



Safe Use of Artificial Intelligence (AI) Policy

Safe, secure and responsible use of AI in our work

Version 1.1 · 27/09/2026

1. Purpose and principles

This policy sets out how Swale Tutoring Service uses Artificial Intelligence (AI) safely, securely and responsibly. It is deliberately proportionate to a small provider delivering one-to-one SEMH tuition, and is principle-based rather than tied to a single product.

Our principles are:

- Protect the information of pupils, families, staff and the company at all times.
- Comply with UK data protection law.
- Use AI to support human work, never to replace professional or safeguarding judgement.
- Keep a person accountable for every decision and every piece of AI-assisted output.
- Be alert to inaccurate, biased or inappropriate AI-generated content.

2. Scope

This policy applies to the Director, the Designated Safeguarding Lead and Deputy DSL, all tutors, contractors, volunteers and anyone else acting on behalf of Swale. It covers all use of AI tools when carrying out Swale business, in any setting.

3. Which AI tools may be used

Swale does not ban AI — it uses approved AI tools as part of normal business, including Anthropic's Claude (through its business/Cowork environment) and Microsoft 365 Copilot. Rather than name a single permitted product, we apply a standard that any tool must meet before it is used for Swale business:

- It is a business or enterprise service operating under a data-processing agreement (DPA) that does not use our data to train its models. Anthropic's commercial services and Microsoft 365 both meet this and are approved.
- It has been approved by the Director for the intended use.

Free or consumer AI tools that do not offer a DPA (for example the free tiers of ChatGPT, Google Gemini, and similar) must not be used for any Swale business that involves personal, confidential or safeguarding information.

4. Data protection — what must never be entered into any AI tool

Regardless of the tool, staff must not enter the following into AI unless there is a specific, documented and lawful reason approved by the Director:

- Information that identifies a pupil or family member — names, date of birth, address, telephone number, email.
- Special-category data — health, SEND or EHCP detail, or other sensitive personal information.
- Safeguarding information, or any detail of a concern, disclosure or investigation.
- Financial account details, passwords, access codes or security credentials.

- Information that is legally privileged or subject to a confidentiality restriction.

Where AI is used to help with pupil-related work, use de-identified or generic information (for example, describe a need or task without naming the child). This policy is read alongside the Data Protection (GDPR) and Data Breach policies.

5. Safeguarding

Safeguarding is our highest priority and remains an entirely human responsibility. Staff must never:

- Use AI to make, or to influence, a safeguarding or welfare decision.
- Use AI to assess or screen a risk to a child.
- Allow AI to communicate directly with a pupil without human oversight.
- Use AI to build behavioural profiles or assumptions about pupils.
- Rely on AI-generated content when identifying or responding to a concern about a child.

Every safeguarding matter is handled by appropriately trained staff in line with the Safeguarding & Child Protection Policy.

6. Human oversight and accuracy

All AI output is reviewed by a person before it is used. The user — not the tool — remains responsible for accuracy, professional judgement, compliance and the final decision. Staff must:

- Fact-check anything important, and verify figures, references and sources.
- Correct errors before anything is shared or relied upon.
- Check that content is appropriate for the age and ability of the pupil.
- Treat AI output as a draft to be checked, never as automatically correct, and stay alert to bias.

7. Acceptable uses

- Drafting and improving written communications and documents.
- Creating lesson materials and resources using non-identifiable content.
- Summarising notes, and supporting research and planning.
- Administrative and operational support, including approved automation (see section 8), always with human oversight.

8. Automation and connected tools

Swale may use AI within automated workflows (for example, help triaging or summarising incoming email). Any such automation must be risk-assessed and approved by the Director before use, must use only DPA-covered services, must exclude identifiable safeguarding content from external processing wherever possible, and must keep a person in the loop for any action that affects a child or family. No automated system takes a safeguarding action on its own.

9. Unacceptable uses

- Entering any of the prohibited data in section 4 into an AI tool without approval.
- Using a non-approved or consumer AI tool for Swale business involving personal or confidential information.
- Using AI to make safeguarding, recruitment or other decisions about individuals.
- Generating misleading, deceptive, discriminatory or offensive content, or fabricating records.
- Bypassing security controls, or using AI for personal purposes during working time unless authorised.

10. Transparency

We are open with families and commissioners that we use approved AI tools for administrative and preparatory support under this policy, and that AI is not used to make decisions about a child.

11. Monitoring and review

The Director may monitor the use of approved AI tools. Breaches of this policy are handled under the company's disciplinary and data-protection procedures, and a breach involving personal data is managed under the Data Breach Policy. This policy is reviewed annually, or sooner as AI tools, the law or DfE guidance change.

Approved by Shelley Wilson, Director & Designated Safeguarding Lead.
Version 1.1 · Approved 27/09/2026 · Reviewed annually.