George Stephenson High School

Use of Artificial Intelligence (AI) Policy V1

April 2026 – April 2029

Policy Compliance Governance Page

Governance	Resources Committee and Governing Body	
Policy Officer	Deputy Headteacher	
Policy Suite	Safeguarding	
Policy Version	V1	
Re-adopted by Governing Date	**To be approved by Governors**	
Last Updated	N/A	
Review Date		
Statutory Policy	No	
Uploaded to School Website and Date	YES	March 2026

DATE	**SECTION**	**FEEDBACK AND PROPOSED AMENDMENTS**
March 26	New Policy	New Policy implemented

Contents

Use of Artificial Intelligence (AI) Policy……………………………………………………….3

1. Policy statement…..………………………………………………………………………..3
2. Scope…………….………………………………………………………………………….3
3. Roles and Responsibilities ...……………………………………………………..……….3
4. Responsible Use of AI……………………………………………………………………..4
5. Legal and Data Protection Compliance……………………………...……………….5
6. Safeguarding and Online Safety…………………………………………………….….5
7. AI in Teaching and Learning…………………………………………………………….6
8. JCQ Assessment and Malpractice Requirements……………………………..…….6
9. Reporting and Incident Process…………………………………………………..…….6
10. Monitoring and Review………………………………………………………………..….7
11. Consequences of Misuse……………………………………………………….……….7

Use of Artificial Intelligence (AI) Policy

George Stephenson High School

1. Policy statement

Artificial Intelligence (AI) is transforming education by enhancing teaching, learning, and administration. To maximise its benefits while mitigating risks, this policy provides clear guidance on the ethical and responsible use of AI by students, staff, and administrators at George Stephenson High School.

This policy aligns with our school ethos of being Respectful, Ready and Safe and is informed by national guidance including:

- Keeping Children Safe in Education (KCSIE)2025
- UK GDPR and Data Protection Act 2018
- DfE Generative AI in Education Guidance 2025
- JCQ Artificial Intelligence Use in Assessments Guidance 2024
- Online Safety Act 2023

2. Scope

This policy applies to all staff, students, governors, parents/carers, and third-party providers using AI in the school environment for teaching, learning, assessment, and administration.

3. Roles and Responsibilities

Effective oversight and accountability are essential to ensure AI is used appropriately and safely within the school. The following sections define the key responsibilities of school leadership, staff, students and IT teams in managing AI systems.

SLT / Leadership and Governance Teams:

- Ensure AI governance aligns with DfE, KCSIE, and GDPR regulations.
- Approve AI tools before they are used in teaching, learning, or administration.
- Conduct annual AI risk assessments and policy reviews.
- Ensure AI use is transparent, fair, and free from bias.
- Engage in annual update training on compliance and safeguarding.

Designated Safeguarding Lead:

- Monitor and respond to safeguarding issues linked to AI, including misinformation, impersonation, and inappropriate outputs.
- Train staff and students on online safety risks linked to AI.

Data Protection Officer (DPO):

- Ensure data protection compliance with UK GDPR and school policies.
- Conduct Data Protection Impact Assessments (DPIAs) for any new AI tool processing personal data.
- Approve only tools that meet data security and privacy requirements.
- Engage in annual update training to ensure compliance and risk mitigation for the latest risks
- Conduct Data Protection Impact Assessments (DPIAs) for any new AI tool processing personal data.

IT/Network Managers:

- Ensure data protection compliance with UK GDPR and school policies.
- Approve only tools that meet data security and privacy requirements.

Teaching Staff:

- Model responsible AI use, educate students on risks and safe practice, and verify that AI use does not compromise learning or assessment.
- Use AI as a teaching aid and not as a replacement for pedagogy.
- AI must not be used to process or upload confidential internal school documents or student-specific data unless the tool is explicitly approved.
- Teaching and support staff must complete annual refresher training to remain up to date with emerging technologies, national guidance, and evolving safeguarding, compliance, and AI-related risks.
- Staff must report to the IT Manager any new or emerging AI tools they become aware of that students are using or discussing in school, to help the school assess risks and update approved tool lists accordingly.

Students:

- Use AI responsibly, follow the Acceptable Use Agreement, and never use AI to cheat, deceive, or input personal/confidential data.

