



Signhills Academy

Use of Artificial Intelligence (AI) Policy

Approved by:	Headteacher	Date: Summer 2026	Version: 1
Next review:	Summer 2027 (or earlier if DfE guidance is updated)		

USE OF ARTIFICIAL INTELLIGENCE (AI) POLICY

1. PURPOSE AND SCOPE

1.1 This policy sets out how Signhills Academy uses artificial intelligence (AI) as a professional tool to improve the quality of our work, reduce unnecessary workload, and meet our compliance obligations, while ensuring that human judgement, professional accountability, and the safety of our pupils remain at the centre of everything we do.

1.2 It reflects the DfE's first statutory AI guidance for schools, published June 2025 and updated August 2025, which affirms that AI, used safely and effectively, can transform education by helping teachers focus on what they do best: teaching.

1.3 Our guiding principle: AI is a tool that amplifies professional expertise. It compresses time spent on research, drafting and compliance checking, so that staff expertise goes where it adds most value: in classrooms, with children, and in professional decision-making. The professional remains accountable for every output.

1.4 This policy applies to all staff, governors, and volunteers who use AI tools in connection with their role at Signhills Academy. It covers generative AI chatbots and tools (such as Claude, ChatGPT, Microsoft Copilot, Google Gemini, KeyGPT, and similar), as well as AI-assisted features embedded in software the school already uses.

1.5 Statutory basis: DfE Generative AI in Education (updated August 2025); DfE Generative AI Product Safety Standards (updated January 2026); DfE AI Training Modules 1–4 (June 2025, Module 3 updated May 2026); DfE Leadership Toolkit (June 2025); Online Safety Act 2023; UK GDPR; Data Protection Act 2018; Data (Use and Access) Act 2025; KCSIE 2025; Equality Act 2010.

2. WHAT WE MEAN BY AI

2.1 Generative AI refers to tools that create new content (text, images, plans, summaries) based on a prompt and/or standing instructions. These tools are trained on large volumes of data and generate responses that can seem authoritative but may be inaccurate, biased, or out of date. This is known as **hallucination**.

2.2 Two categories of tool are relevant to our work:

Tool Type	Key Characteristics
Open AI tools	Accessible to anyone. May store, share or learn from data entered into them. Must never be used with identifiable personal data.
Closed / enterprise AI tools	Commercially licensed tools with contractual data protections (e.g., school-approved platforms). Offer greater security but still require professional checking of all outputs.

3. LEGISLATIVE AND REGULATORY FRAMEWORK

3.1 This policy reflects and complies with the following:

Source	Relevance to This Policy
DfE: Generative AI in Education	Policy paper updated August 2025. Sets out principles for safe, effective and responsible use.
DfE Product Safety Standards	Updated January 2026. Standards for filtering, monitoring, security, data protection, IP, governance, and four additional areas: cognitive development, emotional and social development, mental health, and manipulation.
KCSIE	In force from 1 September annually. See section directing schools to DfE generative AI guidance and product safety standards.

Online Safety Act 2023	Requires generative AI services to conduct risk assessments for content harmful to children, and to use age assurance.
UK GDPR / DPA 2018	Identifiable pupil, staff or parent data must not be entered into open AI tools.
Data (Use and Access) Act 2025	Royal Assent 19 June 2025. Introduces 'children's higher protection matters'; strengthened requirements for meaningful human oversight of automated decision-making.
Equality Act 2010	Section 149 imposes the PSED. AI outputs must be checked for bias as a legal obligation, not simply good practice.
AI Regulation White Paper	Five regulatory principles: safety and robustness, transparency, fairness, accountability, and contestability.
ICO AI and ADM Code	SI 2026/425 (in force 12 May 2026). School will review final code when published.
DfE Filtering & Monitoring	Filtering and monitoring must cover generative AI access. Annual review required.
DfE Cyber Security Standards	All approved AI tools must be compatible: regular patching, MFA, role-appropriate access controls.
DfE Modules 1–4	Foundation knowledge (M1), practical guidance (M2), safe use including 'Need, Read, Proceed' (M3, updated May 2026), use cases and FACTS framework (M4).
DfE Leadership Toolkit	For school leaders: audit tool, safety and opportunity planning, embedding AI in digital strategy.

