4 Information Asset Owners must ensure that their AI systems comply with the requirements in DCB 0160 by identifying, evaluating and mitigating any risks throughout the products lifecycle.
- 6.0.5 The following matrix should be used to assess the risk associated with an AI enhanced technology. Appropriate mitigations should be put in place to minimise any risk to an acceptable level.

		Clinical Risk				
		The AI has no impact on treatment pathways or decisions.	The AI is used to enhance a treatment pathway, but makes no decisions.	The AI is used to provide additional information to a clinician to help with making a decision, but does not directly make a decision.	AI is deciding the treatment pathway, but this is regularly reviewed.	AI is autonomously deciding the treatment pathway or decisions on care for patients without a clinician intervening.
Governance Risk	The model is trained on a third parties data and uses no PII data for its predictions.	Low	Low	Medium	Medium	Very High
	The model uses our data, including commercially sensitive for its training but does not use PII data for its predictions.	Low	Medium	Medium	High	Very High
	The AI model uses PII data provided to it to make predictions, but it does not retain this data for future use.	Medium	Medium	High	High	Very High
	The model uses PII data provided to it to retrain the model in the future, however it can only process defined data assets.	Medium	High	High	Very High	Very High
	The model uses our data provided to it to retrain the model in the future, and it can input uncontrolled data through sensors.	High	High	Very High	Very High	Very High

- 6.0.6 All software with AI enhancements should have a completed AI checklist that has been reviewed by the Data Science & Operational Research team.

6.1 Prevention of Bias and Discrimination

AI systems are trained on existing data which may be implicitly or explicitly unbalanced by either under or over representing characteristics. This can also be true for the creator and third parties developing AI models who may have preconceived perceptions of said data patterns and inadvertently sway the model in a way that leads to discrimination.

The organisation has a responsibility to ensure that any AI system in use is not unlawfully discriminatory under the Equality Act 2010 and the Data Protection Act 2018. Compliance with one does not guarantee compliance with the other.

6.1.1 The Trust and its employees must consider:

- Processing of Personal Data must be 'Fair.' Any processing of personal data using AI that leads to unjust discrimination of people, will violate the fairness principle.
- Data protection aims to protect individuals' rights and freedoms, which includes the right to not be discriminated against. The organisation is responsible for ensuring reasonable technical and organisational measures are in place to prevent this.
- The processing of personal data for profiling and any automated decision-making may lead to discrimination, the organisation is responsible for ensuring reasonable technical and organisational measures are in place to prevent this.
- Article 22 of the GDPR states that the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling which produces legal effects concerning him or her or similarly significantly affects them.

- 6.1.2 Internal and third-party Developers of Artificial Intelligence must provide assurance that their model has been tested against all protected characteristics and does not produce or exacerbate existing biases.

- 6.1.3 Internal and third-party Developers of Artificial Intelligence must provide assurance that their model is trained, where applicable, on data that is representative of the population of Somerset, its patients, and any personnel employed by Somerset NHS Foundation Trust.

- 6.1.4 It is not permitted to use Artificial Intelligence in a way that would restrict or unfairly prevent the public's right to access healthcare or any public service within nationally agreed targets, for example the 18-week Referral to Treatment (RTT) target.

- 6.1.5 Any concerns relating to bias or discrimination in the context of AI should be escalated to the Data Security and Protection Group using InformationGovernance@SomersetFT.nhs.uk in the first instance.

- 6.1.6 The Trust's AI Ethical Use Review Group has the final decision on matters relating to Artificial Intelligence and may where appropriate refuse a models use if it is deemed to not be compliant with any section of this, or national policy.

6.2 Responsibility & Liability

Where Artificial Intelligence has been used, the creator, third party or Trust will need to ensure that clear accountable lines of responsibility and liability are available.

- 6.2.1 All AI models can have human oversight in the decision-making process.
- 6.2.2 All uses of Artificial Intelligence in use for clinical care that has not met the requirements in 7.3.1 must ensure that it clearly states the model is to only be used as a decision support tool. It is not acceptable to only state this in the terms of service.
- 6.2.3 All uses of Artificial Intelligence must, where relevant, have processes in place where a human can intervene if a model produces incorrect, harmful, or misleading information.
- 6.2.4 All third-party applications must disclose (publicly) the names, roles and professional contact information for their Accountable Senior Leader, Lead for Cybersecurity, Lead for Information Governance, and their Lead AI Engineer.
- 6.2.5 All uses of Artificial Intelligence must, where relevant have processes in place to correct or prevent harmful outcomes.
- 6.2.6 All uses of Artificial Intelligence must have contact information that is dedicated to allowing the users to report issues or concerns about the model's behaviour. It is highly recommended that this is not a generic "contact us" email address.
- 6.2.7 It is noted that third parties will require human intervention in their terms of service for any of its AI products, however, when assessing incidents, liability may be attributed as follows:
- In the case that the Artificial Intelligence model was developed by a third party and was used in accordance with the third parties' recommendations and Trust Policy then the liability is with the third party.
 - In the case that the Artificial Intelligence model was developed by a third party and was **not** used in accordance with the third parties' recommendations and Trust Policy then the liability is with the user.
 - In the case that the Artificial Intelligence model was developed internally then the liability is with the organisation.

