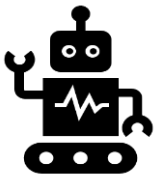
Artificial Intelligence (AI) Policy

AI-24 v1.1

Author	Katie Jones/Rob Montgomery
Review Cycle	Annually
Date Approved	6th March 2025
Approved By	Head's Board
Next Review Date	March 2026

1. Introduction



AI - the ability of a digital https://www.britannica.com/technology/computercomputer or computer-controlled robot to perform tasks commonly associated with intelligent beings.

1.1 There are clear benefits and risks associated with processing data (including voice data) using AI solutions/technologies.

1.2 The Shropshire Gateway Educational Trust is committed to taking a risk-based approach to the implementation and use of IA. This means:

- Assessing the risks to the rights and freedoms of individuals that may arise when using AI
- Implementing appropriate and proportionate technical and organisational measures to mitigate these risks.

1.3 This policy is written to ensure that the use of AI is compliant with all applicable laws, regulations and school policies. It supports the ethical and moral use of AI under the school's instruction.

1.4 This policy provides a framework for the use of AI solutions/technology by school employees (whether temporary or permanent), Governors, contractors, agents, vendors and anyone else processing information in pursuit of the school's activities.

1.5 Given the pace of IA development, this policy will be continually developed to ensure it mirrors legislative/regulatory requirements and best practice.

2. Use of AI

2.1 The use of AI solutions/technologies should always support the school's/Trust's vision, priorities and values.

2.2 Schools and staff that are considering the use of AI should engage with internal stakeholders as part of their due diligence. **As a minimum, the schools Data Protection Officer and ICT Support should be consulted on all AI projects.**

2.3 In the feasibility stage of plans to use AI, schools must consider the relevant governance requirements, any provider practices if 'off the shelf' applications and/or technologies are procured, copyright, confidentiality, disclosure, accuracy and potential integration with other tools.

2.4 The AI solution should have appropriate logging and auditing mechanisms in place to capture activities related to AI usage.

3. Governance Requirements for Using AI

3.1 Any stakeholder looking to use/implement an AI solution/technology must be fully aware of the Trust's policies and procedures relating to data. As a minimum the stakeholder must have a good understanding of the requirements detailed in the following documents:

- Data Protection Policy
- Schools Information Security Policy
- Records Management Policy
- Information Sharing Policy
- Schools Information Retention Schedule

3.2 The risks associated with the introduction and use of an AI solution/technology need to be assessed and managed (essential if the AI product is to process personally identifiable information or AI could affect student

futures e.g. through AI marking). To assist in the identification, mitigation and management of AI associated risks, the school/staff intending to use AI must complete:

- AI Risk Assessment
- AI Data Protection Impact Assessment

Templates for these assessments are at the end of this policy.

Both assessments require approval before the school implements the AI solution/technology.

4. Supplier/Vendor

4.1 Where a school looks to procure AI solutions/technology, engagement should be established with the relevant Information Asset Owner, senior management and developers/vendors.

5. Copyright Considerations

5.1 Copyright law must be complied with when using AI.

5.2 AI must not be used for generating content that infringes upon the intellectual property rights of others, including but not limited to copyrighted materials. If the school is unsure as to whether the intended use of AI may infringe copyright they should contact their legal support.

6. Accuracy of AI Output

6.1 **Information produced by using AI solution/technology must be reviewed by the school/staff for accuracy prior to sharing/using the information. AI tools should complement human judgement not replace it.**

6.2 **If the school/staff have any doubt about the accuracy of AI output then AI solutions/technology should not be used.**

7. Confidentiality

7.1 **Personal and confidential information must not be processed using public AI solutions such as ChatGPT, as this may enter the public domain.**

7.2 If the school is planning to use a non-public AI solution, and this will include processing personal data, then as a minimum an AI Data Protection Impact Assessment must be completed.

7.3 Any processing of personal data using an AI solution must comply with the principles of the UK Data Protection Act 2018.

