UNICORN SCHOOL

AI POLICY

Parents may read this policy on the public section of the website.

RESPONSIBILITY

Staff Member: Head of Teaching and Learning

Last Updated:	**April 2026**
Next Review:	**April 2027**

Aims:

The aim of this policy is to give some guidelines around the rapidly evolving world of the use of AI in schools. It is our intention to review this initial policy every term to ensure it remains relevant. The school's approach to AI education and digital literacy is aligned with the National Curriculum for Computing, which aims for pupils to become digitally literate, able to use technology safely and to evaluate and apply information technology responsibly. The school also follows the DfE's guidance on teaching online safety within existing subjects and the DfE's guidance on using generative AI safely and effectively, including protecting personal data and recognising that AI outputs may be inaccurate or biased. Since our pupils are not yet at an age to be able to use AI directly, the guidelines apply to the adults who teach and support them.

Guiding principles:

1. The intention to integrate AI tools into our practice comes from our commitment to enhance students' learning experiences and foster skill development.
2. The use of AI is strategically employed as a supplemental tool to support and expand upon classroom instruction.
3. Teachers will ensure their pedagogical, behavioural and pastoral knowledge is complemented and not undermined by AI tools.
4. AI will not replace direct instruction or teacher interaction but will serve as an additional resource to enrich the educational experience.

1. Introduction

Purpose: To provide a holistic framework for the integration and management of AI in educational settings, encompassing: ethical compliance; educational enhancement; workload reduction; data security; and innovation, whilst ensuring the safeguarding and protection of our students are at the heart of what we do at Unicorn. In line with the Department for Education's (DfE's) guidance on the use of generative artificial intelligence in education, the school recognises the DfE's expectation that all schools develop their own local policies to ensure AI is used safely, ethically and effectively within their individual context. This policy therefore sets out our school specific approach to managing opportunities, risks, governance arrangements and safe practice in accordance with national guidance. This policy is part of a wider digital ecosystem (Acceptable Use Policy, Safeguarding Policy, Curriculum & Education Policy) - specific approach to managing opportunities, risks, governance arrangements and safe practice in accordance with national guidance.

This policy applies to all staff, students and stakeholders.

2. Definitions

AI: Artificial Intelligence, including machine learning, natural language processing (NLP), and large language models (LLMs).
LLM: Large language models, such as ChatGPT, which have generative capabilities. Generative AI outputs may be incorrect, hallucinated or biased and require verification.

NLP: Natural language processing such as Alexa / Siri - differs from the above and has fewer opportunities for bias and hallucination.

Image generation from LLM: Images can be created via text prompts which can be inappropriate or subject to bias.

DPO: Data Protection Officer

DSL: Designated Safeguarding Lead

DPIA: Data Protection Impact Assessment

KCSIE: Keeping Children Safe in Education (DfE, 205)

Stakeholders: Teachers, students, parents, administrative staff and external partners.

3. Objectives

1. **Educational Enhancement:** To improve teaching and learning outcomes.
2. **Ethical Compliance:** To ensure ethical and legal use of AI.
3. **Data Security:** To protect the privacy and data of all stakeholders.
4. **Workload Reduction:** To utilise AI to reduce the administrative and academic workload of staff.
5. **Innovation:** To remain at the forefront of education by integrating AI to enhance and supplement the school's mission to best support young people.
6. **Protection:** To protect pupils from online harms associated with AI technology (in line with KCSIE 2025).
7. **Equity and Inclusion:** To ensure AI use does not disadvantage vulnerable learners

4. Ethical Use of AI

4a. Respect for Intellectual Property

AI technologies being used are properly licensed and respect intellectual property laws. We respect copyright and intellectual property when using generative AI outputs (e.g. not passing off generated images or text as original without proper disclosure).
Before using any AI tool, all staff should consult the Head of Teaching & Learning to ensure it is approved for educational use.

4b. Transparency and Disclosure

In accordance with the DfE's guidance on the use of generative artificial intelligence in education, staff must clearly and openly label any material that has been created, adapted or meaningfully influenced by AI.

All documents, reports, communications, planning resources or teaching materials that incorporate AI-generated content must include an explicit note indicating AI assistance, ensuring transparency and maintaining professional accountability. Staff remain fully responsible for verifying the accuracy, appropriateness and educational suitability of all AI-supported outputs before use.