Example 1

A person employed by Somerset NHS Foundation Trust has used a large language model on patient identifiable information.

The liability is on the employee for the misuse of patient data. In this circumstance the AI model is not at fault.

Example 2

A person employed by Somerset NHS Foundation Trust used a diagnostic product purchased from a third party. Within the software's terms of use it stated that it was to only be used as a decision support tool (in accordance with this policy), The staff member accepted the AI's diagnosis without review and missed a diagnosis that detrimentally impacted the patient.

The use of AI in this context should only be a decision support tool as using it in this way breached the terms of service and this policy. Therefore, the patient's results should have been checked by an appropriately trained medical professional as such the liability is with the user.

Example 3

The organisation used a third-party AI product that was unfairly biased against a protected characteristic.

The third party should have ensured that their training dataset was sufficient in representing a diverse range of patients. If this was not reported to the organisation then the third party is liable, if the organisation was aware and continued to use the product then they are liable.

6.3 Misinformation

- 6.3.1 Users should be aware of the potential for misinformation in virtual communications outside of the Trust. All users are encouraged to check sources of information or contact the Communications Team should they be unsure of any publications content.
- 6.3.2 Users publicising AI content that may be associated with Somerset NHS Foundation Trust must receive clearance from the Communications Team.
- 6.3.3 When using generative Artificial Intelligence, such as large language models (e.g., Copilot) users should only ask questions in areas they are already familiar with. You should not assume that the output is correct.
- 6.3.4 You should clearly state the origin of any AI outputs. Please see section 7.1.3.
- 6.3.5 Users are not permitted to use Artificial Intelligence in a way that misleads the organisation on their experience or expertise in any subject matter they do not possess. This could include writing reports generated by AI but not stated as such.

6.4 Surveillance

Surveillance uses systematic monitoring and collection of data about individuals or groups through tools such as cameras and sensors. Artificial Intelligence can further enhance surveillance capabilities by enabling real-time analysis, pattern recognition, and making predictions. This can include the tracking of movements, behaviours, and interactions of people which raises significant concerns regarding privacy and consent. It also has a high probability of misuse.

- 6.4.1 It is not permitted to use Artificial Intelligence to track the physical location of any patient, employee, or member of the public without their informed consent.

6.4.2 The use of software that trains on a person's likeness, such as identifying a person's identity from image or video recognition software is not permitted without authorisation by the Trust's AI Ethical Committee.

6.4.3 Any individuals who have opted out of surveillance must be able to do so without penalty.

6.5 Cybersecurity

Artificial Intelligence can be exploited to automate and amplify harassment through chatbots, deepfakes, and social engineering, making it easier to spread harmful content, impersonate individuals, or orchestrate coordinated attacks. Alongside this, the availability of AI enhanced methodologies creates easier access to malicious software and increases the success of scams. Whilst AI can be used to improve the protections of anti-virus and detection, colleagues should be prepared to prevent misuse where possible.

6.5.1 The threat of technologies like deepfakes and generative AI increases the capabilities of threat actors to create realistic fake personas, impersonate real people and create convincing messages. This increases the likelihood of security risks, such as phishing, fraudulent communications, and data breaches. Therefore, it is not permitted to use any AI model that recreates the likeness or can be used to impersonate a member of staff.

6.5.2 With the prevalence of social media, for example LinkedIn, Facebook and X, training AI models to replicate or impersonate employees of Somerset NHS Foundation Trust is widely accessible and should be considered a considerable risk to the Trust. Employees should not take pictures of ID badges or pictures that can be used to support social engineering attacks on social media such as payslips.

6.5.3 Modern malware attacks can avoid detection if used on exploited training data. There is a realistic probability that capable states have sufficient repositories of malware available. All applications of AI require Cybersecurity clearance.

6.5.4 Any Trust information asset that integrates AI generative add-ons within their software need to be assessed to ensure they are compliant with this policy. Information Asset Owners are responsible for ensuring that these are compliant.

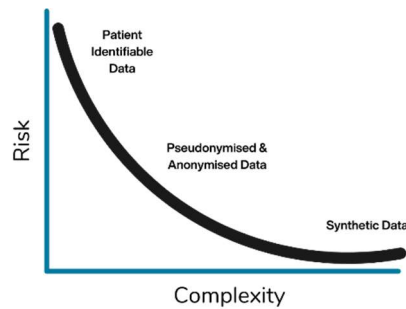
6.5.5 Only tools approved by Cybersecurity and the Data Science & Operational Team are permitted to be used in the development of AI.

