St Chad's Academies Trust

AI Acceptable Use Policy

Children first: in the footsteps of St. Chad

As we follow Christ in the footsteps of St. Chad, we seek to be servant leaders who have a desire to see all those, within our Trust family, truly flourish both spiritually and academically

Document information

Document title	AI Policy		
Owner	Compliance		
Version	1.0	Status Pending	FINAL
Last updated	04 June 2026	Last updated by	Trust Compliance Officer
Approved on	29 June 2026	Effective from	01 July 2026
Review Date	01 July 2028		
Purpose	This policy applies to acceptable use of AI by all users within St Chad's Academies Trust.		
The policy has been implemented in line with statutory practice, with the Trust DPO and Chief of Operations, and the Trust Finance, Risk and Audit Committee (the 'Committee'), and may be amended from time to time, following further consultation with the Committee and/or Trust Board.			
This policy links to:	GDPR Policy Data Retention IT Acceptable Use Disciplinary Policy Complaints Policy Understanding and Quantifying AI Risk AI Principal Statement Public Sector Equality Duty Equality Act 2010 ICO Age-appropriate design code		

Contents

1. Table of Substantive Changes
2. Introduction
3. Aims and application
4. Purpose
5. Scope
6. Policy Statement
7. Data Protection implications of using AI
8. Ethical Use of AI

Appendix 1 Permitted tool and prohibited uses
Appendix 2 AI Incident reporting form

1. Table of substantive changes from previous versions:

This table explains where we have made substantive changes, for your ease of reference and assurance.

Date	Section Amended

2.0 Introduction

2.1 St Chad's Academies Trust ('the Trust') is committed to ensuring that it provides a strong infrastructure to enable our academies to flourish and improve. The Trust recognises that its leaders and colleagues are central to this success and greatly values their commitment and contribution.

2.2 The core values of the Trust form the basis of all discussions with colleagues. We expect all colleagues of St. Chad's Academies Trust to respect and model these values.



3 Aims and application

3.1 St Chad's Academies Trust recognises that Artificial Intelligence (AI) technology is already widely used in both commercial and everyday applications, and its influence is anticipated to grow exponentially, impacting almost all industries and job sectors including education.

3.2 Whilst AI was typically used by specialists to complete a specific task, it has become a widely used tool in a short period of time that is more accessible in a range of disciplines. In particular, the growth in Generative AI has led to new opportunities to use AI tools. Generative AI is a rapidly evolving and increasingly freely available technology, which can generate new writing, audio, codes, images and video simulations. Whilst this offers opportunities for staff in enhancing efficiency, decision-making and service delivery, it also increases risk.

3.3 This policy establishes the expectations for the responsible and effective use of all AI in St Chad's Academies Trust by users.

3.4 By embracing AI technology, we aim to:

- Support colleagues to manage their workload more efficiently and effectively.
- Prepare pupils for a future in which AI technology will be an integral part.
- Use AI to promote fairness in education by supporting the work to bridge learning and accessibility disparities; and
- Ensure value for money in our services by maximising efficient processes using available technology.

3.5 St Chad's Academies Trust needs to ensure that the use of AI is organised and controlled in a manner which will be beneficial to the safety of individuals and groups of people and is in alignment with applicable laws and regulations as outlined on page 2.

3.6 St Chad's Academies Trust recognises that this is a rapidly developing area and like many other organisations, will need to continually review and adapt practice to changes in technology. We are committed to exploring the opportunities offered by AI technology. This policy will be regularly reviewed to ensure that it remains relevant and applicable in practice. The Trust recognises that it is important to provide early appropriate guidance and advice to colleagues, to encourage users to be transparent about the use of AI, and to support a culture of responsible AI use as these rapid changes take place.

4 Purpose

4.1 The purpose of this policy is to ensure users are aware of the controls and methods in place to manage the use of AI. Users are expected to comply with the policy to ensure that AI tools are used appropriately. There are a number of other relevant policies which this policy links with, including the Trust Data Protection, Trust Information Security, and Trust ICT Acceptable Use policies. This policy is supplementary to existing policies and should be read in conjunction with them.

