

NANTWICH PRIMARY ACADEMY & NURSERY

PRINCIPAL - SUE SPENCE

Use of Artificial Intelligence (AI) in School Policy



PAGE: 1 of 14 ISSUE: Four DATE: September 2026 REVIEW: September 2027
--

Approved by: [To be confirmed]

Nantwich Primary Academy & Nursery
Manor Road, Nantwich, Cheshire, CW5 5LX
Tel - 01270 902055
nantwichoffice@sbmat.org

Policy Information and Revision History

This September 2026 revision substantially updates the academy's existing AI policy to reflect current safeguarding, data protection, digital standards and Department for Education guidance. It is intended to support safe, purposeful innovation while keeping professional judgement and the best interests of pupils at the centre of all decisions.

DATE	DETAILS	SIGNATURE
01.07.2023	Policy created	L Bebbington
17.11.2023	Policy updated	L Bebbington
25.01.2025	Policy updated	L Bebbington
09.09.2026	Comprehensive review and update for 2026-27, including KCSIE 2026, DfE AI guidance and product safety standards, data protection, filtering and monitoring, pupil-facing AI and current academy arrangements.	L Bebbington

Related academy and Trust policies

- Child Protection and Safeguarding Policy
- Online Safety Policy
- Acceptable Use and Remote Learning Policy
- Data Protection Policy and privacy notices
- Staff Code of Conduct
- Behaviour and Anti-Bullying Policy
- SEND Policy and Equality duties
- SBMAT IT, cyber security and procurement procedures

Policy status

This revision should be approved through the academy's normal policy process before publication. Operational lists, such as the approved AI tools register, may be updated between policy reviews without requiring a full rewrite of this policy, provided the changes remain within the controls set out here.

Contents

- Purpose
- Scope
- Definitions
- Key principles
- Roles and responsibilities
- Use of AI by staff
- Use of AI by pupils
- Teaching AI literacy
- Safeguarding and online safety
- Data protection and privacy
- Accuracy, bias and human oversight
- Assessment, feedback and pupil work
- SEND, inclusion and accessibility
- Copyright and intellectual property
- AI-generated images, audio and video
- Approved tools, procurement and risk assessment
- Cyber security, filtering and monitoring
- Transparency and communication
- Incident reporting and response
- Training and support
- Monitoring, evaluation and review
- Appendix 1: Practical AI use framework
- Appendix 2: AI tool approval checklist
- Appendix 3: Glossary
- Appendix 4: References and guidance

Purpose

Nantwich Primary Academy recognises that artificial intelligence (AI), including generative AI, can support teaching, learning, accessibility, creativity and efficient administration. Used well, it can help staff create high-quality resources, explore ideas, reduce repetitive workload and give pupils carefully designed opportunities to understand technologies that will shape their future.

AI also introduces significant risks. These include inaccurate or fabricated information, bias, inappropriate content, over-reliance, loss of independent thinking, privacy and data protection concerns, intellectual property issues, cyber security risks, manipulation, impersonation and AI-generated harmful content. This policy establishes clear expectations so that AI is used lawfully, ethically, safely and in the best interests of pupils.

The academy adopts a positive but controlled approach: AI may assist people, but it does not replace professional responsibility, safeguarding judgement, human relationships or the need for pupils to think, practise and learn for themselves.

Scope

This policy applies to all staff, pupils, governors, volunteers, contractors and visitors using AI in connection with academy activity. It applies to school-owned devices, school accounts, personal devices used for school work, third-party educational technology, AI features built into existing software, and any direct or indirect pupil-facing use of AI.

The policy covers generative AI systems that create or transform text, images, audio, video, code or other content, as well as AI-supported analytics, adaptive systems, automated decision tools, chatbots and other AI-enabled services.