4. HOW WE USE AI AT SIGNHILLS

4.1 At Signhills Academy we have adopted a Human-Centred Design approach to AI. This means we start from a clear human need, e.g. saving professional time, improving accuracy, strengthening compliance, and we choose AI tools that serve that need. The tool serves the professional; the professional never serves the tool.

4.2 We distinguish between two modes of use:

Mode	What it means in practice
Augmentation (primary use)	AI compresses time spent on research, drafting and cross-referencing. The professional applies their expertise to review, refine and sign off the output.
Automation (not our approach)	AI performs the task with no meaningful human review. Not acceptable for any task where professional judgement, safeguarding or legal compliance is involved.

4.3 Approved Tools and Use Cases

4.3.1 The headteacher maintains an **Approved AI Tools Register** (Appendix 1) listing each tool, its type (open or closed), permitted uses, and which roles may use it. A companion **Role-Based Use Case Framework** (Appendix 5) maps approved and prospective use cases to specific staff roles, with a status key and recommended next steps. These registers are living documents managed by the headteacher and updated independently of this policy.

4.3.2 Broad categories of approved use include: policy and compliance work; annual pupil reports (see Appendix 3 for the full protocol); administrative communications; curriculum planning and assessment resource creation; SEND and SEMH support frameworks; staff development materials; and research and synthesis. No identifiable personal data may be used in any category.

4.4 The Human Remains Accountable

4.4.1 Whatever tools or resources are used, the professional who produces, signs off or shares any document bears full responsibility for its accuracy, appropriateness and compliance. AI-generated content is a starting point, never a finished product.

4.4.2 Before any AI-assisted output is used, the responsible staff member must:

- verify accuracy against authoritative sources (e.g., gov.uk, HSE, KCSIE)
- check for bias, hallucination or context errors — bias checking against the nine protected characteristics is a legal obligation under the Equality Act 2010 (PSED)
- check for jigsaw identification: even where no name is used, a combination of characteristics can narrow to a single identifiable pupil
- apply their professional judgement to the content
- be able to explain and defend the document if challenged by governors, Ofsted, or parents

5. DATA PROTECTION AND PRIVACY

5.1 AI data protection compliance is a legal obligation under UK GDPR, the Data Protection Act 2018, and the Data (Use and Access) Act 2025. Staff must understand these requirements before using any AI tool.

5.2 Core Rules

- Identifiable personal data about pupils, staff, parents or governors must never be entered into open generative AI tools.
- This includes names, dates of birth, SEND status, medical information, behaviour records, or any combination that could identify an individual (jigsaw identification).
- Approved closed tools may be used with data only where a DPIA has been completed and the DPO has confirmed compliance.
- Any use of AI for automated decision-making must be transparent and compliant with ICO guidance.
- Data protection and intellectual property are distinct legal obligations. Both must be checked.
- Pupils own the copyright of their own work. Uploading pupil work into an AI system that trains on it infringes their IP rights.
- Apply the DfE's 'Need, Read, Proceed' approach before entering data into any AI tool.

5.3 Account Setup

5.3.1 Staff who set up accounts on AI tools for school use must register using their school Google email address. This provides a minimal audit trail. It does not make an open tool a closed one — data protection rules apply regardless.

5.4 Data Breach

5.4.1 If identifiable personal data is entered into an unauthorised AI tool, this will be treated as a data breach. Staff must report any suspected breach to the headteacher immediately.