6.5.6 There is rarely a reason to use patient identifiable information for the training of a machine learning model. To reduce the risk of accidental disclosure, the following information should not be used in a **training** dataset.

- Unique Identifiers (MRN, NHS Number etc.)
- Name
- DOB (You can use age, or age bandings)
- Full Line Address (You can use LSOAs, Postcode Sectors)

Exceptions to this can only be granted through the Trust's AI Ethical Committee and should where possible use the highest level of anonymisation.

- Synthetic Data (highest)
- Anonymised Data (data cannot be reidentified)
- Pseudonymised (data can only be reidentified with the correct key)
- Patient Identifiable Data (lowest)



- 6.5.7 You should not ask any publicly accessible Artificial Intelligence model (e.g. Google Gemini) any question that would not be appropriate to ask a non-Somerset NHS Foundation Trust colleague. This includes any data that would not be appropriate to be in the public domain.
- 6.5.8 Where existing commercially protected AI models are used in the Trust all non-commercially protected equivalents should be blocked through IT Policy.

6.6 Copyright and Intellectual Property

Please note that this section builds upon legislation from the Copyright Act 2022 and Designs and Patents Act 1988. It is recommended to have a good understanding of these two legislations when interpreting this section. For more specific information please see section 7.1.4

- 6.6.1 You should not use Artificial Intelligence Technologies that use unauthorised data or are not transparent about the source of its data for its training set.
- 6.6.2 Users should not attempt to replicate artists style in marketing or communications without the permission of the original artist.
- 6.6.3 Users should not imply they created or own any form of media generated by Artificial Intelligence.
- 6.6.4 Users should clearly state when they have used AI to generate any content, please see section 7.1.3 for more information.

6.7 Transparency

- 6.7.1 The public and our colleagues have a right to know what AI models are being used on their data. All AI models should be disclosed on the Trust's Public website including information on
- Creators contact information (See section 6.2)
 - If applicable, the rationale for using identifiable data.
 - The accuracy of the model (Accuracy, Precision, Recall etc.).

- A layperson description of the model and how it works.
- Contact information for reporting issues or concerns.

- 6.7.2 When purchasing AI supported products the Trust should prioritise companies that are transparent with their operational practices including participating in open research, engaging with public and patient groups, and contributing to open-source initiatives.
- 6.7.3 All AI models should relay their results in an easily understandable way by maximising the use of techniques like Shapley values. It should be recognised that training may be required to interpret results and that this should be included in the procurement exercise for any products.
- 6.7.4 For any AI software being used for clinical care, there should be considerations by the developer to ensure that the results can be explained in layperson terms to aid clinical professionals in relating technical information to patients.

7 Specific Applications of AI

7.1 Communications and public facing media

7.1.1 Generating Creative Media

Creative Media covers any personnel that is using Artificial Intelligence for the creation of media, including images, video, or audio. For generative models on Text see the “General section 7.5.”

7.1.2 Preventing loss of Originality / Creativity / Quality

Users should ensure that any AI generated content follows the same due diligence and quality checks that any other content would be required to follow. AI should only be used as a tool to enhance and inspire human creativity, not to replace it.

7.1.3 Referencing when AI has been used

Where Artificial Intelligence media has been used to generate an image, video, or audio, it must clearly state the tool used, the input and the date the output was generated alongside the applicable AI generation.

Example reference.



Image Generated by: Magic Media
Input “Draw a duck sitting in a tree.”
Date Generated: 11-04-2024.

7.1.4 Use of existing creative media

Artists have a right to receive recognition and credit for their work and are protected under copyright laws; therefore, it is not permitted to ask generative AI to replicate an artist's style without permission from the artist.

It cannot be assumed that the generative AI model has the permission from the artist due to the way that these models are trained.

Example

Acceptable – “Draw an image of a group of people dancing.”

Not Acceptable - "Draw an image of a group of people dancing in the style of Banksy.”

This also applies to video (e.g. create a video in the style of Pixar), text (e.g. write a report in the style of Stephen King) or Audio (e.g. read this text in the voice of Morgan Freeman).

7.1.5 Editing media

Due to the way that way AI media editing works, it can be difficult to prevent unintended changes. You should, where an image contains people, request permission to edit the image from the subjects clearly stating the edits you are proposing. Use caution when using AI to change the appearance of people and ensure that all images are double checked before publication. At a minimum users should check for:

- Inaccurate objects
- Artifacts and Distortion
- Replicating an artist's style
- Over smoothing or unnatural edits

Example of an image referenced as being edited.