Periodic checks by the Head of Teaching & Learning are to ensure transparency measures are consistently applied.

4c. Avoiding Bias and Discrimination

The school will conduct an annual review of all AI tools to identify and mitigate potential bias, ensuring fair and equitable outcomes across protected characteristics. This review will be carried out by the designated AI Lead (Head of Teaching & Learning) in collaboration with the DSL and DPO, reflecting the DfE's expectation that schools actively monitor risks associated with generative AI, including bias, fairness and discriminatory outputs. Findings from this review will be recorded, reported to the governing body and used to inform updates to the school's AI register and safeguarding practices.

4d. Respect for Personal Data and Privacy

All AI tools that process or have the potential to process personal data must undergo a formal Data Protection Impact Assessment (DPIA) prior to approval and use within the school. The DPIA must assess data flows; storage; security measures; risks to children and compliance with GDPR; and safeguarding requirements, as reflected in the school's wider data protection and privacy policies. No pupil data - including names; photographs; videos; behavioural information; academic records or any other identifiable or sensitive information - may be entered into any AI tool unless that tool has been explicitly approved through the

DPIA and vetting process and added to the school's approved tools register (see Appendix 1 & 3). Staff must use only those AI tools that have passed this process and must report any accidental entry of personal data into non-approved AI systems as a data-protection incident in line with school procedures. (see Appendix 2 for Staff "Quick Guide")

5. Workload Reduction

While AI may be used to support staff in reducing administrative workload - such as generating lesson ideas, planning prompts or draft classroom resources - teachers retain full professional responsibility for all materials produced with AI assistance. In line with national guidance and sector best practice, staff must carefully review, verify and adapt any AI generated content to ensure accuracy, appropriateness and alignment with the school's curriculum and safeguarding expectations.-generated content to ensure accuracy, appropriateness and alignment with the school's curriculum and safeguarding expectations.

AI must not be used to write pupil reports, assessment feedback or professional communications unless the teacher has personally reviewed and meaningfully edited the content and its use is clearly and transparently disclosed. Under no circumstances may AI be used to generate unreviewed or unlabelled feedback or reports as accountability for all outputs remains with the member of staff.

6. Responsible Use

6a. Accuracy & Fact-Checking

All AI generated content used for planning, resources, communication or professional tasks must be independently reviewed and verified by the member of staff using it. In line with the DfE's guidance, staff must recognise that generative AI systems may produce inaccurate, misleading or fabricated information and therefore professional judgement must always prevail. Under no circumstances may AI outputs be used without critical evaluation for factual accuracy, curriculum relevance and safeguarding appropriateness.-generated content used for planning, resources, communication or professional tasks must be independently reviewed and verified by the member of staff using it. In line with the

6b. Compliance With Laws & Regulations

All staff must ensure that any use of AI complies with applicable laws and school policies including GDPR; safeguarding requirements; acceptable use policies; intellectual property regulations; and DfE expectations on safe and responsible AI use. Staff must only use AI tools that have been formally approved through the school's vetting and DPIA process. Any uncertainty about legal or regulatory compliance must be escalated to the DPO, DSL or Head of Teaching & Learning before use.-use policies-property regulations

7. Safeguarding

AI tools may introduce or amplify safeguarding risks including: impersonation; deepfakes; online grooming; bullying; harassment; manipulation of images; and exposure to inappropriate content. In accordance with KCSIE-aligned safeguarding practice, staff must report any AI-related safeguarding concerns immediately to the DSL. The DSL will maintain a record of all AI-related safeguarding incidents, monitor emerging risks and incorporate these into ongoing child-protection procedures and whole-school safeguarding training.

8. Data Management

All AI-related data handling must comply with GDPR and the school's Data Protection Policy. Only AI tools that have undergone a completed and approved DPIA may process any category of personal data. Staff must not input pupil information - including names; images; videos; behavioural notes; or any other identifiable data - into AI tools unless the tool appears on the approved register and has been formally risk-assessed. Any accidental entry of personal data into a non-approved AI system must be reported immediately as a data-protection incident.

9. Implementation Plan

The school will adopt a phased implementation of AI tools, beginning with controlled pilot use, risk assessments and staff training. Rollout of any new AI tool will only occur once risks have been evaluated, safeguarding implications have been reviewed and staff have received appropriate training in safe, ethical and educationally effective use. This approach reflects DfE guidance emphasising risk assessment, gradual adoption and informed staff practice.

10. Accountability

Responsibility for AI governance within the school is shared across designated leadership and safeguarding roles. The Headteacher provides strategic oversight; the DPO oversees data protection and DPIAs; the DSL monitors safeguarding risks; and the Head of Digital Learning maintains the approved tools register and provides staff training. All staff remain individually accountable for their use of AI and all AI-related incidents - including misuse, data concerns and safeguarding issues - must be logged and escalated through the appropriate reporting channels including CPOMS, DSL, DPO and Head of Teaching & Learning.

11. Review Cycle

This policy will be formally reviewed annually, with interim reviews conducted termly to assess: new risks; tool performance; safeguarding implications; and updates in national

guidance. The governing body and Senior Leadership Team will receive a summary of AI-related incidents, training outcomes and tool-register updates as part of ongoing oversight. Regular review reflects DfE expectations that AI use in schools must remain dynamic, risk-responsive and continually evaluated in line with emerging technologies and safeguarding requirements.

12. Pupils, Parents & Staff

Pupil Education (Digital Literacy, AI Awareness & Manipulated Media)

The school will embed age appropriate digital literacy and AI awareness within the existing Computing curriculum, PSHE and online safety provision so that pupils develop the foundational skills needed to navigate a digital world safely. In line with the National Curriculum for Computing, pupils will learn to use technology safely and respectfully, understand that online information may be unreliable and begin to evaluate digital content using critical thinking strategies. This will include introducing pupils to the idea that some online text, video, audio or images may be AI generated or manipulated and that such content may be misleading or harmful, reflecting expectations set out in the DfE's *Teaching Online Safety in Schools* guidance. Pupils will also be supported to recognise manipulated or synthetic media and understand simple "pause and check" methods to evaluate trustworthiness, in line with the DfE's 2025 emphasis on misinformation, disinformation and digital harms within safeguarding guidance.-appropriate digital literacy and AI awareness within the existing Computing curriculum, PSHE and online-safety provision so that pupils develop the foundational skills needed to navigate a digital world safely. In line with the National Curriculum for Computing, pupils will learn to use technology safely and respectfully, understand that online information may be unreliable and begin to evaluate digital content using critical thinking strategies. This will include introducing pupils to the idea that some online text, video, audio or images may be AI-generated or manipulated and that such content may be misleading or harmful, reflecting expectations set out in the DfE's

Parent Communication and Transparency

The school is committed to maintaining clear, accessible communication with parents regarding the use of AI and digital tools within the school environment. A parent-friendly summary of the school's AI approach will be published annually (from 2026/27), supported by guidance from the DfE on safe and effective generative AI use in schools.

Consequences and Accountability for Misuse

To maintain a safe and compliant digital environment, the school will apply clear and proportionate accountability measures for misuse of AI or digital technologies. Misuse includes but is not limited to, providing pupil personal data to unapproved AI systems, using non-sanctioned tools for school business or using AI outputs without appropriate verification. These requirements reflect the DfE's expectations for responsible use of generative AI and

the data-protection safeguards required in educational settings. All suspected incidents must be reported promptly through established channels and recorded in accordance with school procedures, as recommended in national guidance on AI-related data-protection risks. The school will distinguish between accidental errors and negligent or deliberate misconduct; however, repeated or serious breaches may lead to disciplinary action under the Staff Code of Conduct, especially where safeguarding or data-protection implications arise.

Staff-Friendly Guidance and Training

To ensure consistent and confident practice, the school will maintain a concise AI “Quick Guide” for staff (see Appendix 2), outlining approved tools, prohibited uses, verification procedures, data-minimisation expectations and reporting pathways. This guide will form part of staff induction and refresher training and will align with DfE guidance on safe and effective use of AI in education, which emphasises risk awareness, transparency and accuracy checking. Staff will receive ongoing training to consolidate understanding of data-protection duties related to AI, including the need to verify outputs, ensure transparency and safeguard pupils’ personal data - reflecting DfE and ICO expectations for compliant use of generative AI in schools. This centralised and user-friendly guidance is intended to support staff workload while ensuring that professional judgement remains at the heart of all AI-supported activity.