8. Integration with Other Tools

8.1 API (Application Programming Interface) and plugin tools enable access to AI and extended functionality for other services. Schools planning to integrate AI should follow Open AI's Safety Best Practices:

- **Adversarial testing** – testing AI should include typical scenarios as well as tests to 'break' the system
- **Human in the loop (HITL)** – a person should review AI output before it is used more widely
- **Prompt engineering** – reduces the chance of producing undesired content
- **Know your customer (NYC)** – AI users should have to register to use the AI solution and have a unique user id
- **Constrain user input and limit output tokens** – limiting the amount and type of input/output can reduce the likelihood of misuse/error
- **Allow users to report issues** – a mechanism should be available to allow AI users to log concerns they have while using the AI solution
- **Understand and communicate limitations** – consider whether the AI solution has limitations that could create offensive and/or discriminatory content

- **End-user IDs** – the use of unique user IDs can help detect improper use of AI

8.2 Any relevant API and plugin tools must be rigorously tested for:

- **Moderation** – AI handles inappropriate input that can be categorised as hate, discriminatory, threatening, etc
- **Factual responses** – establish a ground of truth for the API and review responses against this

9. AI Risks

9.1 The use of AI carries inherent risks. Before AI solution/technology is implemented, a thorough risk assessment should be completed. See 3.2 for what assessments are required.

9.2 Each new AI project will have its own context, data flows, output requirements and therefore needs to be assessed individually against the core requirements of this policy. The completion of the risks assessment and AI Data Protection Impact Assessment will assist the school to manage each AI project.

10. Compliance with Legal and Regulatory Requirements

10.1 Data processed by public facing AI solutions may enter the public domain resulting in potential personal data breaches, breaches of confidentiality and/or compromising intellectual property.

10.2 Schools using AI solutions/technology must ensure that this use complies with all applicable laws, regulations and school polices at all times.

10.3 Unauthorised use of copyrighted material or the creation of content that infringes on the intellectual property of others is strictly prohibited.

11. Bias and Discrimination

11.1 **Some AI solutions may use and/or generate biased, discriminatory or offensive content. Therefore, schools using AI need to understand this and ensure any AI output is comprehensively checked by a human to ensure biased, discriminatory or offensive content can be censored/removed.**

12. Security

12.1 The school is committed to protecting the confidentiality, integrity and availability of its data.

12.2 AI solutions may store personal, sensitive and/or confidential information which could be at the risk of disclosure due to the AI technology being hacked.

12.3 Schools looking to use AI solutions must ensure that the relevant technology in place is secure. Technical controls must be commensurate with the level of risk associated with the information being processed by the AI solution.

12.4 Where the AI solution processes personal data, the school must investigate whether this data can be anonymised.

12.5 Any data processed by an AI solution should be encrypted in transit and at rest.

12.6 The AI solution should have the appropriate security accreditations such as ISO27001, Cyber Essentials+, etc. If the solution uses cloud computing then this should comply with the NCSC 14 Principles of Cloud Computing.

12.7 Schools should check the level of security of any proposed AI solution with their ICT Support and Data Protection Officer.

13. Data Sovereignty and Protection

13.1 Many AI solutions will be hosted internationally. However, under data sovereignty rules any information created or collected in the originating country will remain under the jurisdiction of that country's laws.

13.2 Any AI solution used should be checked for its data sovereignty practices prior to use. If the practices cannot be determined then schools should contact their Data Protection Officer for further advice.

14. Training and Awareness

14.1 All users of AI solutions must receive training on the responsible and secure use of AI. This training should cover topics such as ethical considerations, risk management, security and compliance requirements.

15. Compliance

15.1 This policy applies to all school uses of AI solutions/technology.

15.2 Any suspected or confirmed security incidents related to AI usage must be reported to the Data Protection Officer.

15.3 Failure to comply with this policy may result in disciplinary action being taken.

16. Review

16.1 This policy will be reviewed periodically and updated where necessary to ensure ongoing compliance with all relevant legislation, regulations, other school policies and best practice.

Document Version Control

Version	Date	Author	Sent To	Comments
1.1	06/11/24	R Montgomery	Schools/Academies	Creation of policy based on SOCITM template.

Appendix A: Copilot Guidance

What is Copilot?

Copilot is an AI companion created by Microsoft designed to assist with a wide range of tasks. Whether you're looking to boost your productivity, get answers to questions, brainstorm ideas, or simply have a friendly chat, Copilot is here to help. It can provide information, generate creative content, complete productivity-related tasks, and more.