This image has been edited using AI.

7.2 Recruitment

“Any software using Artificial Intelligence that is used for the management of personnel employed or applying for work with Somerset NHS Foundation Trust.”

- 7.2.1 We support applicants to utilise the benefits of Artificial Intelligence as a support tool when writing applications. However, applicants should not use it to provide misleading

information or imply misleading experience and understanding relating to the application process.

- 7.2.2 During the application process a placeholder should be included explaining 7.2.1, and that the applicant accepts the implication of the application being rejected if it is felt that AI was used to answer the questions in a way that was intentionally misleading.

7.2.3 Questions for exams, applications, or forms

Artificial intelligence makes it extremely easy to answer complex questions on application forms, or in remote interviews. However, it struggles when it needs to apply a question to a scenario that it is not trained on, for example, lived experiences.

For reviewers of applicants, you should be aware of the common mistakes that AI models have when constructing sentences. These are:

- Using incorrect or outdated information
- Lack of depth or personality in the writing
- Repetitive language, structure, or cadence
- Use of uncommon, inappropriate, or complex words

Please note although the above could indicate the use of AI it is not meant as guidance and not a set of rules.

7.2.4 Phrasing questions

When asking questions to potential candidates' recruiters should ensure that questions are phrased to request individual experiences or applied evidence of essential criteria.

7.2.5 Reviewing applicant questions.

When reviewing questions, the reviewer should look to see references that correspond throughout the application. For example, when drawing upon past experiences in questions, this should correlate to the job history and the roles and responsibilities they have stated they had.

7.2.6 Screening Applicants

It is not permissible to use Artificial Intelligence to screen applicants based on protected characteristics or in a way that would be deemed discriminatory (see section 8– Legal regulations for AI). It is heavily advised to not allow any features that would come under these categories to be passed to the Artificial Intelligence model in any form (training or new data) including to a third-party supplier or internally.

7.2.7 Generative AI within Search Engines

Search engines such as Google and Bing have integrated AI into their solutions that can generate summarisations and content from search prompts. The use of non-Trust approved tools for the purpose of generating content or passing sensitive information, including documents is not permitted. However, you can still use the search functionality it provides.

For example, with Google it now provides an AI “Summary” of a search result, the advice is to not use this summary. If you need a summary or any generated content, then you should use the approved Trust generative AI solution.

7.2.8 Non-Medical Device Generative AI tools (e.g. Copilot Chat & Pro)

Non-Medical Device Generative AI refers to Generative AI tools like Copilot that are not approved as a medical device with the MHRA.

7.2.8.1 You must not use Non-Medical Device Generative AI tools in a way where it would be deemed to be removing clinical judgement or for directly interacting with a patient in a way that it could influence their care.

7.2.8.2 You must always review the outputs of any Generative AI before distributing any materials.

7.2.8.3 You must not use any other form of Generative Artificial Intelligence other than those approved for use for completing tasks. To see the latest tools that are available please check the Information Asset Register or consult the Artificial Intelligence intranet page.

7.2.8.4 You must not use a personal device to circumvent the restrictions listed in 7.2.8.3 for completing work-based tasks.

Examples where it is not permitted to use Copilot Pro or Chat

There may be other AI enhanced tools that can complete the below tasks, please visit the Artificial Intelligence intranet page to see if tools have been approved.

- Creating a personalised patient care plan including, but not limited to, diagnosis, investigation and management options.
- Dictating a clinical appointment
- Using the tool to decide the treatment of a patient
- For deciding the clinical pathway for a patient or for deciding the appropriateness for discharge
- For creating personalised information leaflets, including around medications (please use the Trust approved leaflets only).

Examples where it is permitted to use Copilot Pro or Chat

- Helping to design a patient leaflet (that will be approved by our patient leaflet team)
- Helping to create a generic care plan for a service that will then be adapted on a case-by-case basis by a clinician
- Finding useful clinical information for the purpose of research

7.2.9 Agentic Agent Developments

The development of Copilot Agents must be registered on the Trust information asset register (once deployed) and should only be developed by trained professionals. To see a list of approved teams for development please visit the Artificial Intelligence intranet page.

7.3 Clinical Applications

Any AI that is used to influence a clinical treatment or pathway should be registered as a medical device and as such requires MHRA classification. For clarity, here are examples of clinical AI models and Somerset NHS Foundation Trusts associated classification expectations

Class	Examples
Class 1	Ambient Voice Technology (without the ability to summarise)
Class 2a	Hearing aids using AI technology to enhance clarity or Ambient Voice Technology (with the ability to summarise or generate content)
Class 2b	Diagnostic AI systems that have a human-in-the-loop or AI that provides information used in clinical decision-making
Class 3	Virtual nursing systems or Diagnostic AI systems that do not have a human-in-the-loop, or Implanted devices that use AI technologies

7.3.1 Unless the standards below are met, Artificial intelligence can only be used as a decision support tool, and it is not permitted to design or implement AI in a way where it replaces the expertise of a clinical professional or goes against the agreed practices outlined in other Somerset NHS Foundation Trust or national policies. In addition, any device that is assessed as “Very High” in section 6.0.5 needs to meet these requirements.