5.5 Good Practice for AI Prompting

- Work from anonymised or hypothetical examples
- Reference legislation and guidance, not individual cases
- Add specific school context manually after the AI has produced a draft
- Use the DfE's FACTS prompting framework (Focus, Audience, Context, Task, Style)

5.6 Tool Approval Checklist

5.6.1 Before any AI tool is added to the approved register, the headteacher must verify it meets the following criteria:

Criterion	What to check
Data terms	Data is not used to train the model; prompts are not reviewed by humans; activity is not used for model improvements; data is not shared with other users.
Security	Compatible with DfE Cyber Security Standards. MFA, role-appropriate access, regularly patched, resistant to jailbreaking.
Stated purpose	The tool clearly states its intended use case. Claims supported by evidence. Changes communicated.
Governance	Clear risk assessment. Formal complaints mechanism. UK GDPR and DUAA 2025 compliance demonstrated.
Learner-facing (additional)	Content filtering, real-time monitoring with DSL alerts, ability to suspend, age assurance (OSA 2023), DUAA children's higher protection matters, non-expert-readable monitoring reports.

6. SAFEGUARDING

6.1 The use of AI introduces safeguarding risks that must be addressed alongside existing online safety provisions. The DSL is responsible for monitoring these risks and updating training accordingly.

6.2 KCSIE explicitly directs schools to the DfE's generative AI guidance and requires filtering and monitoring arrangements to address AI.

AI tools must not be used in connection with any safeguarding concern, welfare note, CPOMS entry, or child protection documentation, whether or not the child is named. Even anonymised descriptions may enable jigsaw identification.

6.3 Known AI Safeguarding Risks

- AI-generated CSAM: generative AI can create or manipulate sexual images of children. UK legislation criminalises this.
- Deepfakes and image manipulation: realistic fake images or videos of pupils, staff or others.
- AI-enabled grooming: realistic AI avatars and chatbots can simulate human conversation.
- Extremist and radicalisation content: AI can generate synthetic propaganda at scale.
- AI-generated phishing and scam communications targeting school staff or parents.
- Pupils using AI to fabricate communications or images appearing to originate from the school.
- Over-reliance by pupils: AI provides answers rather than explanations, bypassing deeper learning.

6.4 Safeguarding Responsibilities

6.4.1 Any safeguarding concern arising from AI use must be reported to the DSL immediately. The DSL will keep abreast of emerging threats, ensure filtering and monitoring covers AI tools, update annual safeguarding training, and liaise with the headteacher and DPO where AI risks intersect with data protection.

7. ROLES AND RESPONSIBILITIES

7.1 Governing Board

- Holds the headteacher to account for safe, effective AI use and receives an annual update on AI use and any policy amendments.

- Uses only approved AI tools; follows data protection rules at all times. May use approved tools for governance legislation research, scrutiny question frameworks, and briefing paper drafts — no personal data.
- Must ensure governor minutes drafted with AI assistance are fully anonymised before content enters a prompt.

7.2 Headteacher

- Leads day-to-day oversight of AI use across the school. Maintains the approved tool register and signs off on any new tools or use cases.
- Commissions DPIAs before adopting any AI tool involving personal data. Reviews and updates this policy at least annually.
- Ensures all staff complete required DfE training modules before using AI tools. Uses the DfE Leadership Toolkit audit tool. Monitors the ICO's statutory AI and ADM code of practice.

7.3 Data Protection Officer (DPO)

7.3.1 The DPO (Tim Pinto, contactable via the Academy Business Manager) monitors and advises on data protection compliance, including AI use. The DPO must be consulted before any new AI tool involving personal data is adopted.

7.4 Designated Safeguarding Lead (DSL)

Monitors and responds to AI-related safeguarding risks. Keeps filtering and monitoring systems under review in relation to AI tools. Updates staff safeguarding training to address AI risks. Escalates safeguarding incidents involving AI in line with KCSIE.