How to Use Copilot

1. **Getting Started:**
    - Simply start by typing your query or task in the chat. For example, you could ask, "What are some interesting facts about space?" or "Help me draft an email."
2. **Asking Questions:**
    - You can ask Copilot any question, and it will provide a detailed and accurate response. For example, "How does photosynthesis work?" or "What's the weather like today?"
3. **Completing Tasks:**
    - Copilot can assist with a variety of tasks such as writing essays, generating code, creating lists, or even generating images (with certain limitations). Just be specific about what you need help with.
4. **Brainstorming Ideas:**
    - Stuck on a project or need some inspiration? Copilot can brainstorm ideas with you. For example, "Can you help me come up with a story idea?" or "What are some creative ways to promote my event?"
5. **Getting Creative:**
    - You can collaborate with Copilot on creative projects such as writing poetry, composing lyrics, or crafting a story. Just let your imagination run wild!
6. **Conversing:**
    - If you want to have a casual conversation, Copilot is more than happy to chat. You can talk about current events, hobbies, or any other topic that interests you.

Best Practices:

- **Be Clear and Specific:** The more specific you are with your requests; the better Copilot can assist you. Instead of saying "Help me," try "Help me write a cover letter for a job application."
- **Engage in Dialogue:** Feel free to ask follow-up questions or provide feedback on Copilot's responses. It can adapt and provide more tailored assistance based on your interaction.
- **Respectful Interaction:** Always communicate respectfully and professionally with Copilot, keeping in mind the educational and productive environment.

Appendix B: Staff Acceptable Use Policy (AUP) for Microsoft Copilot in an Educational Setting

1. Purpose

This Acceptable Use Policy (AUP) outlines the responsible use of Microsoft Copilot by staff within the Shropshire Gateway Educational Trust. Copilot is a powerful tool designed to enhance productivity, but its use must align with safeguarding, data protection, and professional standards.

2. Scope

This policy applies to all staff members using Copilot on any school-owned or personal device when conducting school-related activities.

3. Acceptable Use

Staff may use Copilot for the following purposes:

- Drafting emails, lesson plans, reports, and other school-related documents.
- Enhancing productivity in non-confidential administrative tasks.
- Supporting teaching, learning, and curriculum development.
- Assisting with summarizing non-sensitive meeting notes or documents. The use of Teams/Copilot for non-sensitive recording/transcribing meetings is acceptable but: a) everyone at meeting needs to know recording will take place b) where you will save the recording and who needs access c) how long you will keep the recording d) how you might share the recording if this is needed

4. Prohibited Use

Staff must not use Copilot for:

- Sensitive Conversations: Transcribing or summarizing meetings involving safeguarding, pupil well-being, HR matters, or confidential staff/student information.
- Personal Data: Processing personal or identifiable information about students, staff, or parents.
- Misleading Information: Generating content that could be false, misleading, or inappropriate.
- Non-Educational Use: Personal tasks unrelated to school activities.

5. Data Protection and Privacy

All data processed through Copilot falls under the school's Data Protection Policy and GDPR guidelines.

Staff must ensure that no confidential or sensitive information is shared or processed through Copilot.

Copilot-generated content remains the responsibility of the user and should be reviewed for accuracy and appropriateness before sharing.

6. Monitoring and Compliance

Usage of Copilot may be monitored to ensure compliance with this policy.

Any misuse may result in disciplinary action in line with the school's ICT and Conduct Policies.

Appendix C: Pupil Acceptable Use Policy (AUP) for Microsoft Copilot in an Educational Setting

1. Purpose

The purpose of this Acceptable Use Policy (AUP) is to establish guidelines for the ethical and responsible use of Copilot, an AI companion created by Microsoft, in an educational setting. This policy aims to promote a positive and productive learning environment while ensuring the safety and privacy of all users.

2. Scope

This policy applies to all students and any other individuals who use Copilot within the educational institution.

3. Responsible Use

3.1. Educational Use Only

- Copilot should be used solely for educational purposes, including research, learning, collaboration, and productivity.
- Personal use of Copilot during school hours is discouraged unless approved by a teacher or administrator.

3.2. Respectful Communication

- Users should communicate respectfully and professionally with Copilot, refraining from using offensive or inappropriate language.
- Harassment, bullying, or any form of discrimination while using Copilot is strictly prohibited.

