



GATEHOUSE
SCHOOL

Artificial Intelligence (AI) Policy

Reviewed by:	Pauline Moisy (Head of Pastoral, DSL) Fiona Tighe (DDSL) Tom Sheldon (Head of Key Stage 1 and 2)
Approved by:	Governors
Date Approved:	September 2026
Next Review:	September 2027

0. Document Control.....	3
1. Introduction.....	4
2. Purpose.....	4
3. Scope.....	4
4. Legislative Background and Key Guidance.....	5
Relevant Legislation and Regulation.....	5
Online Safety Act 2023.....	5
UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018...	5
Ofcom Regulation.....	5
National Guidance and Frameworks.....	5
Related Gatehouse School Policies.....	6
5. Key Principals.....	6
Human oversight.....	6
Safeguarding first.....	7
Data protection.....	7
Transparency.....	7
Professional responsibility.....	7
6. Acceptable Use by Staff.....	7
7. Use of AI by Pupils.....	8
8. Data Protection.....	9
9. Safeguarding Considerations.....	9
9. Roles and Responsibilities.....	10
Headteacher and Senior Leadership Team.....	10
Designated Safeguarding Lead (DSL).....	10
Data Protection Officer.....	10
Staff.....	10
Governors.....	10
11. Training.....	11
12. Reporting Concerns.....	12
13. Monitoring and Review.....	12
Appendix 1: Amendment to Staff Acceptable Use Agreement.....	13
Likelihood and Impact Definitions.....	14

0. Document Control

The table below contains the changes made between the different final editions of this document set for approval. This is to help provide information to those reviewing and approving the document of the changes being made.

Document Edition	Section	Details of change
March 2026	All Sections	New policy
September 2026		

1. Introduction

Artificial Intelligence (AI) technologies are becoming increasingly integrated into education and wider society. AI tools have the potential to support teaching and learning, enhance creativity, improve administrative efficiency and reduce staff workload.

Gatehouse School recognises the opportunities that AI can provide while also acknowledging the potential risks associated with its use, including concerns around safeguarding, data protection, misinformation, bias and ethical use.

This policy outlines the expectations for the responsible, safe and ethical use of Artificial Intelligence within the school community. The safeguarding and wellbeing of pupils remain the school's primary priority in all uses of technology.

2. Purpose

The purpose of this policy is to ensure that:

- AI technologies are used safely, ethically and responsibly
 - staff and pupils understand the benefits and risks of AI
 - personal and sensitive data is protected
 - AI supports teaching, learning and school operations without replacing professional judgement
 - the school remains compliant with UK GDPR and relevant safeguarding guidance
-

3. Scope

This policy applies to:

- all staff
- volunteers
- governors
- pupils
- external partners using school systems

It applies to the use of all AI systems, including but not limited to:

- generative AI tools (e.g. text, image or video generators)
 - AI-powered educational platforms
 - AI used in assessment, planning or administrative systems
 - AI features embedded within software used by the school
-

4. Legislative Background and Key Guidance

The use of Artificial Intelligence (AI) within education continues to develop rapidly. While there is currently limited legislation specifically governing the use of AI in schools, a number of national laws, regulatory frameworks and guidance documents inform how schools must approach the safe, ethical and responsible use of emerging technologies.

Gatehouse School ensures that its approach to Artificial Intelligence aligns with relevant legislation, safeguarding expectations and national guidance relating to online safety, data protection and digital education.

Relevant Legislation and Regulation

The following legislation informs the school's approach to the use of AI and emerging technologies:

Online Safety Act 2023

The Online Safety Act 2023 aims to make the internet safer, particularly for children and vulnerable users. The Act places duties on technology companies to reduce the risk of harmful online content and improve the protection of young people online. While the Act does not directly regulate schools, it provides the wider regulatory framework governing digital services and platforms that pupils may use.

UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018

These laws govern the processing, storage and protection of personal data. When Artificial Intelligence systems are used within schools, they must comply with these requirements to ensure that personal information relating to pupils, staff and families is handled securely and lawfully.

Ofcom Regulation

Ofcom is the UK's regulator for online safety and communications services. Ofcom is responsible for implementing aspects of the Online Safety Act and producing guidance for technology companies regarding their obligations to protect users, including children.