Definitions

- Artificial intelligence (AI): systems designed to perform tasks that normally require aspects of human intelligence, such as recognising patterns, making predictions, generating content or responding to language.
- Generative AI: AI that creates new content, such as text, images, music, audio, video, code or combinations of these.
- Pupil-facing AI: any AI system a pupil interacts with directly, whether through a chat interface, adaptive learning platform, creative tool or AI feature embedded in another service.
- Personal data: information relating to an identified or identifiable person. This includes pupil, staff and parent information and may include prompts, uploaded files, images, audio and chat histories.
- Approved tool: an AI-enabled product or service that the academy and/or Trust has considered appropriate for a stated use. Approval may be limited to specific users, data types or activities.

Key principles

Child-centred and safeguarding first: The welfare, safety, rights and developmental needs of pupils take priority over convenience, novelty or efficiency.

Human responsibility: A member of staff remains accountable for professional decisions and for any output used in teaching, assessment, communication or administration.

Purposeful use: AI should be used only where it adds clear educational or operational value. It should not be used simply because it is available.

Protect thinking and learning: AI must not routinely do the thinking that pupils need to learn to do themselves. Pupil-facing use should support explanation, questioning, practice, feedback and reflection rather than provide complete answers by default.

Privacy by default: Personal, confidential or sensitive information must not be placed into unapproved AI systems. Data use must be lawful, transparent, proportionate and minimised.

Accuracy and fairness: AI output is not assumed to be correct, neutral or unbiased. It must be checked and adapted by a competent human before use.

Inclusion and accessibility: AI should increase access and opportunity, not create new barriers or discriminatory outcomes. Reasonable adjustments and SEND provision remain human-led.

Transparency: The academy will be open about material uses of AI, particularly where AI affects pupils, processes personal data or contributes to significant decisions.

Security and accountability: AI tools must be used within academy and Trust cyber security, filtering, monitoring and procurement arrangements.

Review and learning: AI develops rapidly. The academy will review practice, incidents, emerging risks and new guidance regularly and adjust controls when needed.

Roles and responsibilities

Principal / Senior Leadership Team (SLT):

- sets the academy's overall approach to AI and ensures that use is aligned with safeguarding, curriculum, data protection and Trust expectations;
- approves significant or pupil-facing AI use and ensures appropriate governance oversight;
- ensures staff understand this policy and that concerns are acted upon.

Designated Safeguarding Lead (DSL):

- leads safeguarding responses to AI-related concerns, disclosures, harmful content, grooming, exploitation, self-harm, sexual content, bullying, impersonation and deepfakes;
- reviews relevant monitoring information and ensures urgent concerns are escalated through established safeguarding procedures;
- contributes to risk assessment of pupil-facing AI tools.

Computing Lead / Vice Principal (L Bebbington):

- supports staff with safe and effective AI practice and coordinates the academy's operational approach;
- maintains or coordinates the approved AI tools register with SLT and relevant Trust teams;
- supports curriculum development in AI literacy and provides or coordinates staff guidance;
- reports technical, safeguarding or data concerns to the appropriate lead rather than attempting to resolve matters outside the scope of the role.

SBMAT IT Support Team and Data Protection Officer (DPO):

- provide technical, cyber security, filtering, monitoring and data protection advice;
- support due diligence, contracts, privacy assessment and DPIAs where required;
- manage relevant central systems, including Jamf and filtering/monitoring provision. Jamf is centrally managed by SBMAT IT, with the Computing Lead retaining academy-level administrator access for appropriate local device management.

All staff:

- use AI only within this policy and any related Trust guidance;
- protect personal and confidential information;
- check AI-generated content before use and retain professional responsibility for the final outcome;
- report safeguarding, data, cyber security or conduct concerns immediately through the correct route.

Use of AI by staff

Staff may use approved or permitted AI tools to support professional work where the use is proportionate, secure and does not weaken professional judgement. Appropriate examples can include:

- brainstorming lesson ideas, questions, examples and explanations;
- creating first drafts of non-sensitive teaching resources, quizzes, model texts and accessibility adaptations;
- rewriting generic material for different reading levels or formats;
- supporting planning, organisation and routine administration;
- drafting generic communications which are then checked and personalised by staff;
- creating or editing non-identifiable images, audio, code or other educational content;
- summarising non-confidential information and helping staff explore options or alternative approaches.

