AMDG

# DONHEAD PREPARATORY SCHOOL

# Artificial Intelligence Policy

**Member of Staff Responsible**: Kate Donaghy
**Date Revised:** September 2026
**Governing Committee Responsible:** Safeguarding

**Contents**

Policy Summary .....3

Introduction, Purpose and Scope ..... 3
Guiding Principles ..... 4
Roles and responsibilities ..... 4
Implementation Guidelines ..... 6
AI in Teaching, Learning and Assessment ..... 7
Age Limits and Parental Consent ..... 7
Data Protection and Intellectual Property ..... 7
Plagiarism ..... 7
External Assessments ..... **Error! Bookmark not defined.**
Appropriate Use by Pupils ..... 7
Use of Generative AI by Teachers ..... 8
AI and Digital Literacy ..... 8
Policy Review and Acknowledgement ..... 8
Appendix A: AI Tool Evaluation Checklist for School Leaders ..... 9

**Review Date:** September 2027, or sooner following material changes to legislation, statutory guidance, technology or school practice

## Policy Summary

This policy outlines Donhead School's commitment to the responsible, ethical, and effective use of Artificial Intelligence (AI) technologies across all educational and administrative settings. It aligns with:

- Department for Education guidance: *Generative artificial intelligence (AI) in education*; *Generative AI: product safety standards* (updated January 2026); and the DfE materials on the safe and effective use of AI in education;
- *Keeping Children Safe in Education 2026*, including its requirements for online safety, staff understanding and effective safeguarding arrangements;
- DfE digital and technology standards, including the Filtering and Monitoring Core Standard and relevant cyber security standards for schools and colleges;
- The UK General Data Protection Regulation and Data Protection Act 2018, as amended, together with the Information Commissioner's Children's Code where applicable;
- The Copyright, Designs and Patents Act 1988;
- Current Joint Council for Qualifications guidance on AI use in assessments, where applicable; and
- The Independent School Standards and the current ISI inspection framework and handbook.

**Commented [OR1]:** @Kate Donaghy @Headteacher Change to "The UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and the Data (Use and Access) Act 2025, together with current Information Commissioner's Office guidance and the Children's Code where applicable"

The policy provides:

- Clear guidelines for selecting, implementing, and evaluating AI tools
- Defined roles and responsibilities for AI use
- Measures to ensure safety, privacy, fairness, and academic integrity
- A framework for educating pupils about the opportunities and limitations of AI

AI is used to enhance teaching, learning, and school operations—without replacing human judgment or compromising educational values.

## Introduction, Purpose and Scope

The School recognises the potential of AI, including generative AI (Gen AI) and large language models (LLMs), to transform leadership, teaching, learning, and administration. This policy sets out how we use AI to improve educational outcomes, reduce staff workload, and prepare pupils for the future.

Our approach ensures safe, fair, and inclusive implementation of AI in line with UK regulations, including UK GDPR, the Data Protection Act 2018 and the Information Commissioner's Children's Code. The policy applies to all pupils, teachers, staff, and third-party providers across all key stages.

Key objectives:

- Promote safe, secure, and ethical AI use
- Support academic excellence through AI-enhanced learning
- Provide clear expectations for pupil and staff use of AI
- Prevent misuse and uphold academic integrity
- Ensure transparency and human oversight
- Embed AI literacy and critical evaluation in the curriculum

This policy applies to all AI technologies in use, including generative AI tools (e.g., ChatGPT, Microsoft Copilot, Google Gemini and approved Microsoft 365 AI services), administrative systems, feedback platforms, data analysis tools, and personalised learning systems.