National Guidance and Frameworks

In addition to legislation, the school takes account of national strategies and guidance relating to Artificial Intelligence, digital technologies and online safety. These include:

- [AI Roadmap - GOV.UK](#)
- [National AI Strategy - GOV.UK](#)
- [Ofcom's 2024 Online Nation Report](#)

- [EU Artificial Intelligence Act 2024 - Useful high-level 4-point summary of considerations](#)
- [NESCO AI Competency Framework for Students \(Guidance\)](#)
- [UNESCO AI Competency Framework for Staff \(Guidance\)](#)
- [Responsible AI Toolkit - GOV.UK](#)
- [Data protection in schools - Artificial intelligence \(AI\) and data protection in schools - Guidance - GOV.UK](#)
- [SWGfL – Artificial Intelligence and Online Safety](#)
- [Generative AI: product safety standards](#)

These documents help inform best practice for the safe and responsible implementation of AI technologies within educational settings.

Related Gatehouse School Policies

This policy should be read in conjunction with the following Gatehouse School policies, which collectively support the safe and responsible use of technology:

- Online Safety Policy
- Behaviour Management Policy
- Data Protection Policy
- Safeguarding and Child Protection Policy
- Digital Images Policy
- Teaching and Learning Policy
- Computing Policy

Together these policies provide the framework through which Gatehouse School ensures that digital technologies, including Artificial Intelligence, are used in ways that prioritise **pupil safety, responsible use of technology and compliance with legal and regulatory requirements**.

5. Key Principals

Gatehouse School recognises that Artificial Intelligence may support:

- personalised learning
- lesson planning and resource development
- assessment support
- administrative efficiency
- creative and exploratory learning opportunities

However, the school maintains the following principles:

Human oversight

AI must support professional judgement and decision-making, not replace it. All outputs must be reviewed by a member of staff before being shared with the school community or actioned.

Safeguarding first

The safety, wellbeing and privacy of pupils and staff will always take precedence over technological convenience.

Data protection

No personal, confidential or sensitive data relating to pupils, staff or families should be entered into AI systems unless the system has been formally approved and assessed for compliance with **UK GDPR**.

Transparency

Where AI has been used to assist in producing professional work (such as reports, communications or planning materials), staff should ensure outputs are reviewed, edited and verified before use.

Professional responsibility

Staff remain accountable for any work produced with the assistance of AI.

6. Acceptable Use by Staff

Staff may use AI tools to support professional practice where appropriate.

Appropriate uses may include:

- generating lesson ideas or resources
- supporting differentiation
- drafting communications
- summarising information
- supporting administrative tasks
- creating example texts or prompts for learning

Staff must ensure that:

- no identifiable pupil data is entered into AI systems
- confidential or strategic school information is not uploaded
- outputs are checked for accuracy, bias and appropriateness
- AI systems comply with data protection requirements
- AI is not used to impersonate individuals or create misleading content

Staff must not rely solely on AI outputs without professional review.

7. Use of AI by Pupils

Gatehouse School recognises that pupils are increasingly interacting with Artificial Intelligence in their everyday lives, often without realising it. From voice assistants and search engines to games, video platforms and educational applications, AI technologies are embedded within many of the digital services children use both at home and in school.

Research from the UK communications regulator **Ofcom** demonstrates that children are already interacting with AI technologies from a young age.

For example:

- Ofcom's *Online Nation Report (2024)* found that **more than half of children aged 8–15 had used a generative AI tool within the past year.**
- The same research indicates that **teenagers aged 13–15 are particularly likely to use AI tools**, with around **two thirds reporting use**, while **almost half of children aged 8–12 have also used generative AI technologies.**
- Ofcom also reports that **over half of children who use AI tools have used them to support homework or learning tasks.**

These findings highlight that children are increasingly interacting with AI technologies both intentionally and indirectly, often through services that incorporate AI features.

As children are already interacting with AI systems in everyday digital services, schools have a responsibility to ensure pupils develop the knowledge and critical thinking skills required to use these technologies safely.

As these technologies increasingly shape the information pupils see and the digital services they use, it is important that pupils develop the understanding needed to engage with them safely, responsibly and critically.

Teaching pupils about Artificial Intelligence therefore supports the aims of the **National Curriculum for Computing**, which requires pupils to:

- understand how digital systems operate
- evaluate digital content critically
- understand how search technologies select and rank results
- use technology safely, respectfully and responsibly.