- Ethical Committee approval
- Class 3 MHRA certification including conformity assessment
- The company supplying the AI model have taken on legal responsibility for any failings, misdiagnosis or harmful outcomes caused by their AI model.
- The company supplying the AI model have financial stability or insurance to handle any litigation for the duration of the contract.
- Completed DCB0160 & DCB0129 assurance process and documentation
- Clinical Safety team review and all requirements met
- Named Clinical Safety Officer at Somerset NHS Foundation Trust
- Named Clinical Safety Officer at the supplying company
- Completion of section 6 of this policy
- Leaflets explaining the AI model to ensure informed consent is given to any patient whose data will be used in the AI model.
- A plan outlining the procedure for staff to follow should the system stop working, or the company is no longer able to operate to ensure colleagues can return to the original way of working.
- Robust business continuity arrangements must be in place, including escrow models or equivalent safeguards, to ensure access to critical systems and data if the supplier ceases trading.
- The procurement contract should specify redundancy measures and contingency plans to maintain clinical operations in the event of supplier insolvency or service disruption.
- Post market surveillance and regular audits
- DPIA, DTAC, DSPT, CREST approved Pen testing
- Supply chain risk assessment

If the model is intended to be used on or uses novel information pertaining to colleagues working at Somerset NHS Foundation Trust, then will be required by representatives from staff side. This will be decided by the Trusts AI Ethical committee.

For Software and AI as a Medical Device that have been developed outside of Somerset NHS Foundation Trust, or where Somerset NHS Foundation Trust is a joint partner then the following apply.

- 7.3.2 All Artificial Intelligence models that have been classified as Software and AI as a Medical Device must be compliant with the Medical Device Regulations 2002 (UK MDR 2002) and any additional Medicines & Healthcare Regulatory (MHRA) recommendations including but not limited to Software and AI as a Medical Device Change Programme WP9-01 to 11.
- 7.3.3 All Artificial Intelligence models being used or designed that meet the DCB definition of a Health IT System must be compliant with the recommendations outlined in DCB0129: Clinical Risk Management: its Application in the Manufacture of Health IT Systems
- 7.3.4 All Artificial Intelligence models being used or designed that meet the DCB definition of a Health IT System must be compliant with the recommendations outlined in DCB0160: Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems.
- 7.3.5 Incidents relating to Artificial Intelligence within Software and AI as a Medical Device should be reported via the yellow card scheme / app.
- 7.3.6 Third party companies working with Software and AI as a Medical Device must have completed and had approved a Digital Technology Assessment Criteria (DTAC) before the commencement of any work.
- 7.3.7 Third party companies working with Software and AI as a Medical Device must have completed and had approved a Data Protection Impact Assessment (DPIA) before the commencement of any work.

The following apply for all Software and AI as a Medical Devices, and any AI applications developed by Somerset NHS Foundation Trust.

- 7.3.8 All Software and AI as a Medical Device intended for use in a clinical setting must have been approved by the AI Ethical Committee of Somerset NHS Foundation Trust.
- 7.3.9 All Artificial Intelligence models being used or designed that meet the DCB requirements need to be registered on the Trust Clinical Risk Management System.
- 7.3.10 All applications that have been trained using data from Somerset NHS Foundation Trust must comply with section 5.6.