## Guiding Principles

- **Educational Benefit:** AI must support learning with demonstrable academic value.
- **Fairness & Accessibility:** AI should promote inclusion and not disadvantage any pupil.
- **Safety & Security**: Risk assessments and cybersecurity protocols protect users. Only adopt AI tools where the educational benefits clearly outweigh the risks.
- **Privacy & Data Protection**: Use of AI must comply with data protection regulations including the UK GDPR, with clear data handling policies.
- **Oversight**: AI assists, but does not replace, professional judgment with human oversight.
- **Transparency**: Pupils, parents and staff should understand how AI tools work and how decisions are made.
- **Academic Integrity:** AI must not be used to plagiarise or circumvent learning.
- **Bias & Limitations**: AI-generated content must be critically evaluated for accuracy and fairness.
- **Environmental Sustainability:** AI tools should be assessed for long-term environmental and social impact.

## Safeguarding and the Use of AI in Education

AI can generate convincing text, images, audio and video and may expose pupils to inaccurate, biased, manipulative, illegal or harmful content. Risks include bullying and harassment, impersonation, deepfakes, AI-generated sexual imagery, the creation or sharing of AI-generated nude or semi-nude images, grooming, misinformation, financially motivated sexual extortion (sextortion), inappropriate reliance on conversational systems, and attempts to create, access or distribute illegal material. Safeguarding is everyone's responsibility. All staff must understand these risks, follow *Keeping Children Safe in Education 2026*, the school's Child Protection and Safeguarding Policy and Online Safety arrangements, and receive appropriate training.

Any AI-related safeguarding concern, including harmful content, bullying, cyberbullying, discriminatory content, deepfakes, AI-generated sexual imagery, grooming, misuse of pupil data, suspected illegal material, radicalisation concerns or online exploitation, must be reported immediately to the Designated Safeguarding Lead or a deputy in accordance with the school's safeguarding procedures. The concern must be recorded and managed under the Child Protection and Safeguarding Policy, with referrals to external agencies made where required. AI-related behaviour concerns will also be addressed under the Behaviour and Anti-Bullying policies, but safeguarding action takes priority.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out risk assessments for any new AI tool being used by the school. Our school's requirements for filtering and monitoring also apply to the use of AI, in line with Keeping Children Safe in Education.

The creation, possession, sharing or distribution of AI-generated nude or semi-nude images of children, whether depicting real or fictitious individuals, will be treated as a safeguarding concern. Staff must not investigate such incidents independently and must report concerns immediately to the DSL. The school will respond in accordance with the Child Protection and Safeguarding Policy, Online Safety Policy and relevant statutory guidance.

## Roles and responsibilities

**Governors**

- Ensure that the school's arrangements safeguard and promote pupils' welfare and meet the Independent School Standards and current statutory guidance.
- Approve this policy and receive at least annual assurance on implementation, staff training, the approved-tools register, risk assessments, data protection, incidents, and filtering and monitoring.
- Ensure that appropriate resources, expertise and oversight are available and that actions arising from review are completed.

**Headteacher**

- Hold executive accountability for the school's AI strategy, policy implementation, resourcing and staff training.
- Authorise educational and administrative use of AI following appropriate advice and documented assessment.
- Ensure that AI does not replace accountable professional judgement in decisions affecting pupils, staff or the school.

**Computing Lead**

- Identify educationally beneficial uses of AI and advise the Headteacher on implementation.
- Maintain, with relevant colleagues, a register of approved AI tools and coordinate evaluation, curriculum guidance and review.
- Support staff and pupils to use approved tools critically, safely, ethically and in accordance with this policy.

**Designated Safeguarding Lead**

- Lead the safeguarding response to AI-related concerns and ensure that staff understand reporting and escalation procedures.
- Work with the Headteacher, Computing Lead and Network Manager to assess safeguarding risks and review the effectiveness of filtering and monitoring.
- Ensure that AI-related incidents are recorded, reviewed and referred in accordance with the Child Protection and Safeguarding Policy and statutory guidance.

**Data Protection Officer**

- Advise on lawful basis, transparency, data minimisation, retention, processor arrangements, international transfers and data subject rights.
- Determine whether a data protection impact assessment is required and approve data protection controls before personal data is processed through an AI tool.
- Support investigation and reporting of personal data breaches.

**Network Manager**

- Implement and maintain approved AI systems securely, including access controls, updates, logging, backup and incident response.
- Advise on supplier security, integration, cyber security, filtering and monitoring, and technical risks.
- Ensure that pupil use on school systems is appropriately supervised and subject to the school's filtering and monitoring arrangements.
- Escalate security, filtering, monitoring or data incidents promptly to the appropriate school lead.

**Teachers and Staff**

- Responsible use of AI tools in teaching and administrative tasks
- Reporting any concerns or issues with AI systems
- Participating in relevant training and development

**Pupils**

- Appropriate use of AI tools in their learning
- Reporting any concerns or issues to teachers or staff
- Understanding and following regulations concerning the use of AI in assessments

## Implementation Guidelines

**Selection and Procurement**

Only AI tools approved by the Headteacher, following advice from the Computing Lead, Data Protection Officer, Designated Safeguarding Lead and Network Manager as relevant, may be used for school business or with pupils. Approval must be documented in the school's approved-tools register and must include the Appendix A evaluation, an educational and safeguarding risk assessment, and a data protection impact assessment where required. Procurement and renewal checks must cover the tool's stated purpose, target age, accessibility, bias, content moderation, security, retention and deletion, processor terms, international transfers, breach arrangements, intellectual property, whether prompts or outputs are used for model training, and the availability of effective human oversight. Approval must be reviewed periodically and following any material change to the product, supplier terms, risk profile or intended use.

- Staff must not enter personal data, special category data, confidential information, safeguarding information or identifiable pupil work into an AI tool unless that specific processing has been expressly approved and all required controls are in place.
- Where an approved tool is used for drafting, information must be anonymised or minimised unless authorised otherwise, and the member of staff remains accountable for checking accuracy, tone, bias, confidentiality and fitness for purpose.
- AI output must not be used as the sole basis for a decision that has a legal or similarly significant effect on a pupil, parent, applicant or member of staff.
- Staff must use school-managed accounts and approved configurations where these are provided and must follow supplier terms, licensing and copyright requirements.

**Data Management**

All processing of personal data through AI must comply with the UK GDPR, Data Protection Act 2018 and the school's Data Protection Policy. Before use, the school will identify and record the purpose and lawful basis, apply data minimisation, provide appropriate privacy information, agree retention and deletion arrangements, complete processor due diligence and contracts, assess international transfers, and undertake a data protection impact assessment where the processing is likely to result in high risk. Personal data breaches must be reported immediately under the school's breach procedure.

**Training and Support**

Staff receive annual training on AI use and policy expectations, with ongoing CPD opportunities integrated into the broader staff development programme. Support is available via INSET, training sessions, and staff meetings.

**Monitoring and Filtering**

The school's filtering and monitoring arrangements apply to AI-generated and AI-mediated text, images, audio and video. The DSL and Network Manager will review their effectiveness at least annually and after any significant incident, change in technology or new deployment. The review will consider school-managed devices and networks, supervised use, alerts and reporting routes, known limitations, and the needs and ages of pupils. Material findings and actions will be reported to the Headteacher and governors. Staff must not attempt to bypass filtering or monitoring and must report concerns or gaps immediately.

**Ethical Considerations**

Ethical use of AI is central to our approach. We:

- Regularly assess potential ethical implications
- Ensure AI use reflects school values

## AI in Teaching, Learning and Assessment

**Age Limits and Parental Consent**

Pupils may use only school-approved AI tools, for an authorised educational purpose, through approved accounts and settings, and with supervision appropriate to their age, needs and the activity. The school must verify each provider's current minimum age, account and consent terms before use. Parental consent will be obtained where required, but consent does not override a provider's minimum-age restriction or remove the school's safeguarding and data protection duties. Pupils must not create personal accounts for school-directed use unless expressly authorised.

**Data Protection and Intellectual Property**

AI platforms may use prompts and other input to train their models. There is a risk that personal data used in training could be exposed by the model.

Pupils own the intellectual property rights to their work. Staff should not submit pupil work (e.g. homework) to an AI model which might use it as training data or otherwise infringe the pupil's copyright.

Commented [OR2]: @Kate Donaghy @Headteacher Change to "AI platforms may retain or process prompts, uploaded files and other inputs, and some services may use this content to develop or train their models. Before an AI tool is approved, the School must establish how submitted information is processed, retained, shared and deleted, and whether it is used for model training. Pupil work must be treated in accordance with applicable copyright, intellectual property and data protection requirements. Staff must not upload identifiable pupil work, photographs, recordings, creative work or other pupil-generated content to an AI system unless that specific use has been approved by the School and appropriate data protection, safeguarding, copyright and intellectual property considerations have been addressed."

Personal data, special category data, safeguarding information, confidential information and identifiable pupil work must not be entered into an AI system unless the use has been expressly approved, a lawful basis and appropriate safeguards have been documented, and any required data protection impact assessment has been completed.

Further detail is set out in the school's Data Protection Policy. Staff wishing to trial or introduce an AI platform must obtain approval through the process in this policy before proceeding; they should contact the Computing Lead in the first instance.

**Plagiarism**

It is plagiarism to represent AI generated work as your own. This applies to all work undertaken at school including homework and external assessments. Plagiarism may be sanctioned following the relevant school policies.

### *External Assessments*

Where Joint Council for Qualifications or awarding-body rules apply, the school will ensure that staff and candidates receive the current AI guidance before work begins. AI must not be used in an examination or other assessment where it is prohibited. Where use is permitted, candidates must acknowledge the tool and material used, record the date and manner of use, retain required evidence such as prompts and outputs, and sign the relevant declaration only when satisfied that unacknowledged work is their own. Teachers and assessors must authenticate work, investigate doubts about authorship and report suspected malpractice in accordance with current regulations and the school's malpractice procedures.

**Appropriate Use by Pupils**

It is imperative that pupils develop the knowledge, skills and understanding of the subjects they are studying, and do not rely on AI.

Pupils should follow age limits and other terms and conditions when using AI platforms. AI tools can support learning, creativity, and revision but must never be relied on to complete work or bypass meaningful learning effort.

Pupils should be aware that generative AI can confidently report incorrect or misleading information.

**Use of Generative AI by Teachers**

AI can support teaching by reducing workload, providing timely feedback, and facilitating personalised learning. It should be used to enhance, not replace, the professional judgment of teachers.

- AI may assist with feedback and planning, but the output of AI grading tools must always be reviewed by teachers.
- Predictive tools (e.g. learning analytics) must not be used to restrict or limit pupil opportunities.
- Homework policies should promote effective, age-appropriate AI use and discourage over-reliance.
- Any AI-driven monitoring will be transparent, proportionate, and clearly explained to pupils and parents.

## AI and Digital Literacy

We are committed to preparing all pupils and staff for a future in which AI plays an increasing role.

Our approach includes:

- Teaching pupils, in an age-appropriate manner, how to use emerging technologies, including generative AI, safely, ethically and effectively, including understanding online risks such as deepfakes, misinformation, online manipulation and AI-generated content.
- Helping pupils understand the limitations, biases, and reliability issues of AI-generated content
- Particular attention will be given to supporting pupils with SEND who may face additional difficulties in identifying inaccurate, manipulated or misleading AI-generated content and understanding its potential consequences
- Developing digital skills such as online safety, content creation, and critical thinking
- Encouraging exploration of ethical and societal implications of AI
- Reinforcing that AI is a tool to support learning, not a substitute for original thought

**Commented [OR3]:** @Kate Donaghy @Headteacher Add "Teaching will help pupils understand that AI systems may communicate in human-like ways but do not think, feel or understand in the same way as people. Pupils will be taught, in an age-appropriate manner, about anthropomorphism, persuasive design and the risks of placing inappropriate trust in, or developing emotional reliance on, conversational AI systems."

For staff:

- Annual training on the role of AI in education
- Ongoing CPD on ethical use, bias awareness, and effective AI integration in teaching, learning and school organisation
- Staff model responsible AI use and guide pupils accordingly

## Policy Review and Acknowledgement

- This policy will be reviewed at least annually and sooner following material changes to legislation, statutory guidance, technology, supplier terms, school practice or the risk profile.
- Safeguarding concerns must be reported immediately to the Designated Safeguarding Lead or a deputy. Data protection, cyber-security and technical concerns must also be reported promptly through the relevant school procedure.
- The school will retain proportionate evidence of implementation, including staff training, approved-tool records, risk assessments and DPIAs, filtering and monitoring reviews, incidents, governor oversight and relevant curriculum provision.
- This document was structured and summarised with assistance from ChatGPT, an AI language model developed by OpenAI, and reviewed by the school.

## Appendix A: AI Tool Evaluation Checklist for School Leaders

| Area | Required evidence before approval |
|---|---|
| Purpose and educational benefit | Clear intended use, target users and age range; evidence of educational value; proportionate use that supports rather than replaces teaching and professional judgement. |
| Safeguarding and wellbeing | Documented safeguarding risk assessment covering harmful or illegal content, manipulation, impersonation, bullying, grooming, misinformation, moderation, reporting routes and vulnerable pupils. |
| Data protection | Purpose and lawful basis; data minimisation; privacy information; retention and deletion; processor contract; international transfers; data subject rights; breach arrangements; and a DPIA where required. |
| Security | Supplier assurance, access controls, authentication, encryption, updates, logging, resilience, incident response and compatibility with school cyber-security standards. |
| Training data and intellectual property | Clear terms on whether prompts, uploaded material or outputs are retained or used for training; copyright and licensing position; ownership of outputs; and an effective opt-out or protected education configuration where necessary. |
| Age, accounts and consent | Provider age terms verified; approved account model; parental consent where required; supervision arrangements; and no reliance on consent to override minimum-age restrictions. |
| Accuracy, bias and accessibility | Testing for accuracy, bias, discrimination and accessibility, including SEND needs; clear limitations; and controls to prevent unfair or exclusionary outcomes. |
| Human oversight | Named accountable owner; staff review of outputs; ability to intervene or override; no solely automated significant decisions; and clear escalation routes. |
| Filtering and monitoring | Compatibility with the school's filtering and monitoring arrangements across text, image, audio and video; known limitations documented; alerts |

**Commented [OR4]:** @Kate Donaghy @Headteacher Change to "Documented safeguarding and wellbeing risk assessment covering harmful or illegal content, manipulation, persuasive or anthropomorphic design, impersonation, bullying, grooming, misinformation, content moderation and reporting routes. The assessment must also consider potential impacts on pupils' cognitive development, emotional and social development, mental health and wellbeing, including risks of over-reliance on, emotional attachment to, or inappropriate trust in AI systems. Particular consideration must be given to the age and developmental stage of pupils and to pupils with SEND or other vulnerabilities."

| | |
|---|---|
| | and incident handling agreed. |
| Assessment integrity | Alignment with current JCQ or awarding-body rules where applicable; clear pupil instructions; authentication, acknowledgement and evidence requirements. |
| Implementation and review | Training, support, cost, accessibility, contractual exit, deletion on termination, review date, owner and triggers for re-assessment recorded in the approved-tools register. |

**Approval record:** The evaluator must record the decision, conditions of use, accountable owner, review date and any required actions. A tool must not be used until all mandatory controls are satisfied and approval is entered in the approved-tools register.

**Evaluator's Name**: ..... **Date of Evaluation**: .....

Recommendation (delete as appropriate):

**Outcome (delete as appropriate):** Approved / Approved with conditions / Further assessment required / Not approved

| |
|---|
| Comments: |
| Any additional comments: |