Staff must apply the following controls:

- AI-generated material must be checked for factual accuracy, curriculum suitability, age appropriateness, bias, tone, accessibility and safeguarding implications before use.
- Staff must not present AI output as authoritative simply because it is fluent or confident.
- AI may assist with professional tasks, but the member of staff remains responsible for the final resource, message, judgement or decision.
- Staff must not enter identifiable pupil, parent, staff, safeguarding, medical, SEND, behaviour, attainment or other confidential information into a public or unapproved AI tool.

Nantwich Primary Academy and Nursery
Use of Artificial Intelligence (AI) in School Policy

- Commercially sensitive, confidential Trust information, passwords, security details, unpublished assessment materials or information covered by legal privilege must not be entered into unapproved AI systems.
- Staff should not upload copyrighted or licensed material, including substantial extracts from commercial schemes, books or assessment resources, unless the school has the right to do so and the AI service's terms permit it.
- AI-generated code, formulas, scripts or technical instructions must be reviewed before being run on school systems. High-risk technical changes must be referred to SBMAT IT.

Use of AI by pupils

Nantwich Primary Academy is a primary setting. Many general-purpose AI services have minimum age requirements or are not designed for independent use by younger children. Pupils must not create personal accounts for general-purpose AI services for school activity unless the specific service, account arrangement and educational use have been explicitly approved.

Direct pupil use of AI is permitted only when all of the following are satisfied:

- the activity has a clear educational purpose;
- the tool is approved for the pupil age group and intended use;
- the provider's age requirements and terms are met;
- appropriate filtering, moderation and monitoring safeguards are in place;
- pupils use school-managed accounts or a teacher-mediated approach where appropriate;
- staff provide suitable supervision and pupils know how to report anything worrying or inappropriate;
- the task is designed so that AI supports learning rather than replacing the pupil's own thinking.

Unless specifically approved as part of an educational activity, pupils must not:

- use AI to complete work that is intended to show their own knowledge, understanding or skill;
- submit AI-generated work as their own;
- enter personal information about themselves or others into AI tools;
- upload photographs, recordings or identifying information about pupils or staff to AI services;
- attempt to bypass safeguards, filters, age restrictions or moderation;
- use AI to bully, threaten, impersonate, sexualise, embarrass or deceive another person;
- create or share harmful deepfakes, fake accounts, cloned voices or misleading synthetic media;
- use AI companionship, relationship or emotionally persuasive chatbots that have not been specifically approved for a bounded educational purpose.

Teaching AI literacy

The academy will teach pupils, at an age-appropriate level, that AI systems are tools rather than people and that generated responses can be inaccurate, biased, persuasive or inappropriate. AI literacy will be developed through Computing and, where relevant, other curriculum areas.

Pupils should learn to:

- understand in simple terms what AI and generative AI can and cannot do;
- question where information comes from and verify important claims using trusted sources;
- recognise that fluent AI output can still be wrong or fabricated;
- understand that AI can reflect bias or stereotypes;
- protect personal information and respect the privacy of others;
- recognise synthetic or manipulated media and understand the risks of deepfakes and impersonation;
- acknowledge when AI has materially helped with a task where this is required;
- know that AI cannot replace trusted adults, teachers, friends, family or professional support;
- know how and when to stop an interaction and seek help from an adult.

Safeguarding and online safety

All AI use must align with Keeping Children Safe in Education 2026, the academy's Child Protection and Safeguarding Policy and the Online Safety Policy. AI-related safeguarding concerns are safeguarding concerns and must be treated with the same urgency as concerns arising through any other route.