- 7.3.11 Access to Somerset NHS Foundation Trust data for the purpose of training Artificial Intelligence models must be approved for each data exchange from the AI Ethical Committee.
- 7.3.12 Where Somerset NHS Foundation Trust, or any employee of Somerset NHS Foundation Trust representing the organisation, is the creator of a Software and AI as a Medical Device and intends to distribute the software externally then you must act as a third party and comply with the conformity and UKCA marking procedures.
- 7.3.13 Exemptions for Medical Device Regulations 2002 may exist where work has been commissioned by a valid institution, and where Somerset NHS Foundation Trust is acting as a specialist research and development laboratory. Colleagues seeking any exemptions must seek approval from the AI Ethical Committee.
- 7.3.14 No Artificial Intelligence tool is permitted to delete or alter any clinical or legally binding document including patients' medical notes and contracts. Such tools should only be permitted to add information, and in the case of amendments must be reviewed by a professional before overwriting.
- 7.3.15 Any Artificial Intelligence model used in clinical applications must be extensively tested to ensure accurate predictions across a wide range of demographic groups. For example, in the case of skin image analysis, the full range of Fitzpatrick skin types should be used. It is recommended that any results are independently reviewed.
- 7.3.16 **Ambient Voice Technology (AVT)**
As per the NHS England definition “Ambient scribing products involve tools that use advanced speech technologies to automatically convert spoken words into text and other outputs, requiring minimal user intervention. They are designed to support clinical or patient documentation and workflows.”
- 7.3.17 Staff are only permitted to use the approved Ambient Voice Supplier, please check the dedicated Artificial Intelligence page on the Intranet for more information on our approved supplier.
- 7.3.18 Any Ambient Voice supplier will be required to meet the standards below.
- Digital Technology Assessment Criteria DTAC
 - Data Security and Protection Toolkit DSPT
 - Cyber Essentials Plus
 - CREST-approved pen testing
 - DCB0129 compliance
 - Data Protection Requirements as set by ICO
 - Clinical Safety Officer(s) named and accountable
 - End-to-end encryption and GDPR compliance
 - No unsafe functionality e.g. prompt injection access
 - Appropriate NHS clinical system integration (API or FHIR/HL7 compliance and write-back capability)

- The responsibility for translation accuracy remains with the AVT supplier.

7.3.19 Additional requirements for advanced AVT functionality

- **Medical Device Classification** – All AVT solutions that undertake summarisation require, at least, MHRA Class 1 medical device status. Companies must NOT extend system capabilities to produce generative diagnoses, management plans, or other medical referrals and calculations without seeking at least MHRA Class 2a approval.
- **Data Protection** – Patient data from clinical sessions (e.g. immediate inference) should be automatically deleted unless legally or operationally required, in line with UK GDPR and DPA 2018 principles on data minimisation and storage limitation.
- **System integration** – Ensure appropriate integration with your IT infrastructure, systems and workflows.

7.4 Data Science, Analytics and Research

Data Scientists within the Trust create, use, and modify AI models to interrogate data and generate predictions or simulations. While the scenarios outlined here aim to cover a broad spectrum of applications, it is essential to remain vigilant for potential edge cases that may emerge in the future. In instances of uncertainty, you should gain advice from the Data Science & Operational Research Team and the AI Ethical Committee.

7.4.1 Predictive & Prescriptive Analytics

- 7.4.2 Predictive & Prescriptive Analytics covers a wide range of Data Science and Operational Research methodologies, including but not limited classification, regression, clustering, anomaly detection, simulation modelling, deep learning, neural networks, forecasting, natural language processing, sentiment analysis.
- 7.4.3 Predictive and Prescriptive techniques should only be performed by trained professionals.
- 7.4.4 All Artificial Intelligence models developed or modified by Somerset NHS Foundation Trust must have full version control.
- 7.4.5 All Artificial Intelligence models created internally with the intent for use outside of Somerset NHS Foundation Trust must be registered on the Trust's Information Asset Register.
- 7.4.6 All Artificial Intelligence models developed within Somerset NHS Foundation Trust should prioritise the use of free and open-source technologies, during development, deployment, and dissemination.
- 7.4.7 Artificial Intelligence applications that become part of critical infrastructure must be approved by the Trust's AI Ethical Committee.

7.5 General

7.5.1 Use of Demographic Information

No Artificial Intelligence model should include the demographic information listed below of any person, including employees and patients. The only permissible identifier is the NHS number of a patient, where it complies with GDPR and is necessary to link the prediction of a machine learning model to a record.

- Postcode, Address (use LSOA)
- Contact Information including Email and Phone Numbers
- Social media account information

You should not use protected characteristic information unless approved by the Trust's AI Ethical Committee.

7.5.2 Redundancy of AI systems

All applications of AI within Somerset NHS Foundation Trust, where they are part of a critical business function, must have redundancy built in that prevents a loss of service should the tool become unavailable for any reason.

Any deployed model used for decision-making, including those by third parties must maintain a minimum uptime of 99%.

7.5.3 Use of AI for Office Efficiency Tools

It is encouraged where possible to utilise spelling and grammar tools that have been enhanced with Artificial Intelligence where these exist within the agreed productivity suite already installed by IT. It is not permitted to use online web-based tools not owned or managed by Somerset NHS Foundation Trust, for example ChatGPT for this purpose.

Users should use AI where it can improve administrative workflows, providing these tools exist in software that has been signed off by Cybersecurity and Information Governance.

7.5.4 Use of large language models

The use of large language models is permitted where it does not breach GDPR, use data that would be deemed sensitive or confidential and does not bring Somerset NHS Foundation Trust into disrepute.

No member of the Trust should use patient or employee data with unapproved AI models. Specifically, patient data should never be uploaded to ChatGPT or similar services.

