STEEL RIVER
ACADEMY TRUST

Artificial Intelligence (AI) Use and Teaching Policy



Review Date	1.9.26
Review Frequency	1 year
Date for Next Review	1.9.27
Author	John Frost

1. Purpose

This policy outlines the safe, ethical, and educationally considered use of Artificial Intelligence (AI) in Steel River Academy Trust. It ensures alignment with national safeguarding guidance, including 'Keeping Children Safe in Education' (2025) and supports the responsible integration of AI into teaching and learning. This policy also reflects the principles and recommendations set out in the Department for Education's 'Generative artificial intelligence (AI) in education' (2025), emphasising teacher empowerment, safe and ethical use, supervised pupil access, staff training on AI literacy and ethics and ongoing review. An AI policy by Helen Hogan of Safeguarding Matters (2025) has also been used to inform this policy, most notably regarding safeguarding considerations. This policy will be updated annually but reviewed throughout the year to consider the rapid changes in this field.

2. Scope

This policy applies to:

- All staff, including teachers, teaching assistants, and administrative personnel.

- Pupils exploring and potentially using AI tools under supervision in the future.

- Parents and carers, in terms of awareness of AI usage in schools.

- External providers offering AI-based educational tools or services.

3. Guiding Principles

- Child Safety First: All AI use must comply with safeguarding policies and data protection laws (UK GDPR and Data Protection Act 2018).

- Teacher-Led Learning: AI must support—not replace—teacher-led instruction.

- Transparency and Accountability: Staff must verify AI-generated content and ensure it is age-appropriate and accurate.

- Equity and Inclusion: AI tools must be accessible to all pupils and not reinforce bias or discrimination.

- Digital Literacy: Pupils will be taught to understand AI's role, limitations, and ethical considerations.

4. Acceptable Use of AI

4.1 For Staff

- Planning lessons and generating teaching resources with careful consideration and scrutiny.

- All AI-generated content must be reviewed, fact-checked and approved by a member of staff before use.

- Supporting with administrative tasks such as letters, reports, social media posts and data analysis.

- Not for making decisions about pupil behaviour, attainment, or safeguarding without human review.

- Consider and pilot marking and providing feedback (with human oversight) through carefully selected and approved resources. Staff from Whale Hill to trial after training.

- To support children with SEND or EAL through selected programmes or resources such as Seeing AI.

- Staff remain responsible for ensuring that AI-generated content respects copyright, licensing requirements and intellectual property rights.

- Responsibility for decisions relating to teaching, assessment, parental communication, SEND provision and safeguarding always remains with the member of staff and cannot be delegated to an AI system.

4.2 For Pupils

- Exploring age-appropriate AI tools under supervision.

- Using AI to support creativity, problem-solving, and digital literacy.

- Not permitted to use AI tools unsupervised or for assessments unless explicitly approved.

5. Safeguarding and Data Protection

- AI tools must not collect or store identifiable pupil data without explicit consent. Staff must not enter personal, confidential or safeguarding information relating to pupils, families or staff into public AI systems unless the system has been formally approved and covered by a Data Protection Impact Assessment.

- Schools in the Trust will ensure that any AI tools accessed and used comply with GDPR and do not store or process personal student data.

- Staff must ensure AI tools comply with the school's Data Protection Impact Assessment (DPIA). Before adoption, all AI tools should be assessed for:

- safeguarding risks
- age appropriateness
- data protection
- accessibility
- bias
- content moderation
- filtering and monitoring compatibility

- Schools in the Trust will ensure that AI use does not expose students to harmful or inappropriate material.

- Staff will be aware of potential bias, misinformation, disinformation and conspiracy theories that may be produced or perpetuated by AI. This will be monitored to prevent inaccuracies or biased perspectives being taught or shared in the classroom.

- Staff should use Copilot for school-related tasks because it offers secure, reliable, and tailored support aligned with educational needs—unlike free AI models, which may lack data privacy, consistency, and integration with our school's systems.

- AI must not be used to monitor pupils or make automated decisions affecting their welfare. AI must not be used as a replacement for human judgment in safeguarding decisions.

- Training will be delivered in schools to ensure staff understand their safeguarding responsibilities regarding AI and to monitor its use in school.

- All AI products used within the Trust should be assessed against the Department for Education's Generative AI Product Safety Expectations and approved through the school's procurement and safeguarding processes.

5.1 Responding to AI-Related Safeguarding Risks

If a safeguarding concern arises due to AI usage, the Trust will take the following steps:

- Immediate Assessment – Staff will assess the nature and severity of the concern. This could involve AI-generated content that is inappropriate, biased, misleading, or violating data protection laws.
- Reporting Procedures – Any safeguarding concerns will be reported to the Designated Safeguarding Lead (DSL).
- Staff will record the incident, including the AI tool involved, its output, and any potential risks identified.