Parents/Carers

- Stay informed about how AI is used in school.
- Encourage safe AI use at home.
- Report any concerns or misuse to school staff.
- The school will provide regular communication to parents/carers on safe AI use, either via newsletters, website updates, or information sessions

4. Responsible Use of AI

- Use AI to support, not replace, learning and decision-making.
- Critically assess AI outputs for bias, misinformation, and accuracy.

- Ensure transparency when AI tools are used to generate content.
- Do not rely solely on AI for assessments or high-stakes decisions.

5. Legal and Data Protection Compliance

AI tools must not be used to input:

Personally identifiable or sensitive data such as:

- Student names (e.g. Emily Smith, Year 10)
- Staff names or contact details
- Dates of birth
- Home addresses or phone numbers
- SEN (Special Educational Needs) status
- Behaviour or safeguarding records
- Health or wellbeing information (e.g. “Student suffers from anxiety and takes medication”)
- Exam access arrangements
- Attendance or exclusion details
- Any data that could identify an individual, even indirectly
- Confidential documents or internal materials
- Personal assessment data,
- wellbeing concerns

A DPIA must be completed if the AI tool processes personal or sensitive data, makes automated decisions that could affect individuals, or presents a high risk to rights and freedoms (e.g., profiling).

All AI tools used must be vetted and listed in the Approved AI Tools Appendix.

6. Safeguarding and Online Safety

- Staff and students must not use AI to produce or share harmful, misleading, discriminatory, or inappropriate content (e.g. deepfakes, fake news).
- Staff and students must be trained to recognise and respond to AI-related risks.
- AI-generated content must never be used to impersonate others.
- School filtering and monitoring systems must include AI-generated threats.
- Staff and students should report any suspicious or harmful AI-generated content (e.g., deepfakes, impersonations, or content causing distress).
- The school will maintain systems to detect inappropriate AI content (in line with DfE Filtering & Monitoring Standards).
- Staff will receive annual safeguarding updates specifically covering AI-related risks.

7. AI in Teaching and Learning

- Teachers may use AI to support planning, feedback, and lesson design.
- Staff must not use AI to write official school communications (e.g., reports, emails to parents) without oversight.

Students may use school approved, age-appropriate AI tools to support research and learning, but:

- Must not submit AI-generated work as their own.
- Must declare if AI was used and cite any tools and prompts.
- Must not use AI in assessments unless clearly allowed.

8. JCQ Assessment and Malpractice Requirements

In line with JCQ guidance:

- All student assessment submissions must be their own independent work.
- Any AI-assisted work must be declared.
- Unauthorised use of AI may result in malpractice investigations and disqualification from qualifications.
- Teachers and assessors must investigate suspicious work and report suspected AI misuse.

9. Reporting and Incident Process

All users (staff and students) must report any concerns related to AI use, including:

- Harmful, misleading, or inappropriate AI outputs (e.g. discriminatory content, false information, or impersonation)
- Suspected misuse in assessments (e.g. undeclared AI-generated coursework)
- Data breaches or input of sensitive personal or school-related information
- Use of unapproved or unsafe AI tools

Reports should be made to:

- The Designated Safeguarding Lead (DSL)
- The Data Protection Officer (DPO)
- A member of SLT or your line manager

Staff are encouraged to self-report any accidental misuse of AI or mistakes made when using AI tools. Reports will be handled supportively, with a focus on learning and continuous improvement.

Staff should also report any concerns about others' use of AI, including low-level concerns, to help safeguard students and uphold professional standards.

All incidents will be managed confidentially and in line with the school's safeguarding, data protection, and conduct policies.

10. Monitoring and Review

AI technologies and regulations evolve rapidly. This section ensures the school regularly reviews its AI policy, assesses risks and gathers feedback to maintain compliance and best practices.

- This policy is reviewed annually
- Updates will reflect changes in national guidance, school needs, and emerging technologies.
- All AI use in school is subject to review, audit, and oversight.

11. Consequences of Misuse

- Misuse of AI will lead to disciplinary action in line with school conduct and safeguarding policies.
- Repeated or severe breaches may result in restricted access, formal warnings, or reporting to exam boards.

Policy Compliance Statement

All staff, students, and third-party providers accessing AI George Stephenson High School must adhere to this policy. Any breaches may result in disciplinary action in line with school policies and national regulations. We cannot stress the importance of ensuring compliance with this policy, particularly in light of Ofsted's role in ensuring mitigation of risk and support of governance of the use of AI and technology. This policy ensures AI is used to enhance education while upholding legal, ethical, and safeguarding standards and supports our values of being **Respectful, Ready and Safe**.