Risks considered by the academy include:

- harmful, sexual, violent, extremist, self-harm or otherwise inappropriate generated content;
- grooming, exploitation or unsafe contact facilitated through AI-enabled systems;
- deepfakes, image manipulation, voice cloning, impersonation and sexualised synthetic content;
- AI-generated misinformation, scams and persuasive or manipulative content;

- pupils disclosing personal, emotional or safeguarding information to conversational systems;
- over-anthropomorphising AI, emotional dependency, excessive use or systems that attempt to prolong engagement;
- content or interactions that undermine real-world support networks or encourage secrecy;
- bias, discrimination or harmful stereotyping;
- cognitive offloading where pupils rely on AI instead of developing essential knowledge and skills.

Where a pupil encounters harmful content, makes a concerning disclosure through an AI system, or uses AI in a way that raises a safeguarding concern, staff must report this to the DSL or deputy without delay. Staff should preserve appropriate evidence in line with safeguarding procedures but should not unnecessarily copy, circulate or store harmful material.

Data protection and privacy

AI use must comply with UK GDPR, the Data Protection Act 2018, relevant changes introduced by the Data (Use and Access) Act 2025, academy and Trust data protection policies, privacy notices and the principles of data minimisation, purpose limitation, security and transparency.

The academy adopts the following default rule: personal, confidential or sensitive information must not be entered into public or unapproved generative AI services.

Where an approved AI system is proposed for processing personal data, the academy and Trust must be satisfied that:

- there is a clear and documented purpose and lawful basis for the processing;
- only the minimum necessary data will be used;
- the provider's privacy notice, retention, deletion, hosting, sharing and model-training arrangements are understood;
- appropriate contractual and security controls are in place;
- the DPO has been consulted where required and a Data Protection Impact Assessment (DPIA) has been completed where the processing is likely to result in high risk;
- privacy notices are updated where required and pupils/parents are given age-appropriate information about relevant processing;
- access to prompts, chat histories, monitoring data and reports is restricted to authorised people.

Parental consent is not automatically the appropriate lawful basis for processing personal data through AI. The correct lawful basis and any additional conditions for special category data must be determined through the academy's normal data protection arrangements.

If personal or confidential information is accidentally entered into an unapproved AI system, the member of staff must stop using the tool and report the incident promptly through the academy's data protection and, where relevant, safeguarding procedures. Staff must not attempt to conceal or independently resolve a potential data breach.

Accuracy, bias and human oversight

Generative AI can fabricate facts, citations, quotations, calculations, events and sources. It can also reproduce or amplify bias present in data or system design. Human review is therefore required before AI output is used in school.

- Important factual claims must be checked against reliable sources.
- Staff must check that resources are suitable for the intended age, curriculum and local context.
- AI output that concerns protected characteristics, culture, religion, disability, family circumstances or other sensitive topics requires particular scrutiny for bias and stereotyping.
- Where an AI system produces recommendations or analytics about pupils, staff must understand the limitations and independently consider the evidence.
- AI must not be the sole basis for a safeguarding, SEND, behaviour, attendance, attainment, grouping, admission, disciplinary or other significant decision about a pupil or member of staff.
- AI tools that infer emotion, mental state, risk, ability or other sensitive characteristics must not be introduced without explicit approval, appropriate evidence, data protection assessment and safeguarding consideration.

Assessment, feedback and pupil work

AI may support staff in designing questions, success criteria, examples, feedback structures and formative assessment materials, provided outputs are checked and adapted. It must not replace the teacher's knowledge of the pupil or professional responsibility for assessment.

- Pupils must complete work intended to demonstrate their own learning themselves unless the teacher has explicitly defined an approved AI-supported element.
- Teachers should make expectations clear for homework and independent tasks. At primary level, independent general-purpose AI use should not be assumed or required.
- Where pupils use AI as part of an approved learning activity, the teacher should make clear what use is permitted and what must remain the pupil's own work.
- AI must not be used as the sole marker or sole decision-maker for pupil assessment.
- AI detection tools, if ever used, must be treated as one possible source of information rather than proof. Suspected misuse must be considered fairly using wider evidence and professional judgement.