7.5 All Staff

7.5.1 All staff are encouraged to use approved AI tools to reduce workload and improve the quality of their professional outputs. Before using any AI tool, staff must complete the required training (Section 8). In all AI use, staff must:

- use only approved tools listed in Appendix 1 and register using their school Google email address
- apply the 'Need, Read, Proceed' approach before entering any data and use the FACTS prompting framework to structure prompts effectively
- ensure no identifiable personal data is entered into open AI tools
- fact-check and critically review all AI outputs before use
- acknowledge AI assistance when sharing substantially AI-drafted documents
- report safeguarding concerns to the DSL and data concerns to the headteacher or DPO

8. STAFF TRAINING

8.1 The DfE has published a four-module training programme for school staff, available free via gov.uk. All staff must complete Modules 1 and 2 before using AI tools. Modules 3 and 4 are recommended for all staff. The DfE Leadership Toolkit is required for the headteacher and SLT. Class teachers using the Claude Project report workflow must read the Annual Report Writing Guide (Appendix 3) in full before use.

Training Resource	Who and Why
Module 1: Understanding AI	For all staff. What AI is, how it works, using AI alongside professional expertise. Required before any AI use.
Module 2: Interacting with AI	For all staff. Practical guidance on using generative AI tools effectively, checking outputs, understanding limitations.

Module 3: Safe Use (updated May 2026)	Recommended for all. Five risk areas: safeguarding, ethics, data protection, IP, academic integrity. Includes 'Need, Read, Proceed'.
Module 4: Use Cases	For all staff. Approved use case categories, FACTS prompting framework, case studies.

8.2 All staff must read this policy in full before using any AI tool for work purposes. The Chartered College of Teaching offers a free certified AI assessment; staff are encouraged to complete this as part of CPD.

9. ETHICAL USE AND INTELLECTUAL PROPERTY

9.1 We apply the five regulatory principles from the DfE and AI Regulation White Paper:

Principle	How we apply it
Safety and robustness	We use only tools that are secure and safe. We anticipate risks including misuse and hacking.
Transparency	We are open about our use of AI. Staff do not present AI-generated material as entirely their own unaided work.
Fairness	We check AI outputs for bias, particularly against the nine protected characteristics (PSED legal obligation).
Accountability	Professional responsibility rests with the staff member who produces or signs off the output.
Contestability	Staff are empowered to overrule, discard or correct AI suggestions at any time.

9.2 Staff and governors must not use AI tools to: impersonate, bully or harass any person; generate offensive, discriminatory or inappropriate content; produce content that could facilitate harm to children; or make decisions about individual pupils without appropriate human review.

9.3 Most generative AI tools are trained on data submitted by users. Content entered into open tools may be used to train AI models. Confidential school documents, unpublished curriculum materials, or content owned by third parties must not be entered into open AI tools without appropriate authorisation. Pupils own the intellectual property rights to original content they create; staff must not use pupils' work to train AI models without appropriate written consent.

10. PUPILS AND AI

10.1 Signhills Academy does not currently use generative AI tools directly with pupils. This is a deliberate position based on the DfE's advice that evidence on pupil-facing AI use is still emerging, the age restrictions carried by most tools, the significant safeguarding and developmental risks, and the children's higher protection matters introduced by the DUAA 2025.

Embedded AI in approved learning tools — important distinction: Some school-approved online learning tools (such as Nessy) incorporate AI features as part of their core design. These have been procured through normal approval processes, operate within closed, age-appropriate environments, and are governed by their own data protection controls. Their use is not restricted by this policy.

10.2 If pupil-facing AI is ever considered, the DfE Product Safety Standards and DUAA 2025 require assessment of cognitive development (risk of deskilling), emotional and social development, mental health, and manipulation (persuasive or addictive design). Any future pupil-facing AI tool requires headteacher sign-off, DPO and DSL advice, a full DPIA, and demonstration the tool meets the high bar in Section 5.6.