5.2 Risk Mitigation Measures

- The Trust will immediately restrict the AI tool in question while further investigation occurs.
- The Trust will ensure that any affected students or staff receive appropriate support, including intervention from the Designated Safeguarding Lead if necessary.

5.3 Investigation & Decision-Making

Following the incident, the DSL, along with senior leadership and IT specialists, will investigate to determine the root cause and whether AI misuse, bias, or data exposure occurred.

If the AI tool was responsible for exposing students to harmful material, it will be permanently removed or adjusted appropriately to ensure it is compliant.

5.4 Parent/Carer & Stakeholder Communication

Where relevant, parents and guardians will be informed immediately of any safeguarding risks involving AI.

Designated Safeguarding Leads will seek advice and guidance from external safeguarding agencies if the risk has broader implications, such as online safety threats. This may include contacting statutory agencies including the police and children's service social care.

Children and parents will continue to receive regular education and learning on the risks and benefits of AI and safe digital engagement.

5.5 AI-Generated Content, Deepfakes and Synthetic Media

Staff, pupils and parents will be supported in understanding:

- AI-generated images, audio and video may be used maliciously.
- The creation or sharing of AI-generated content intended to harm, embarrass or impersonate others will be treated as a safeguarding and behaviour incident.
- Staff must report suspected deepfake or synthetic media incidents to the DSL.
- How to identify manipulated content and understand associated risks.

6. The Law around Online Safety Incidents

From 25.07.2025 there is a new law around online age verification on pornography sites. Platforms must use highly effective methods to verify users' ages before showing any pornographic material.

6.1 Accepted Verification Methods

Sites may use one or more of the following:

- Facial age estimation via photo or video
- Open banking checks to confirm age via financial data
- Digital identity wallets storing verified age credentials
- Credit card verification
- Photo ID matching (e.g. passport or driving licence)
- Mobile network age filters
- Email-based age estimation using linked services like banks or utilities.

6.2 The Online Safety Act 2023

6.21 New Communications Offences

These are designed to replace and modernise older laws under the Malicious Communications

Act 1988 and Communications Act 2003:

- False Communications (Section 179)

Sending a message that the sender knows is false, intending to cause non-trivial psychological or physical harm to a likely audience.

- Threatening Communications (Section 181)

Sending a message that conveys a threat of death or serious harm (including GBH, rape, or serious financial loss), intending or being reckless as to whether someone fears it will be carried out.

- Flashing Images Offence (Section 183)

Sending or showing flashing images electronically with intent to cause harm—particularly targeting individuals with epilepsy (known as Zach's Law).

- Encouraging or Assisting Serious Self-Harm (Section 184)

Doing any act (including sending or showing content) intended to encourage or assist serious self-harm, even if no harm occurs.

6.22 Sexual Image Offences (Amendments to Sexual Offences Act 2003)

These expand protections against non-consensual image sharing:

- Cyber-Flashing (Section 66A)

Sending unsolicited images of genitals with intent to cause alarm, distress, or for sexual gratification.

- Sharing or Threatening to Share Intimate Images (Section 66B)

Includes revenge porn, deepfakes, and down-blousing. Covers both actual sharing and threats to share, even if the image is fake.

6.23 Other Notable Offences

- False Reporting of Child Sexual Abuse to the NCA (Section 69)

Criminalises knowingly making false reports of child sexual exploitation or abuse to the National Crime Agency.

7. <u>Curriculum Integration</u>

AI will be explored through the computing and PSHE curriculum.

Pupils will learn:

- What AI is and how it works (in simple, age-appropriate terms).

- How to use AI responsibly and critically.

- The importance of human judgement and ethical considerations.

- Recognising misinformation and disinformation.

- Understanding AI-generated images and videos.

- Identifying fake or manipulated content.

- Considering ethical implications of AI.

- Understanding bias in AI systems.

- Understanding ownership and authorship of digitally created work.

8. Staff Training and Professional Development

This policy will be reviewed and updated to prevent future safeguarding concerns.

All staff will receive additional training on AI-related risks and responsible usage to reinforce best practices as and when new technology emerges or new systems are integrated into school.

8.1 Training Objectives

- Build confidence in using AI tools for teaching, learning, and administration.
- Ensure understanding of safeguarding and data protection implications.
- Promote critical thinking about AI-generated content.
- Encourage ethical and inclusive use of AI in the classroom.

8.2 Training Content

2025 - 2026:

1. Introduction to AI in Education
   - What AI is and how it works (basic concepts).
   - Examples of AI tools used in education.
   - Benefits and limitations of AI in a primary setting.

2. Safeguarding and Data Protection
   - Risks of AI misuse (e.g., misinformation, bias, over-reliance).
   - Ensuring compliance with Keeping Children Safe in Education (2026) and UK GDPR.
   - Conducting Data Protection Impact Assessments (DPIAs) for AI tools.

3. Practical Use of AI Tools
   - Using AI to support lesson planning, marking, and differentiation.
   - Evaluating AI-generated content for accuracy and age-appropriateness.
   - Case studies and hands-on demonstrations.