By addressing Artificial Intelligence within the curriculum, Gatehouse School aims to help pupils:

- recognise when technology is generating or influencing information
- question the reliability and accuracy of digital content
- understand the ethical implications of emerging technologies

- develop responsible digital behaviours.

This approach ensures that pupils are **equipped to navigate an increasingly AI-driven digital environment**, while supporting the broader aims of the National Curriculum to develop **responsible, competent and confident users of technology**.

Misuse of AI by pupils will be addressed through the school's **Behaviour Management** and **Online Safety Policy**.

8. Data Protection

The school recognises that AI systems may process large amounts of data and may present additional risks.

Staff must:

- only use AI systems approved by the school where personal data may be involved
- anonymise any data before use
- comply with the school's **Data Protection Policy**
- consult the **Data Protection Officer** where there are concerns regarding AI systems

Where necessary, a **Data Protection Impact Assessment (DPIA)** will be conducted before implementing new AI tools.

9. Safeguarding Considerations

The school recognises that AI technologies may introduce safeguarding risks, including:

- exposure to harmful or inappropriate content
- AI-generated bullying or harassment
- deepfakes or impersonation
- misinformation
- manipulation or emotional harm

To mitigate these risks the school will:

- maintain robust filtering and monitoring systems
- educate pupils about AI safety and digital responsibility
- ensure staff training includes emerging online risks
- investigate and record incidents appropriately

All safeguarding concerns involving AI must be reported in line with the school's **Safeguarding and Child Protection Policy**.

9. Roles and Responsibilities

Headteacher and Senior Leadership Team

The Headteacher and Senior Leadership Team are responsible for:

- ensuring the safe and responsible use of AI across the school
- establishing clear procedures for AI use
- ensuring staff receive appropriate training
- reviewing emerging technologies and associated risks

Designated Safeguarding Lead (DSL)

The DSL is responsible for:

- monitoring safeguarding risks related to AI
- ensuring concerns are recorded and responded to appropriately
- supporting staff with safeguarding issues linked to digital technologies

Data Protection Officer

The DPO will:

- provide guidance on data protection implications of AI use
- oversee compliance with UK GDPR
- support DPIAs for new technologies

Staff

All staff are responsible for:

- following this policy
- using AI tools responsibly
- safeguarding pupil data
- reporting concerns or misuse

Governors

Governors will:

- maintain oversight of the school's approach to AI
 - ensure risks are considered within safeguarding and data protection frameworks
 - review this policy as part of governance responsibilities
-

11. Training

As Artificial Intelligence (AI) becomes an increasingly significant part of modern education, Gatehouse School recognises the importance of ensuring that staff are equipped with the knowledge and confidence to use AI technologies effectively, responsibly and safely.

Training will support staff in understanding both the opportunities and risks associated with AI and ensure that its use enhances teaching, learning and administrative processes while maintaining high standards of safeguarding, ethics and data protection.

The school will:

- Provide **appropriate training and guidance for staff and governors** on the effective and responsible use of AI technologies within education.
- Ensure staff understand the **benefits, limitations and potential risks of AI systems**, including issues such as misinformation, bias, privacy concerns and safeguarding risks.
- Integrate **AI awareness into safeguarding and online safety training**, ensuring staff understand how emerging technologies may impact pupil safety and wellbeing.
- Provide training on **data protection and confidentiality**, ensuring staff understand how to use AI tools in compliance with UK GDPR and the school's Data Protection Policy.
- Support staff in developing **AI literacy**, enabling them to confidently evaluate AI-generated outputs and use AI tools appropriately within their professional practice.
- Provide guidance on **ethical and responsible AI use**, promoting fairness, inclusivity and awareness of potential bias within AI systems.
- Ensure staff are able to **support pupils in developing safe and responsible approaches to AI**, helping them understand how to evaluate information critically and use technology responsibly.
- Provide training to help staff **identify and respond to potential risks**, including harmful content, bias, misinformation, impersonation, or safeguarding concerns linked to AI technologies.
- Encourage staff to use AI as a **supportive professional tool**, while maintaining appropriate human oversight and professional judgement in all decisions affecting pupils.

AI-related training may be delivered through:

- safeguarding and online safety training
- staff professional development sessions
- digital safety briefings
- external training opportunities
- guidance shared through internal school systems.

The school will review training provision regularly to ensure staff remain informed about **emerging technologies, evolving risks and best practice in the use of AI within education**.