7.5.5 Use of AI for Programming

It is permitted to use programming assistance tools where these exist in already approved applications or where the question is generic and not related specifically to Somerset NHS Foundation Trust. Web based models should not be supplied with any code owned by Somerset NHS Foundation Trust or its suppliers.

7.5.6 Use of AI for Translation

The use of AI to facilitate translation of real time speech and text documents provides enormous potential for improving diversity and inclusion for non-English speakers.

However, users should be aware that relaying critical information (especially medical) may be inappropriate, due to the possibility of misinterpretation and should be reviewed on a case-by-case basis factoring in the risk of, or distress caused by using said tools.

Examples

Acceptable: Translating an appointment letter from Spanish

Where you should use a professional human translator: Translating a cancer diagnosis to a patient.

7.5.7 Use of AI for Meeting Transcription

In general, the risk posed by incorrect meeting translation is low, however, transcripts should be checked at the end of meetings to ensure accurate portrayal of the meeting.

In some circumstances, especially where the meetings transcript will be in the public domain or is legally required to be transcribed, it is recommended that a human transcriber is used.

Any model that is used for the use of meeting translation should be checked to ensure that it can identify a wide range of accents including those where English may not be their first language with a high accuracy.

7.5.8 Non-Clinical Automation

The use of autonomous nonclinical AI is permitted upon approval from the Trusts Ethical Committee if the standard requirements for AI and digital systems have been met (section 6).

If the model will also use any information pertaining to colleagues working at Somerset NHS Foundation Trust, then will be required by representatives from staff side.

Developers and Third Parties that have developed any AI automated workflow should ensure that a regular review process is conducted to ensure that the scope of the workflow still meets the original scope and complies with this policy.

7.6 Third party applications

- 7.6.1 All third-party software (including web based) must be compliant with Section 6.

8 Legal regulations for AI

Due to the recent emergence of AI, legal frameworks are still being developed. However, the current legal acts currently apply and should be considered when using or designing AI.

8.1 Data Protection law

Which controls data collection and processing for AI. This is the remit of the Information Commissioner's Office (ICO)

- Data Protection Act 2018

8.2 **Equalities, Privacy and Common laws**

Which controls the outputs of AI systems and decisions which may discriminate or have human rights implications. This is the remit of the Equalities and Human Rights Commission.

In addition, privacy and common laws limit the degree to which employers can substitute AI decision-making for their own judgement and places restrictions on the use of surveillance tools to monitor workers.

- Equality Act 2010
- Human Rights Act 1998

8.3 **Intellectual Property Laws**

Which controls the ownership and legal use of any intellectual property in the outputs of AI or in training datasets. This is the remit of the Intellectual Property Office (IPO) to enforce.

- Copyright Act 2022
- Designs and Patents Act 1988

Emerging

8.4 **UK Artificial Intelligence Regulation Framework**

Which will control the safety, security, robustness, transparency, explainability, fairness, accountability, governance, contestability, and redress of AI in the UK. The regulator is yet to be decided.

Whilst not part of our legal framework, the EU's AI Act is likely to influence providers and applications of AI across all industries and geographies.

9 **Restricted Practices**

The practice of Artificial Intelligence has additional protections in place on top of the normal ethical framework, this list demonstrates implementations of Artificial Intelligence considered considerable risk to our patients, our colleagues and the reputation of Somerset NHS Foundation Trust and are **therefore highly discouraged without ethical approval**. They include.

- Cognitive behavioural manipulation of people or specific vulnerable groups: for example, using automated chat bots to provide clinical advice to a patient.
- Using Artificial Intelligence in a way that invades the rights to privacy for our colleagues or patients.
- Artificial Intelligence that contradicts with the safety or technology recommendations of any device, technology or agreed practice. I.e. using Artificial

Intelligence in a way that would not be compliant with NICE guidance; such uses should use a research approach.

- Any use of Artificial Intelligence that negatively impacts the wellbeing of our patients or colleagues for example, using generative Artificial Intelligence to create edited images of said persons without their permission.
- Using Artificial Intelligence in a way that it becomes part of the critical infrastructure in the Trust without appropriate fail safes being in place.
- Any model that is designed to edit (without stating its edits) or delete any legally binding document, policy or medical record including patient notes, diagnostics, and electronic healthcare records etc.
- Any use of Artificial Intelligence for deciding the right of access to any service provided by an NHS organisation.
- Using any form of Artificial Intelligence to engage with patients without physical oversight. For example, sending a patient letter generated solely with ChatGPT without a human checking the document or a statistically significant sample of the population being checked.
- Relaying critical medical information or providing recommendations on care without physical oversight by an appropriately trained medical professional.
- Using automated translation software to relay critical medical information or providing recommendations on care without physical oversight by a trained translator.
- Using Artificial intelligence to scan cohorts of job applicants for positions within the Trust where protected characteristics have been used in the training set or where the application of AI is likely to cause discrimination.