5 Scope

5.1 This policy applies to the use and configuration of all AI tools that have either been provided by the Trust as part of general IT tools available to staff such as Microsoft Co-pilot/Chat GPT /Google Gemini, other AI tools, which may be available for free or on a subscription basis and directly accessed by users via the internet, or procured by the Trust for a specific use.

5.2 These rules apply when using all academy/trust-owned devices which may be used for academy/trust business.

5.3 This policy applies to all colleagues, agency staff, contractors, volunteers, apprentices, and student/work experience placements who have access to these tools, described as "users" within this document. All users are responsible for reading and understanding this policy before using any AI technology.

6 Policy Statement

6.1 Appendix 1 to this policy sets out which AI tools are permitted, and which are expressly not permitted. Users are permitted to explore and utilise the listed permitted AI-based tools and technologies to assist in managing their work, but this use is subject to the restrictions in this and related policies. Users must not use the prohibited tools or use AI for the prohibited uses listed in the annex.

6.2 Examples of business tasks that users may use AI for include suggesting drafting improvements to documents, call transcription, summarisation of large or specialist documents, translation, drafting of communications materials, content creation, reviewing materials for accessibility.

6.3 Examples of teaching tasks that users may use AI for include lesson planning, marking, adapting materials, report writing i.e. annual reports giving due attention to personal data that should not be included, and plans to ensure they are accessible to all pupils, timetabling, monitoring IT and online activity for safeguarding purposes and attainment tracking.

6.4 All users of AI will comply with applicable laws, regulations, policies, and guidelines including those relating to intellectual property, copyright, data protection, safeguarding, and formal assessment including the guidance given by the Joint Council for Qualifications (JCQ) or individual Exam Board requirements.

6.5 All users of AI will recognise that the technology is rapidly evolving and will be committed to adapting ways of working, as necessary and will engage with AI training facilitated by the academy and Trust as directed.

6.6 Users will be transparent about their use of AI technology so that the Trust understand where and how AI is used.

6.7 Users will not rely on AI to replace strategic decision making or rely on it to make decisions that could have a significant impact on people.

6.8 Users remain professionally responsible and accountable for the quality and content of any output generated by AI, however generated or used and should rely on their expertise to ensure that they review and tailor any AI output.

6.9 Users should refer to appendix 1 for the tools that are permitted and should complete the GDPR training that is set through the Trust compliance system (Smartlog). Users also have a responsibility to identify any additional training, and development needs to ensure they adhere to this policy and should raise these with their line manager.

6.10 Users should be aware of procedures for any potential data breach and ensure the Trust Data Protection Officer is informed at DPO@stchads.uk if they identify an issue or risk, equally, Safeguarding issues should be referred to the Designated Safeguarding Lead and Trust Data protection officer.

6.11 User should be aware that improper use of AI tools or failure to comply with the AI acceptable use policy could result in disciplinary action, in line with Trust policy and procedures.

7 Data Protection implications of using AI

7.1 Users should be aware that any information entered into some AI models may no longer be private or secure. Users must not enter any information containing personal data, intellectual property or private information (including confidential information, such as contracts) into any AI model without checking whether it is permitted to do so.

7.2 Users who wish to utilise new AI tools or new AI functionality within existing tools must follow the Trust Data Protection Policy and Data Protection Impact Assessment Procedure, support for this can be obtained from the Trust Data Protection Officer. Users should be aware that it is not always easy to recognise when AI tools are processing personal data, and they should not presume that no processing is taking place.

8 Ethical use of AI

8.1 The use of AI systems, in particular Generative AI, will be carried out with caution and an awareness of their limitations. Users should be mindful of the following considerations:

8.1.2 **Bias** - data and information generated by AI will reflect any inherent biases in the data set accessed to produce it. This could include content which may be discriminatory based on factors such as race, gender, or socioeconomic background. Users must ensure they follow the requirements of the Equality Act 2010.

8.1.3 **Accuracy** – information may be inaccurate when generated so any content should be fact-checked. Tools may provide highly plausible and coherent results but may still contain errors.

8.1.4 **Human oversight-** a lack of human intervention may result in AI outputs going unchecked. Users should ensure that outputs align with societal values, and users should be aware that Generative AI lacks flexibility, human understanding, and compassion.

8.1.5 **Currency** – some AI models only collate data prior to a certain date so content generated may not reflect the most recent information.