3.3. Privacy and Security

- Users should not share personal, sensitive, or confidential information with Copilot.
- Copilot should not be used to access, store, or transmit any data that violates privacy laws or institutional policies.

3.4. Intellectual Property

- Users must respect copyright laws and intellectual property rights when using Copilot.
- Copying, sharing, or distributing copyrighted material without proper authorisation is prohibited.

4. Prohibited Use

4.1. Inappropriate Content

- Users must not use Copilot to create, access, or share content that is violent, sexually explicit, discriminatory, or otherwise inappropriate for an educational setting.

4.2. Academic Integrity

- Copilot should not be used to engage in academic dishonesty, including plagiarism, cheating, or any other unethical academic practices.

4.3. Unauthorised Activities

- Users must not attempt to gain unauthorised access to Copilot or any other systems or networks.
- Modifying or tampering with Copilot's settings or functionality is prohibited.

5. Consequences of Misuse

Violations of this Acceptable Use Policy may result in disciplinary actions, including but not limited to:

- Loss of access to Copilot.
- Detention, suspension, or expulsion for students.

6. Reporting Violations

Users are encouraged to report any violations of this policy to a teacher or administrator. Reports will be handled confidentially and investigated promptly.

7. Policy Review

This Acceptable Use Policy will be reviewed and updated periodically to ensure it remains relevant and effective in promoting responsible use of Copilot in an educational setting.

Appendix D: IA Risk Assessment

(Based on the ICO AI Risk Assessment Toolkit)

REF	CONTROL	ACTION REQUIRED	COMPLETE?	COMMENTS
1.	Conduct a DPIA.	Complete the DPIA and ensure this is signed off by the DPO/SIRO/AI Board.	Choose an item.	
2.	Assign technical/operational roles/responsibilities and provide clear direction and support on use of AI and application of DPA.	A) Appoint a senior owner to drive accountability.	Choose an item.	
		B) Operational procedures, guidance and manuals to support AI use and compliance with DPA are in use.	Choose an item.	
3.	Document each purpose for using personal data at each stage of AI lifecycle and keep purpose computability under review.	A) Provide clear transparency information to inform individuals on outset of use in privacy notice.	Choose an item.	
		B) Complete data flow mapping exercise and ensure a lawful basis is identified.	Choose an item.	
4.	Record how you will facilitate individual rights requests throughout lifecycle of AI system.	A) Personal data in IA system will be indexed and retrievable in response to individual rights requests.	Choose an item.	
		B) Consider user testing to ensure privacy information is effective.	Choose an item.	
5.	Data flow process must include meaningful human review before a final decision is made.	Changes made to AI output via human intervention must be recorded.	Choose an item.	
6.	Document clear criteria and lines of accountability for the labelling of data.	A) Clear data labelling should be in place.	Choose an item.	
		B) Training manuals and guidance should be in place for data labelling.	Choose an item.	
7.	Test if AI system produces similar outcomes for individuals who have different protected characteristics.	A) Measure different types of AI output error.	Choose an item.	
		B) Ensure test dataset is adequate.	Choose an item.	

Appendix E: Data Protection Impact Assessment (DPIA)

Basic Version v3.2

FOR ARTIFICIAL INTELLIGENCE SOLUTIONS ONLY

This assessment template complies with the latest requirements as set out by the Information Commissioners Office (ICO) and the UK General Data Protection Regulations.

Background Information

Project Name	**Project Purpose**
Current Information Asset Owner (IAO)	**Current System Administrator**

Target Implementation Date	Click here to enter a date.

Assessment Completed By:

Name	
Job Title	
Contact Number	
Email Address	
Project/Business Role	
DPIA Approved By (AD or SDM)	

Date Assessment Completed	Click here to enter a date.