SEND, inclusion and accessibility

AI can offer valuable accessibility functions, such as text simplification, speech-to-text, text-to-speech, translation, visual supports and alternative ways of presenting information. Such use should support, not replace, high-quality teaching, reasonable adjustments, specialist advice or statutory provision.

- The needs of pupils with SEND must be considered when selecting AI tools, including usability, communication needs, sensory needs, comprehension, safeguarding and the risk of over-reliance.
- AI-generated adaptations must be checked by staff for accuracy, dignity, age appropriateness and alignment with the pupil's actual needs.
- The academy will consider equality impacts and seek to avoid digital exclusion or differential access creating unfair advantage or disadvantage.
- AI must not be used to diagnose SEND, mental health conditions or developmental needs.

Copyright and intellectual property

AI use does not remove existing copyright, licensing or intellectual property responsibilities. Staff and pupils must consider both what is uploaded to AI systems and what is generated in return.

- Copyrighted or licensed material must not be uploaded where the academy does not have permission or where the provider's terms would allow unauthorised storage, reuse or model training.
- Pupil work, staff-created resources and academy-owned intellectual property must not be used to train or improve third-party AI systems unless this is specifically authorised and legally permitted.
- AI-generated output should be checked for close copying, inaccurate attribution or fabricated references before publication or wider distribution.
- Where material has been materially generated by AI and transparency matters, the academy will acknowledge this appropriately.
- Staff remain responsible for ensuring that final resources used or published by the academy do not infringe third-party rights.

AI-generated images, audio and video

Synthetic media can be educationally useful but creates additional risks around consent, reputation, misinformation and safeguarding.

- Real images, video or audio of pupils must not be uploaded to public or unapproved AI generation or editing services.
- Pupil faces or voices must not be cloned or used to generate deceptive synthetic media.
- AI must not be used to create sexualised, humiliating, threatening, defamatory or misleading content about any pupil, staff member or other person.
- Use of a real staff member's likeness or voice in synthetic media requires a clear legitimate purpose and their knowledge; high-risk or public-facing uses should be approved by SLT.
- Where a synthetic image, recording or video could reasonably be mistaken for a real event or person, it should be labelled or explained appropriately.
- Safeguarding concerns involving synthetic media, including deepfakes, must be referred to the DSL immediately.

Approved tools, procurement and risk assessment

The academy will maintain an operational register of AI tools that are approved or permitted for defined uses. Approval is use-specific: a tool that is acceptable for generating a generic worksheet may not be approved for pupil accounts or for processing personal data.

Before introducing a significant, pupil-facing or data-processing AI service, the academy will consider, with SBMAT IT and/or the DPO as appropriate:

- the intended purpose, educational benefit and evidence of effectiveness;
- the age range, terms of service and suitability for primary pupils;
- the DfE Generative AI Product Safety Standards, including filtering, monitoring, reporting, security, privacy, intellectual property, governance, cognitive development, emotional and social development, mental health and manipulation;
- what data is collected, where it is stored, how long it is retained, who it is shared with and whether prompts or outputs are used for model training;
- whether a DPIA, contract review or privacy notice update is required;
- content moderation, safeguarding alerting and how the DSL is contacted for high-risk incidents;
- administrator controls, authentication, role permissions and account management;
- accessibility, equality and SEND implications;
- supplier transparency, complaints processes and how safety issues are escalated;
- the impact of model updates or new AI features, which may require re-review.

Staff must not procure, subscribe to or introduce an AI service that will process pupil personal data or provide direct pupil access outside the academy's normal approval and procurement arrangements.

Cyber security, filtering and monitoring

AI systems can introduce cyber security risks through malicious links, unsafe code, prompt injection, data exfiltration, credential theft and attempts to bypass safety controls. All AI use must therefore comply with academy and Trust cyber security arrangements.

- School devices and network activity are subject to the academy's filtering and monitoring arrangements, including Schools Broadband and Lightspeed.
- AI-generated content and AI-enabled services are considered as part of the academy's filtering and monitoring review.
- The DSL receives daily Lightspeed monitoring updates and safeguarding concerns are escalated through established routes.
- Filtering decisions and technical changes are managed centrally by the SBMAT IT Support Team.
- Guest Wi-Fi is filtered. Staff personal phones should not connect to the school Wi-Fi and should use their own mobile data, in line with academy expectations.
- Pupil iPads remain on site. Jamf is centrally managed by SBMAT IT, with appropriate academy-level administrator access held by the Computing Lead.
- Users must not attempt to jailbreak AI systems, evade safety features, use VPNs/proxies to bypass controls, or follow AI-generated instructions that would compromise school systems.

Transparency and communication

The academy will be open with pupils, parents, staff and governors about its overall approach to AI. This policy will be published through normal academy channels.

- Parents and carers will be informed where a new pupil-facing AI service materially changes how pupil data is processed or requires accounts, consent/authorisation arrangements or specific home-use expectations.
- Pupils will be told, in age-appropriate language, when an AI tool is being used in a way that directly affects their learning or processes their information.
- Staff do not need to label every minor use of AI in internal drafting. However, material AI involvement should be acknowledged where failing to do so could mislead, where required by assessment rules, or where transparency is important to a decision or published output.
- The academy will not make exaggerated claims about the capabilities, accuracy or educational impact of AI tools.

Incident reporting and response

AI-related incidents will be managed according to their nature and seriousness, using existing academy and Trust procedures rather than a separate slower process.

Nantwich Primary Academy and Nursery
Use of Artificial Intelligence (AI) in School Policy

- Safeguarding concern or harmful content: report to the DSL or deputy without delay.
- Personal data or privacy incident: report promptly through the academy/Trust data protection route and to the DPO where appropriate.
- Cyber security or technical concern: report to SBMAT IT Support and relevant academy leadership.
- Staff conduct concern: follow the Staff Code of Conduct, low-level concerns and allegation procedures as applicable.
- Pupil misuse: respond proportionately under safeguarding, behaviour and online safety procedures, with education and support as well as sanctions where appropriate.
- Serious illegal content, threats or suspected criminal activity: the DSL/SLT will involve external agencies in line with safeguarding and legal duties.

Records should capture the concern, action taken, decisions, rationale and outcome. Lessons from incidents should inform training, tool approval, filtering and policy review.

Training and support

AI literacy is an ongoing staff development need. The academy will provide proportionate training and guidance so that staff can use AI safely, understand its limitations and know when to seek specialist advice.

- All staff should receive core guidance on safeguarding, data protection, accuracy, bias, intellectual property and safe use of generative AI.
- Relevant DfE training materials, including the 2026-27 safe use of generative AI materials, may be used to support staff development.
- New staff will be introduced to the academy's AI expectations as part of induction where relevant to their role.
- DSL, SLT, Computing Lead, SBMAT IT and DPO roles should remain connected so that educational opportunities are considered alongside safeguarding and technical risk.
- Pupils will receive age-appropriate AI literacy teaching and reminders about safe, honest and thoughtful use.
- Parents may be offered guidance where new AI risks or pupil-use expectations would benefit from home-school consistency.

Monitoring, evaluation and review

The academy will evaluate AI use proportionately, focusing on whether it improves teaching, learning, accessibility or workload without introducing unacceptable risk. Evaluation should consider staff experience, pupil impact, safeguarding incidents, data protection issues, tool changes and emerging evidence.

The policy will be reviewed at least annually and sooner where there is a significant change to legislation, statutory guidance, DfE standards, Trust arrangements, academy technology, pupil-facing AI provision or the risk landscape. The next scheduled review is September 2027.

A change to an AI product's model, terms, privacy arrangements or safety features may require the tool to be reassessed even if the policy itself is unchanged.

Appendix 1: Practical AI use framework

This quick framework is intended to help staff make proportionate day-to-day decisions. Where there is doubt, staff should stop and seek advice from the Computing Lead, DSL, SBMAT IT or DPO as appropriate.

PERMITTED / LOW RISK	CHECK / APPROVAL NEEDED	NOT PERMITTED
Drafting a generic worksheet with no personal data.	A new AI tool that pupils will use directly.	Entering identifiable or sensitive pupil data into an unapproved/public AI service.
Brainstorming lesson ideas or examples, then checking and adapting them.	Any AI service that will process pupil personal data.	Using AI as the sole basis for safeguarding, SEND, behaviour, attainment or other significant decisions.
Creating a generic model text, quiz, vocabulary list or explanation and fact-checking it.	Uploading substantial copyrighted/licensed material.	Creating harmful, humiliating, sexualised or deceptive synthetic media about real people.
Using AI to reformat non-confidential material for accessibility.	Generating or editing synthetic media using a real staff member's likeness or voice.	Pupils creating personal accounts on unapproved or age-inappropriate AI services.
Using non-identifiable prompts to draft a generic parent letter, then personalising outside the AI tool.	Using AI analytics to inform decisions about individual pupils.	Bypassing filters, age restrictions, safety controls, monitoring or account permissions.
Teacher-mediated demonstration of AI where pupils do not create accounts or share personal data.	Introducing AI-generated code or technical instructions to school systems.	Uploading real pupil photos, recordings or voices to unapproved AI generation/editing systems.

A simple staff check: STOP - CHECK - USE

STOP: Does the task involve personal data, safeguarding information, a real pupil image/voice, a significant decision, copyrighted material, a new pupil-facing tool or anything confidential? If yes, do not proceed automatically.

CHECK: Is the tool approved for this use? Is the data necessary? Are the age terms suitable? Do I need DSL, DPO, SBMAT IT or SLT advice?

USE: If the use is permitted, keep prompts minimal, check the output carefully, adapt it professionally and remain accountable for the final result.

Appendix 2: AI tool approval checklist

This checklist should be used proportionately for significant, pupil-facing or data-processing AI tools. It can also support discussions with SBMAT IT, the DPO and suppliers.

CHECK	QUESTIONS TO CONSIDER
Purpose and pedagogy	What problem does the tool solve? Is there a clear educational or operational benefit? Is AI necessary? Does it support rather than replace learning and professional judgement?
Age and intended users	Is the tool designed and tested for the intended age group? Are its terms compatible with primary pupils and school-managed use?
Safeguarding	How does the tool prevent harmful content? How are disclosures and high-risk interactions identified? Can the DSL receive appropriate alerts?
Filtering and monitoring	Does the tool maintain effective moderation throughout interactions? Are prompts/activity logged appropriately? Can the school review trends and incidents?
Data protection	What personal data is collected? What is the lawful basis? Where is it stored? Is it used for training? What are retention/deletion arrangements? Is a DPIA needed?
Security	Does the service support secure authentication, role permissions, updates, logging and protection against misuse or jailbreaking?
Intellectual property	What happens to uploaded and generated content? Does the supplier claim rights to inputs? Can pupil/staff work be used for model training?
Accuracy and bias	What evidence exists about accuracy, bias and reliability? How will staff verify output? Are limitations clear?
SEND and equality	Is the tool accessible? Could it disadvantage any group? Are reasonable adjustments supported?
Cognitive development	Does the tool encourage pupils to think and attempt tasks, rather than automatically giving full answers?
Emotional and social development	Does the tool avoid pretending to be a person, encouraging secrecy, emotional dependency, excessive engagement or personal disclosure?
Supplier governance	Is there a clear complaints/safety escalation route? Are terms, privacy information and safety documentation transparent?
Change control	How will the academy know if the model, terms, data use or safety features change? What triggers reassessment?
Exit plan	Can accounts and data be deleted? Can the academy stop using the tool without losing access to essential records or teaching materials?

Suggested approval record

- Tool/service name and supplier
- Approved users and age groups
- Approved purpose(s)
- Permitted data types and prohibited data types
- Decision owner and date
- DPIA / DPO / SBMAT IT review reference where applicable
- Review date or trigger for reassessment

Appendix 3: Glossary

AI assistant / chatbot: An AI system that interacts through natural language or another conversational interface.