8.1.6 **Environmental issues** - use of AI requires energy to run. Therefore, it should only be used when relevant, appropriate and proportionate, where it is the most suitable and sustainable option.

8.1.7 **Reputational** - trust in our systems and relationships with stakeholders may be harmed if we do not demonstrate our commitment to ensuring they are not harmed by our use of AI.

Appendix 1

Category 1 Permitted AI Tools approved for all data

Tool Category	***Example Tools***	***Approved Use Cases***
Generative AI	*ChatGPT Enterprise, Claude for Business, Google Gemini for Workspace*	*Drafting internal memos, Knowledge-sharing/ scoping, summarising non-sensitive meetings.*
Productivity	*Microsoft 365 Copilot, Google Workspace AI*	*Email drafting, spreadsheet formulas, PowerPoint creation.*
Specific	*GitHub Copilot (Enterprise), Cursor (Pro)*	*Boilerplate code, debugging, unit tests (using internal repos only).*
Search/Research	*Perplexity Pro, Webb (AI Search)*	*Market research, technical documentation lookup.*

Category 2 Restricted (Conditional use only)

Tool Category	***Example Tools***	***Approved Use Cases***
Free-Tier Chatbots	*Free Chat GPT or Free Claude*	Permitted for general learning or creative prompts that contain **zero** company information.
Creative Design tools	*Midjourney, Canva magic media, Adobe firefly*	Permitted for marketing concepts but avoid uploading real pupil and employee faces.
Translation tools	*DeepL, Google translate*	Permitted for general text; prohibited for sensitive legal contracts unless using a Pro/Business account.

Category 3 Prohibited

Tool Category	***Example Tools***	***Approved Use Cases***
Non-vetted browser extensions	*Any AI Assistant*	*Any "AI Assistant" Chrome/Edge extension that asks for "read/write" access to your browser data without IT approval.*
Unauthenticated Wrappers	*Third part websites*	*Third-party websites that "wrap" ChatGPT (e.g., "https://www.google.com/search?q=FreePDFSummarizer.com") as they often scrape your uploaded files.*
Shadow AI	*Private AI*	*Any AI tool purchased on a personal credit card and used for work tasks without being logged in the company's software registry.*
Deepfake/Impersonation Tools	*AI that Clones*	Tools used to clone voices or faces of colleagues or pupils unless for a specific, pre-approved marketing campaign.

Prohibited uses

The following uses are prohibited:

- AI systems designed to deceive, coerce or influence human behaviour in harmful ways.
- AI tools that prey on an individual's vulnerabilities, such as age, disability, or socio-economic status.
- Emotion recognition within the workplace or educational settings.
- AI systems that use AI for 'social scoring' where scores are assigned to individuals based on their behaviour, affecting access to services, employment or other opportunities.
- Biometric categorisation based on sensitive biometric attributes such as race.
- Real-time biometric identification in publicly accessible spaces for law enforcement purposes.
- AI used to predict criminal offences solely based on profiling or assessing personality traits.

Appendix 2

AI Incident Reporting Form

Reporter information

Full Name	
Position	
Contact Information	
Academy	

Incident details:

Date and time of incident	
Location/platform where the incident occurred	
Description	
What happened?	
How was it discovered?	
Who is affected	

Type of AI incident (please tick):

☐ Data breach

☐ Biased decision-making

☐ Malfunctioning algorithm

☐ Unauthorised access

☐ Non-compliance with school AI principles

☐ Harmful output

☐ Potential misuse of AI by a student or staff member

☐ Other (please specify)

Impact assessment:

- What is the immediate impact of the incident?

- What, if any, potential long-term impacts do you foresee?

- How many individuals are affected?

Response actions taken:

- What immediate actions have been taken in response to the incident?

- Have you notified or told anyone else about this incident (e.g., IT department, DPO, Trust Headteacher, RHL?)

- Have you informed the vendor of the issue, or do you consider that the vendor should be notified?

- If necessary, have any systems been isolated or shut down?

Documentation:

- Are there any logs, error messages, or other documentation related to the incident? (attach any appropriate documentation to the reporting form)

Additional information/comments:

- Is there any other information that might help in the investigation and resolution of this incident?

Confirmation and submission:

Signature:

Date: