



The Grange School Acceptable Use of Artificial Intelligence (AI) Policy

Effective from: September 2026

Applies to:	Students and School Staff
Date of Governing Body Approval	September 2026
Next Review	July 2027

Document Control

Title	The Grange School Acceptable Use of Artificial Intelligence (AI) Policy
Originator / Author / Owner	A Haycock
Review Cycle	Every year
Published Location	Intranet and Website
Supporting documents	None
Classification	Advisory

Change Record

Version	Date	Updated by	List Change made to document	Document Status

Document Management

Governance Area of Responsibility:

Curriculum	
Finance	
Health and Safety	
Safeguarding	
SEND	
Personnel	
Other:	X



The Grange School Acceptable Use of Artificial Intelligence (AI) Policy

Policy Date: September 2026
Review Date: July 2027

1. Purpose

The Grange School recognises that Artificial Intelligence (AI) is becoming an important part of education and society. AI may be used to support teaching, learning and administrative tasks where it enhances understanding, promotes independent thinking and helps prepare students for an increasingly digital future. The school's approach is guided by:

- Keeping Children Safe in Education (KCSIE) 2026
- Department for Education (DfE) guidance on Generative AI in Education
- UK GDPR and Data Protection Act 2018
- Existing Grange School policies, including:
 - Child Protection and Safeguarding Policy
 - Online Safety Policy
 - Behaviour Policy
 - Staff Code of Conduct
 - Computer Usage Policy
 - Mobile Phone Policy

2. Key Principles

All AI use at The Grange School must be:

- Safe and safeguarding-led
- Educationally purposeful
- Ethical and responsible
- Age-appropriate and supervised
- Critically evaluated rather than trusted automatically
- Compliant with data protection requirements

AI should support learning and professional practice but must never replace human judgement, independent thinking or safeguarding responsibilities.

3. Approved AI Platforms

To protect school information and personal data:

- Microsoft 365 Copilot is the school's approved AI platform for staff and students.
- Staff and students must not use unapproved AI platforms for school-related work where confidential or school data could be exposed.

4. KCSIE Safeguarding Expectations

In line with KCSIE 2025, AI is considered part of the school's online safety and safeguarding responsibilities. Staff must remain alert to risks including:

Content Risks

- Misinformation and disinformation
- Inaccurate or biased information
- Harmful or inappropriate content

Conduct Risks

- Academic dishonesty
- Bullying, harassment or harmful content creation
- Over-reliance on AI

Contact Risks

- Manipulative chatbot interactions
- Unsafe advice or inappropriate interactions

Emerging Risks

- Deepfakes
- AI-generated impersonation
- Manipulated images and media

Any AI-related safeguarding concern must be reported through normal safeguarding procedures and referred to the Designated Safeguarding Lead (DSL) where appropriate.

5. Student Use

Students may use AI when authorised by staff and for clear educational purposes such as:

- Understanding concepts
- Revision and retrieval practice
- Generating ideas

- Improving spelling, grammar or presentation

Students must:

- Use AI responsibly and respectfully
- Verify AI-generated information
- Follow all Computer Usage and Mobile Phone Policy expectations
- Report concerning or inappropriate AI content to staff

Students must not:

- Submit AI-generated work as their own
- Use AI to cheat or gain unfair advantage
- Generate harmful or inappropriate content
- Attempt to bypass school filtering and monitoring systems
- Enter personal or confidential information into AI tools

6. Staff Use

Staff may use AI to support:

- Lesson planning
- Resource creation
- Differentiation
- Administrative tasks
- Professional development

Staff remain fully accountable for all decisions and materials produced using AI. AI outputs must always be checked for:

- Accuracy
- Bias
- Suitability
- Safeguarding implications

Staff must:

- Model safe and responsible AI use
- Supervise student use appropriately
- Promote digital literacy and critical thinking
- Report safeguarding concerns arising from AI use

7. Data Protection and Confidentiality

In line with UK GDPR, the Data Protection Act 2018 and existing Grange School policies:

Staff and students must never enter in AI systems:

- Student names or identifiable information
- Safeguarding information
- Assessment records
- Staff information
- Parent/carers information
- Any confidential school information

Failure to comply may constitute both a data protection breach and a safeguarding concern.

8. AI and Devices

In line with the Mobile Phone Policy:

- Students must not use AI tools on personal mobile devices during the school day.
- AI should only be accessed through approved school devices and systems.
- AI activities should take place within supervised educational contexts.

This ensures use remains safe, monitored and educationally focused.

9. Academic Integrity (JCQ Aligned)

All submitted work must represent the student's own understanding and effort.

Students may use AI to:

- Support planning
- Generate ideas
- Improve presentation

Students must not:

- Submit AI-generated work as their own
- Copy or paraphrase AI output without acknowledgement
- Use AI to complete assessed work without demonstrating understanding

Unacknowledged AI use may constitute malpractice under JCQ regulations and could result in sanctions, including loss of marks or disqualification from qualifications.

10. Online Safety and Critical Thinking

The school will promote AI literacy through curriculum and pastoral programmes.

Students should be taught to:

- Question AI-generated content
- Verify information from trusted sources
- Understand bias and misinformation
- Recognise deepfakes and manipulated content
- Make safe and ethical choices online

11. Misuse and Sanctions

Misuse of AI includes:

- Cheating
- Plagiarism
- Creating harmful or inappropriate content
- Breaching safeguarding expectations
- Circumventing school security systems
- Misusing personal or confidential data

Consequences will be applied in accordance with:

- Behaviour Policy
- Safeguarding procedures
- Staff disciplinary procedures
- JCQ malpractice regulations where relevant

12. Leadership and Governance

The Headteacher, Senior Leadership Team, Governors and DSL will ensure that:

- AI use remains aligned with KCSIE and DfE guidance
- Filtering and monitoring systems remain effective
- Staff training is provided
- Safeguarding risks are appropriately managed
- The policy is reviewed annually or sooner if guidance changes