Algorithm: A defined set of computational rules or processes used to solve a problem or make a calculation.

Automated decision-making: A decision made using automated processing. This policy does not permit AI to be the sole decision-maker for significant academy decisions about individuals.

Bias: Systematic unfairness or distortion in data, model behaviour or output which can disadvantage individuals or groups.

Cognitive offloading: Using a tool to perform thinking or problem-solving that the learner would otherwise need to do themselves.

Deepfake: Synthetic or manipulated image, audio or video made to appear as if a real person said or did something they did not.

DPIA: Data Protection Impact Assessment. A structured assessment used to identify and reduce data protection risks, particularly for higher-risk processing.

Generative AI: AI that generates new text, images, audio, video, code or other content in response to prompts or other input.

Hallucination: A confident-sounding but incorrect, fabricated or unsupported output generated by an AI system.

Large language model (LLM): A type of AI model trained on large amounts of text and other data to generate and respond to language.

Model training: The process by which an AI model learns patterns from data. Some services may use user inputs or outputs to improve models unless settings, contracts or terms prevent this.

Personal data: Information relating to an identified or identifiable person.

Prompt: The instruction, question, image, file, audio or other input given to an AI system.

Synthetic media: Images, audio, video or other media generated or substantially altered using AI.

Pupil-facing AI: An AI product or feature with which pupils interact directly.

Public/unapproved AI tool: An AI service that has not been approved by the academy/Trust for the intended school use. Such tools must not receive personal, confidential or sensitive school information.

Appendix 4: References and guidance

This policy has been developed with regard to the following current legislation, statutory guidance and national guidance. These sources should be checked at each review because AI regulation and education guidance continue to change.

Keeping Children Safe in Education 2026 (DfE): <https://www.gov.uk/government/publications/keeping-children-safe-in-education--2>

Generative artificial intelligence (AI) in education (DfE): <https://www.gov.uk/government/publications/generative-artificial-intelligence-in-education>

Using AI in education settings: support materials, updated for 2026-27 (DfE):
<https://www.gov.uk/government/collections/using-ai-in-education-settings-support-materials>

Safe use of generative AI in education: module 3 (DfE): <https://www.gov.uk/government/publications/safe-use-of-generative-ai-in-education-module-3>

Generative AI: product safety standards (DfE, updated January 2026):
<https://www.gov.uk/government/publications/generative-ai-product-safety-standards/generative-ai-product-safety-standards>

Filtering and monitoring: core standard (DfE, updated September 2026): <https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-core-standard>

Data protection in schools: generative AI and data protection in schools (DfE, updated July 2026):
<https://www.gov.uk/guidance/data-protection-in-schools/generative-artificial-intelligence-ai-and-data-protection-in-schools>

Data protection in schools: Data (Use and Access) Act 2025 (DfE): <https://www.gov.uk/guidance/data-protection-in-schools/the-data-use-and-access-act-2025>

How Ofsted looks at AI during inspection and regulation: <https://www.gov.uk/government/publications/ofsteds-approach-to-ai/how-ofsted-looks-at-ai-during-inspection-and-regulation>

ICO: Children and the UK GDPR: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/children-and-the-uk-gdpr/>

Ofqual: AI in coursework resources for schools (2026): <https://www.gov.uk/government/publications/ai-in-coursework-resources-for-schools>

Data Protection Act 2018: <https://www.legislation.gov.uk/ukpga/2018/12/contents>

Equality Act 2010: <https://www.legislation.gov.uk/ukpga/2010/15/contents>

Copyright, Designs and Patents Act 1988: <https://www.legislation.gov.uk/ukpga/1988/48/contents>

Online Safety Act 2023: <https://www.legislation.gov.uk/ukpga/2023/50/contents>

Contact Information

Nantwich Primary Academy
Manor Road, Nantwich, Cheshire, CW5 5LX
Tel: 01270 902055
Email: nantwichoffice@sbmat.org