Risk Mitigation and Responding to AI Failures or Harm

The school recognises that AI systems can generate inaccurate, unsafe or biased outputs and will therefore implement a structured risk-mitigation and incident-response approach. Staff must never treat AI as an authoritative source and must verify all outputs for factual accuracy, appropriateness and safeguarding suitability, consistent with DfE advice on the inherent risks and limitations of generative AI. Any problematic or harmful output - such as discriminatory, misleading or inappropriate content - must be withdrawn immediately, reported and investigated following internal safeguarding or data-protection procedures, reflecting national expectations for responsible oversight and error-handling. Escalation will occur where an incident may constitute a safeguarding concern, potential data breach or repeated accuracy issues. These incidents will be documented and reviewed to identify emerging risks, inform staff training needs, and adjust approved-tool configurations where necessary.

Appendix 1: Use of Microsoft Copilot and Other Approved Closed-System AI Tools

1. Approved Use of Microsoft Copilot for Microsoft 365 (Education Tenant)

Microsoft Copilot for Microsoft 365 (Education) is an approved AI tool at Unicorn School for use by staff in accordance with this policy. Copilot operates entirely within the school's secure Microsoft 365 Education tenant and inherits the platform's built-in GDPR protections, encryption, access controls and compliance framework. Copilot does not use school data to train public AI models and all processing takes place within the school's organisational environment.

Because the school has completed a DPIA for Copilot, implemented appropriate governance arrangements, and ensured technical safeguards and correct configuration, staff *may enter pupil personal data into Copilot* where this is necessary for a legitimate educational or administrative purpose and where doing so complies with the principles of data minimisation, purpose limitation and safeguarding.

Pupil data must only be processed in Copilot when all of the following conditions are met:

- The staff member is logged into their school Microsoft 365 account.
- The processing relates directly to a legitimate school purpose.
- Only the minimum necessary pupil data is entered.
- The staff member reviews and verifies all outputs before any use.
- No Copilot output is shared outside the school's safeguarded systems unless permitted under the Data Protection Policy.
- The task does not replace professional judgement, in line with DfE expectations on AI in education.

2. Prohibited Uses

Even with DPIA approval, staff must not:

- Input *excessive or irrelevant* pupil data beyond what is needed for the task.
- Use Copilot to make sole or automated decisions about pupils.
- Use Copilot via any personal account, public web interface, or unmanaged device.
- Use Copilot (or any AI tool) to generate *unreviewed* assessment feedback or reports.

These restrictions align with GDPR's fairness, accountability and non-automated decision-making requirements and with school-level AI data-protection frameworks.

3. Other GDPR-Appropriate Closed-System AI Tools

Some AI tools may be considered GDPR-appropriate when they operate inside a secure, school-controlled environment; inherit the organisation's security and privacy standards; and do not use school data for model training.

These tools may only be adopted following:

(1) a completed DPIA,
(2) a data-processing agreement,
(3) vetting and sign-off by the DPO and DSL, and
(4) entry onto the school's approved AI tools register."

Other closed AI features embedded within approved educational platforms:
(e.g. AI analytics within the school's MIS (Engage), or teacher-facing AI suggestions within a vetted LMS) may be approved if their data processing remains within the school's controlled ecosystem and after DPIA review.

4. Reporting and Oversight

- Any concerns, errors, or suspected incorrect data handling in Copilot must be reported immediately to the DPO and DSL.
- The DPO maintains oversight of Copilot's data-processing arrangements, conducts periodic audits, and reviews compliance with GDPR and safeguarding duties.
- The DSL monitors any AI-related safeguarding implications, reflecting KCSIE-aligned AI governance practice.
- Copilot is included in the school's annual AI tools review, including bias, accuracy, and safeguarding risk assessments.

Appendix 2: Unicorn School – Staff Quick Guide to AI Use

What AI tools can I use?