10.3 All pupils benefit from developing an informed understanding of AI as part of a knowledge-rich curriculum. Staff will incorporate age-appropriate discussion of what AI is, how it works, its limitations, and its implications for society into relevant areas of the curriculum. The school recognises that pupils increasingly have access to AI tools at home; teachers will

address this through age-appropriate conversations and communication with parents. Further guidance is in the homework policy.

11. CONCERNS, MONITORING AND REVIEW

11.1 Staff and governors are encouraged to raise concerns about any proposed or actual use of AI with the headteacher. The school will not penalise staff for raising concerns in good faith.

11.2 Breach of this policy by staff will be managed in line with the staff code of conduct and may result in disciplinary action. Breach by governors will be managed in line with the governor code of conduct. Parents, carers or pupils who believe AI use has resulted in unfair treatment may raise this through the school's standard complaints procedure.

11.3 AI technology evolves rapidly. This is a live policy document. The headteacher will update it whenever there is a significant change to DfE guidance, material change in how AI is used at school, a safeguarding or data protection incident involving AI, or a significant change to the legislative landscape.

11.4 The governing board will receive an annual report on AI use, compliance, and any incidents.

12. LINKS WITH OTHER POLICIES

12.1 This policy should be read alongside: Data Protection Policy; Child Protection and Safeguarding Policy; Online Safety Policy; ICT Acceptable Use Policy; Staff Code of Conduct; Equality Policy; Behaviour Policy; Curriculum Policy; Homework Policy; and the KS2 Assessment Policy (which sets out the use of AI in curriculum assessment).

A1. APPROVED AI TOOLS REGISTER

This register is maintained by the headteacher and updated independently of this policy. Open tools must only be used for tasks requiring no personal data. Staff must use their school Google email when registering.

Tool	Type	Approved Uses	Approved For
KeyGPT	Closed	Letters, job descriptions, interview questions, policy drafting, research, governor support	Teachers, Governors, Admin
Oak National AI	Closed	Lesson planning	Teachers, HLTAs
National College AI	Closed	Lesson planning, resource creation, research	Teachers, HLTAs, TAs
Claude (claude.ai)	Open*	Policy drafting, compliance research, admin communications, annual reports (anonymised — Appendix 3), SDP drafts, Ofsted prep. No personal data.	HT, SLT, Class teachers (reports)
Microsoft Copilot	Open*	Document drafting, summarising, email composition. Not on school licence — treat as open tool.	All staff
Google Workspace AI	Closed	Document drafting, summarising, email composition within school Google tenancy	All staff

* **Open tools:** no identifiable personal data may ever be entered. All outputs must be critically reviewed. School Google email required for registration.

A2. GDPR COMPLIANCE REFERENCE

Use Case	GDPR Position
Annual pupil reports	No personal data enters the AI tool. Pupils identified by number only. Real names added manually in Word. AI is not a personal data processor under this workflow.
Policy and compliance drafting	No personal data used. Prompts reference legislation and guidance only.
Admin communications	No PII in open tools. Template letters drafted without identifiable information; personalised manually.
Curriculum planning	No personal data used. Plans drafted at year group and subject level. IP: copyrighted materials must not be uploaded.
SENCo provision planning	No personal data. Anonymised frameworks only. All pupil-specific detail added manually. Jigsaw identification risk applies.
Governor governance support	No personal data. Scrutiny questions and briefing drafts contain no named individuals. Minutes must be fully anonymised.
Multilingual communications	No personal data. Generic parent letter templates only. Translation quality verified by competent speaker.

A3. USE CASE GUIDE — ANNUAL PUPIL REPORTS

A3.1 Overview

A3.1.1 Each teacher creates a private Claude Project. Into this project they upload the school report template and five anonymised example reports from their own previous writing. When drafting a report, the teacher writes notes about the child using a number as the pupil identifier and states gender. Claude produces a narrative draft. The teacher edits it, then replaces the number with the real name in Word only — never inside the AI tool.