Assessment Information

1. What personal / special category (sensitive) information will be processed as part of this project?

Mark all categories that apply *(click box in end column)*

Personal Information	Name	☐
	Address (includes post code)	☐
	Date of birth	☐
	Personal email address	☐
	Personal phone number	☐
	Financial details	☐
	Unique identifiers, e.g., customer ref. number, IP address, cookies, NHS number, etc., (give details below)	☐
Special Category	Physical/Mental Health	☐
	Ethnic Origin	☐
	Religion/Philosophical Beliefs	☐
	Criminal record (includes ongoing proceedings)	☐
	Trade union membership	☐
	Sexual life (including orientation)	☐
	Political opinion	☐
	Genetic and biometric information	☐

2. What unique identifiers will be processed?

Ref	Requirement	Response
3	What is the intended outcomes for the individuals whose data you are processing and the wider society?	
4	What alternatives to using AI have been investigated and why has it been decided not to use them?	
5	What impact will there be on the individuals whose data are being processed?	a) What is the allocative harm: result of decision to allocate goods/opportunities among a group? b) What is the representational harm: processing reinforces subordination of groups along identity lines, e.g. stereotyping?
6	Describe the processing of personal data. This should include: • A description of the processing activity • Data flow diagrams • Stages when AI processes personal data and makes automated decisions • Explains the margin of error in the performance of the system which may affect fairness • Description of the scope and context of processing • Number of data subjects whose information will be processed • Source of data to be processed • Extent to which individuals are likely to expect processing	
7	What human involvement is involved in the decision-making process and at what stage does this take place?	
8	Who is the data controller/joint data controller and processor and what are roles for each?	

9	What stakeholder consultation has taken place including consulting with individuals whose data will be processed?	
10	Have all the processing purposes for the personal identifiable information (PII) been identified? What are the purposes?	
11	How will the PII be collected and how are individuals made aware of what information is being collected and for what purpose, e.g., privacy notice.	
12	What conditions in Articles 6 (for personal information) and 9 (for special category / sensitive personal data) are you applying to process the PII? See Appendix A.	
13	If you are relying on consent to process PII how will this be collected and recorded and what is the process to handle withdrawn consent?	
14	Who will have access to which sets of PII?	
15	What measures are in place to ensure PII is only available to those with a legitimate need to access it?	
16	What technical and organisational measures are in place to protect access to PII?	
17	Does any system used to process PII have the facility to amend/delete data?	
18	What processes are in place to check the accuracy/quality of PII being processed?	
19	If marketing is involved are individuals given the option to opt out of further marketing?	
20	What process for ensuring adequate training and instructions are in place for staff to know how to operate the system and process PII?	

21	Will PII be transferred off-site from Council premises? If so, where (what country) and how?	
22	Does data processed have a retention policy in place and the system being used have the facility to delete PII where necessary?	

Trade off analysis – privacy vs benefits

Harm to individual rights and freedoms	Benefits to individuals/wider society

Identification, Assessment and Mitigation of Risks

REF	Risk Description	Likelihood of harm	Severity of harm	Overall risk	Mitigation	Effect on risk/ Residual risk

Any risk that cannot be mitigated must be reported to the ICO by the Audit & Governance.

KEY:

Likelihood of harm – remote, possible or probable
Severity of harm – minimal, significant or severe
Overall risk – low, medium or high
Effect on risk – eliminated, reduced or accepted
Residual risk – low, medium or high

DPIA Sign Off

IG Sign Off By		**Date**	

To be signed off by Information Governance Team

Appendix A

Article 6 - Lawfulness of processing conditions for PII

6(1)(a) – Consent of the data subject

6(1)(b) – Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract

6(1)(c) – Processing is necessary for compliance with a legal obligation

6(1)(d) – Processing is necessary to protect the vital interests of a data subject or another person

6(1)(e) – Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

6(1)(f)* – Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject

** Note that this condition is not available to processing carried out by public authorities in the performance of their tasks.*

Article 9 - Lawfulness of processing conditions for special category PII

9(2)(a) – Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law

9(2)(b) – Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement

9(2)(c) – Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent

9(2)(d) – Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent

9(2)(e) – Processing relates to personal data manifestly made public by the data subject

9(2)(f) – Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity

9(2)(g) – Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards

9(2)(h) – Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional

9(2)(i) – Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices

9(2)(j) – Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)

Document Version Control

Version	Date	Author	Sent To	Comments
1.1	23/8/17	R Montgomery	ICT	Version incorporates SB comments
1.2	29/8/17	R Montgomery	Information Security Group	Includes LB comments
3	10/11/22	R Montgomery	Corporate - intranet	Updates include addition of risk section
3.1	8/11/23	R Montgomery	IDT and Anthea Lowe	Updated to make it specific to AI processing
3.2	26/6/24	R Montgomery	Corporate	Updated version pushed to the intranet