4. Teaching AI Literacy to Pupils
   - How to introduce AI concepts to children in an age-appropriate way.
   - Encouraging critical thinking and digital citizenship.
   - Addressing ethical questions (e.g., fairness, bias, transparency).

5. Monitoring and Reporting

- Identifying and responding to concerns about AI use.

- Reporting inappropriate content or safeguarding issues.

- Logging and escalating concerns to the DSL or ICT Lead.

Suggested topics for training 2026 -2027:

- deepfakes and synthetic media
- AI-enabled cyberbullying
- copyright and intellectual property
- prompt writing and verification
- AI bias
- AI-generated misinformation
- evaluating AI outputs

8.3 Delivery Format

- Regular training delivered to all staff.

- Termly refreshers: short updates on new tools, risks, and best practices.

8.4 Evaluation and Feedback

- Staff confidence and competence will be assessed through surveys and informal feedback.

- Training content will be updated annually based on staff needs, technological developments, and changes in national guidance. A log of resources suitable and unsuitable for use in school will be kept and updated regularly.

9. Monitoring and Review

- The policy will be reviewed annually or in response to new guidance.

- The Designated Safeguarding Lead (DSL) will oversee AI-related safeguarding concerns.

- Feedback from staff, pupils, and parents will inform updates.

10. Roles and Responsibilities

- Headteacher: Ensures policy implementation and compliance.

- DSL and safeguarding team: Monitor safeguarding risks related to AI.

- Teachers: Use AI tools responsibly and model safe use.

- Online Safety Lead: Evaluates and approves AI tools for classroom use.

References

Department for Education (2026) *Keeping Children Safe in Education.* chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://assets.publishing.service.gov.uk/media/6a4cf903b7203c4c023fd2f3/Keeping_children_safe_in_education_2026_.pdf [Accessed 20 July 2026]

Department for Education (2025) *Generative Artificial Intelligence (AI) in Education: Guidance for Schools and Colleges.* https://www.gov.uk/government/publications/generative-artificial-intelligence-in-education [Accessed 20 July 2026]

Department for Education (2026) *Using AI in education settings: support materials.* *https://www.gov.uk/government/collections/using-ai-in-education-settings-support-materials* [Accessed 20 July 2026]

Department for Education (2026) *Generative AI: product safety expectations*. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://dera.ioe.ac.uk/id/eprint/41041/1/Generative%20AI%20product%20safety%20expectations%20-%20GOV.UK.pdf [Accessed 20 July 2026]

Department for Education (2023) *AI Revolution to Give Teachers More Time with Pupils.* https://www.gov.uk/government/news/ai-revolution-to-give-teachers-more-time-with-pupils [Accessed 20 July 2026]

Helen Hogan (2025) *Artificial Intelligence (AI) Policy for schools 2025 – 2026.* Safeguarding Matters. [Accessed 29 August 2025]

Appendix A: Proposed AI Staff Training Schedule (2026–2027)

Term	Training Topic	Key Content
Autumn 1	AI Policy Update and Staff Responsibilities	Changes to Trust AI policy, staff accountability, human oversight requirements, acceptable and unacceptable use of AI.
Autumn 1	Keeping Children Safe in Education and AI	AI-related safeguarding concerns, reporting procedures, role of the DSL, AI and online safety incidents.
Autumn 2	Data Protection, GDPR and AI	Safe use of AI systems, handling pupil data, confidentiality, DPIAs, approved and non-approved tools.
Autumn 2	Prompt Writing and Quality Assurance	Effective prompting techniques, checking accuracy, recognising hallucinations, fact-checking AI outputs.
Spring 1	Deepfakes, Synthetic Media and Impersonation Risks	AI-generated images, videos, voice cloning, online bullying, reputational harm, safeguarding responses.
Spring 1	Copyright, Intellectual Property and AI	Copyright considerations, ownership of AI-generated content, use of images, text and educational resources.
Spring 2	Using AI to Reduce Workload Safely	Lesson planning, reports, letters, resource creation, meeting notes, workload reduction while maintaining professional responsibility.

Term	Training Topic	Key Content
Spring 2	Inclusive and Ethical AI Use	AI bias, fairness, accessibility, supporting SEND and EAL pupils, avoiding discrimination.
Summer 1	Teaching AI Literacy Across the Curriculum	Age-appropriate teaching of AI, links to Computing, PSHE, Online Safety and Digital Literacy.
Summer 1	Misinformation, Disinformation and Critical Thinking	Identifying fake content, evaluating online information, recognising AI-generated misinformation.
Summer 2	Emerging Technologies and Future Risks	New AI developments, current safeguarding concerns, updates to legislation and national guidance.
Summer 2	Review, Reflection and Good Practice Sharing	Staff case studies, evaluation of approved tools, lessons learned and priorities for the following year.