A3.2 What Must and Must Not Go into the AI Tool

Category	Detail
Must go in	Anonymised example reports (no real names, SEND or medical info). Teacher notes using a number as identifier. Factual observations about learning, attitude and progress.
Must never go in	Real pupil names. DOB. SEND status, EHCPs or support plans. Medical or mental health information. Family circumstances. Safeguarding information. Any combination enabling jigsaw identification.

A3.3 Editing Checklist

- Read the full draft aloud. Does it sound like you?
- Are all facts accurate? Did Claude include anything you did not provide?
- Are pronouns correct throughout?
- Does the report address parents and carers — not the pupil?
- Is the tone warm, professional and consistent with your other reports?
- Check for bias: does the language treat all pupils equitably (PSED)?
- Replace the pupil number with the child's real name in Word.
- Add any SEND, medical or pastoral context deliberately excluded from the prompt.
- Final check: would you be happy for this report to go home as it stands?

A3.4 GDPR Compliance Basis

A3.4.1 The AI tool is not a personal data processor under this protocol. No personally identifiable information enters the tool at any stage. Entering a real pupil name, SEND status, medical information or any identifying detail constitutes a data breach and must be reported immediately.

A4. USE CASE GUIDE TEMPLATE (FOR FUTURE GUIDES)

When the headteacher approves a new AI use case, a guide following this structure should be completed:

Section	Content
Use case	Describe the task: what is being produced, for what purpose, by whom
Tool	Name of approved tool and its type: open/closed
Who this applies to	Role(s): must have completed DfE Modules 1–3 and read this guide before use
Workflow overview	Step-by-step from prompt to final output. Reference the FACTS framework.
What goes in	List permissible information in prompts
What must never go in	Categories of data that must never be included — including jigsaw identification combinations
Checking and sign-off	What must be checked before use — including PSED bias checking — and who signs off
GDPR position	Personal data processed? Lawful basis? DPIA required? DUAA 2025 implications?
IP considerations	Any IP considerations relevant to this use case
Date approved	Date — approved by: Headteacher

A5. APPROVED USE CASES BY STAFF ROLE

A5.1 This appendix maps approved and prospective AI use cases to specific staff roles. It applies the Human-Centred Design approach: AI serves a clearly identified human need, compresses professional time, and the professional remains accountable for every output. The no-PII constraint is absolute throughout.

A5.2 Status Key

Status	What it means
Currently approved	Listed in the approved uses register (Appendix 1). A use case guide exists or is in preparation.
Lower risk	No PII risk and limited compliance complexity. Suitable for formal approval with HT sign-off.
Needs protocol	Valid use case with identified risks requiring a use case guide before approval.
HT sign-off required	Sensitive content, compliance obligations, or proximity to PII. Requires DPIA, DPO advice, full guide.

Full role-based use case tables for Headteacher/SLT, Class Teachers, SENCo/ELSA/Learning Mentors, HLTAs/TAs, Administration Staff, Governors, and Cross-School Use Cases are maintained as a working supplement to this appendix. See the headteacher for the current version.

A5.3 Recommended Next Steps

#	Action	Who	Priority
1	Formally approve lower-risk use cases and add to registers	Headteacher	High
2	Commission SENCo use case guide with jigsaw identification and PSED guidance	HT with SENCo	High
3	Produce prompt framework guide for HLTAs and TAs	Headteacher	Medium
4	Add governor AI use note to induction materials	HT / Clerk	Medium
5	Draft multilingual communications protocol	HT with DPO	Medium
6	Develop position statement on pupil AI use outside school	HT with teachers	Medium
7	Commission use case guides for SEF, website, assessment, governor minutes	HT with DPO	Lower

This appendix does not constitute approval of any use case not already listed as 'Currently approved'. All uses marked 'Lower risk', 'Needs protocol' or 'HT sign-off required' remain unapproved until formally signed off.