- When connected to the school network or using a school device, all AI use must be for work purposes only. Staff should use Microsoft Copilot and any other school-approved AI tools, all of which operate within our secure Microsoft 365 education tenant and meet DfE data protection expectations.
- Personal use of AI tools is permitted but only on personal devices and personal accounts and must not involve any school-related information including pupils, staff, data, documents, or lesson materials.
- Public AI platforms (e.g. ChatGPT, Google Gemini) must not be used for any work-related activity unless the school has explicitly approved a managed, secure version of the tool.
- Some educational platforms (e.g. Kahoot!, Wayground) may include AI features — these may be used only if the platform itself has already been approved by the school.

---

2. What data can I input?

- Pupil data must never be entered into any AI tool except Copilot, which has a completed DPIA and is protected within the school environment.
- Always follow data minimisation: only input what is strictly necessary.
- If you accidentally enter personal data into an unapproved tool, report immediately to the Data Protection Officer (DPO) or the Head of Teaching & Learning.

---

3. How should I use AI safely and professionally?

- AI can help with ideas, drafts, resources, admin tasks, and workload reduction — but you remain responsible for the final output.
- Always check accuracy, ensure content is age-appropriate, and review for bias or safeguarding concerns.
- Never use unedited AI output in reports, feedback, or communications.
- Label clearly whenever AI has meaningfully influenced what you produce.

---

4. Safeguarding: what should I watch for?

- AI can generate or amplify risks such as fake images, impersonation, bullying, grooming, or misinformation.
- Report any AI-related safeguarding concern immediately to the DSL.
- Pupils should not use generative AI in school — but they may encounter it at home. Encourage them to speak up if something online worries them.

---

5. What happens if AI goes wrong?

- If an AI tool produces incorrect, biased, unsafe or inappropriate content:
    1. Stop using the output immediately.
    2. Replace/withdraw the material.
    3. Report issues to the relevant lead (Head of T&L / DSL / DPO).

- AI is a support tool, not a dependency — always be ready to revert to non-AI methods.

---

6. When should I report?

Report immediately if you notice:

- Potential data-protection issues,
- Unapproved AI use,
- Safeguarding concerns involving AI (deepfakes, impersonation, bullying),
- Inaccurate or harmful AI outputs.

Use the usual channels: CPOMS / DSL / DPO / Head of Teaching & Learning as appropriate.

---

7. Key principles to remember

- Verify everything.
- Disclose AI use.
- Protect pupil data.
- Prioritise safeguarding.
- Use only approved tools.

Appendix 3: Approved AI tools

Tool Name / Platform	Tool Type / Function	Approved Use Cases / Educational Purpose	Age Group / Pupil Involvement	Personal Data Input Allowed?	DPIA Status	Safeguarding Risks Considered	Risk Level	Restrictions / Prohibited Uses	Approver(s)	Date Approved	Review Cycle / Next Review	Notes / Conditions
Microsoft Copilot (M365)	Generative AI (text & image) inside secure tenant	Staff planning, drafting, admin efficiency, resource creation	Staff only	Yes, within M365 only (data minimised)	DPIA completed	Accuracy errors; bias; safeguarding risks; misinformation	Medium	Not for automated decisions; not for unreviewed reports	HT, DPO, DSL	27.02.26	Annual	Must be accessed via school account only
Kahoot!	Quiz platform with optional AI features	Classroom quizzing, retrieval practice	Staff + pupils (quiz participation only)	No pupil data input into AI features	Not required (no AI data processing)	Misuse of AI-generated questions; inappropriate content	Low	AI question-generation disabled unless approved	Head of T&L	27.02.26	Annual	Must only be accessed with school Microsoft accounts
Wayground (formerly Quizizz)	Educational platform with limited AI suggestion tools	Classroom quizzing, retrieval practice	Staff + pupils (quiz participation only)	No pupil data to be entered	Not required (teacher-facing only)	Inaccurate content; bias	Low	Not for generating reports or assessment comments	Head of T&L	27.02.26	Annual	Must only be accessed with school Microsoft accounts
Gamma	Generative AI (presentations, documents, visuals)	Staff-facing use only for drafting presentations, slide decks, visuals, training materials	Staff only	**No** pupil personal data allowed	DPIA completed	Inaccurate content; bias; risk of inappropriate image generation	Medium	Not to be used for reports, assessments, parent communications, or decision-making; no uploads of pupil images/work	HT, DPO, DSL	27.02.26	Annual	Must only be accessed with school Microsoft accounts