10 Procurement of products containing AI

- 10.1.0 The approval process for any software or hardware containing Artificial intelligence features is available on the Artificial Intelligence and Procurement intranet pages.
- 10.1.1 All systems that have Artificial Intelligence features must ensure they are compliant with Section 6.
- 10.1.2 Any software system that retrospectively adds in an Artificial Intelligence feature that was not present on the signing of the contract must ensure they are compliant with Section 6.
- 10.1.3 The Information Asset Owner is responsible for the yearly review using the Trusts Information Asset Register and for ensuring that the AI Procurement checklist is completed and updated.
- 10.1.4 All novel (where the use case of the AI has not been used before) uses of Artificial Intelligence must be reviewed the Trusts AI Ethical Committee before any procurement process is commenced.
- 10.1.5 Third party suppliers of AI systems have a legal responsibility (Health and Social Care Act 2012) to provide the following during the procurement process

- A full outline of the scope of their system
- An outline of the systems functionality
- Its intended care setting
- Any hazards identified following a clinical risk management process
- A risk assessment supported by clinical explanation and justification
- Appropriate risk control evidence
- Any outstanding test issues or defects within the system that have or may have a clinical safety impact
- A summary safety statement written by their named Clinical Safety Officer and if applicable approval by the corresponding manufacturer's Clinical Safety Officer,
- Full disclosure of the identification and justifications of any third-party products used in their system.

11 References

- 11.1 Data Protection Act 2018
- 11.2 Copyright Act 2022
- 11.3 Designs and Patents Act 1988
- 11.4 Equality Act 2010
- 11.5 Human Rights Act 1998
- 11.6 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts
- 11.7 A pro-innovation approach to AI regulation (Department for Science, Innovation and Technology)
- 11.8 Data saves lives: reshaping health and social care with data Policy Paper (Department of Health & Social Care)
- 11.9 Better, broader, safer: using health data for research and analysis (Department of Health & Social Care)
- 11.10 AI Ethics & Governance in Practice (Alan Turing Institute)
- 11.11 Use of Artificial Intelligence in government (National Audit Office)
- 11.12 Code of Practice for General-Purpose AI Models – Safety and Security Chapter (European Commission)
- 11.13 Code of Practice for General-Purpose AI Models – Transparency Chapter (European Commission)
- 11.14 Code of Practice for General-Purpose AI Models – Copyright Chapter (European Commission)
- 11.15 Medical Device Regulations 2002

- 11.16 Medical Device Change Programme
- 11.17 DCB0129: Clinical Risk Management: its Application in the Manufacture of Health IT Systems
- 11.18 DCB0160: Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems.
- 11.19 Health and Social Care Act 2012

12 Monitoring

Element of policy for monitoring	Section(s)	Monitoring method - Information source (e.g. audit)/ Measure / performance standard	Item Monitoring Lead	Monitoring frequency /reporting frequency and route	Arrangements for responding to shortcomings and tracking delivery of planned actions
All systems using AI need to be logged and regularly reviewed (yearly)	6.0.2, 6.5.4, 7.2.9, 7.4.5, 10.1.3-10.1.4	Audit of compliance on the Information Asset Register	Data Science & Operational Research Team	Quarterly to the Data Security and Protection Group (DSPG) with local monitoring monthly to the AI Policy Group	Handled by the Data Security Protection Group
Transparency & Public Disclosure	5.5.1, 6.2.4, 6.7.1-6.7.4, 7.1.3	Audit of any Artificial Intelligence system that is using Somerset NHS Foundation Trusts data for its training should be stated as such on the Trusts public facing website.	Data Science & Operational Research Team	Yearly to DSPG	Handled by the Data Security Protection Group
Clinical Applications of AI	6.2.2, 7.3.1-7.3.5, 7.3.14-7.3.15	Audit of AI enabled clinical systems to ensure they have disclaimers of being a decision support tool or exemption through a valid medical devices certification.	Digital Clinical Safety Team	Yearly to DSPG	Handled by the Data Security Protection Group
Third Party Applications Compliance	6.0.1-6.0.4, 6.0.6, 6.2.4, 6.6.1-6.6.7, 7.3.6-7.3.7,	Compliance with the AI procurement framework for all new AI enabled software	IT Procurement Lead	On all new AI procurements but concerns by exception to the AI Ethical Use Review Group	Handled by the AI Ethical Committee

	7.6.1, 10.1.0-10.1.5				
Complaints or Concerns raised relating to AI (including in relation to concerns in bias and discrimination)	All	By individual case	Andy Mayne	DSPG	Handled by the AI Ethical Committee and Data Security Protection Group