12. Reporting Concerns

Concerns relating to AI misuse should be reported through the school's normal safeguarding and reporting procedures.

This may include concerns relating to:

- inappropriate AI-generated content
- data protection breaches
- cyberbullying or harassment involving AI
- impersonation or deepfake content

Where necessary, incidents may be reported to relevant external agencies.

13. Monitoring and Review

This policy will be reviewed annually or sooner if:

- new AI technologies are introduced
 - safeguarding guidance changes
 - legislative changes occur
-

Appendix 1: Amendment to Staff Acceptable Use Agreement

Amendment to staff acceptable use policy:

All staff must ensure they use Artificial Intelligence responsibly and in accordance with this policy.

Staff confirm that they will:

- use AI technologies responsibly and ethically
- ensure personal or sensitive data is not entered into AI systems
- verify AI-generated outputs before use
- respect copyright and intellectual property
- report any misuse or safeguarding concerns

Failure to comply with this policy may result in disciplinary action.

Appendix 2: Risk Assessment Matrix

The following risk assessment matrix is intended to help identify, evaluate, and mitigate risks associated with implementing Artificial Intelligence (AI) in educational processes.

The matrix considers potential risks across various domains, including data protection, ethical considerations, and operational integrity. There is a particular focus on safeguarding and wellbeing issues, highlighting potential risks to student welfare and offers strategies to mitigate these risks effectively. Schools should amend the content of the matrix as necessary and consider the risk profile that is relevant to their own circumstances.

Likelihood and Impact Definitions

Likelihood: The likelihood that the identified risk will occur.

- Low: Unlikely to occur under normal circumstances.
- Medium: Possible occurrence based on past trends or vulnerabilities.
- High: Likely to occur without intervention.

Impact: The severity of impact should the risk materialise.

- Low: Minimal disruption with limited consequences.
- Medium: Moderate disruption affecting key processes.
- High: Significant disruption with severe consequences.

Risk Area	Risk Description	Likelihood	Impact	Risk Level	Mitigation Measures
Data Protection and Privacy Breaches	Unauthorised access to sensitive data or personal information, leading to safeguarding, privacy and organisational risks.	Medium	High	Medium	Only use school-approved AI systems. Minimise personal and sensitive data entered into AI tools. Complete DPIAs where required and ensure GDPR-compliant data processing and appropriate security measures are in place. Provide guidance to pupils, staff and, where appropriate, parents on protecting personal information when using AI.

Risk Area	Risk Description	Likelihood	Impact	Risk Level	Mitigation Measures
Cyberbullying	AI tools may facilitate bullying, harassment, impersonation or the creation and sharing of harmful content.	Medium	High	Medium	Maintain appropriate filtering and monitoring. Establish clear reporting mechanisms and acceptable-use expectations. Include AI-related cyberbullying, impersonation and harmful content within the curriculum. Work with parents where appropriate to reinforce expectations and respond to concerns.
Over-reliance on AI	Over-reliance on AI may reduce independent thinking, interpersonal interaction and pupil learning. Excessive use by staff could reduce professional judgement and teacher autonomy.	Medium	Medium	Medium	Define clear boundaries for appropriate AI use. Balance AI-supported activities with independent and collaborative learning. Ensure teachers retain responsibility for professional and educational decisions. Develop pupils' understanding of when AI use is and is not appropriate.
Emotional Manipulation	AI systems may influence pupils' emotions, behaviour or decision-making, particularly where systems simulate human relationships or provide personalised responses.	Low	High	Medium	Ensure pupils understand that AI systems are not people or substitutes for trusted adults. Include age-appropriate teaching about AI relationships and interactions within the curriculum. Maintain staff oversight and work with parents where concerns arise.
Inappropriate Content or Conduct	AI systems may expose learners to harmful, age-inappropriate or unsuitable content or behaviour.	Medium	High	Medium	Assess AI tools before use, considering age appropriateness and safeguarding risks. Apply effective filtering and monitoring. Develop curriculum coverage around safe AI use, including how pupils should respond to inappropriate AI-generated content. Communicate

Risk Area	Risk Description	Likelihood	Impact	Risk Level	Mitigation Measures
					expectations and concerns to parents where appropriate.
Mental Health Impacts	Excessive or inappropriate use of AI tools may contribute to stress, anxiety, dependency, reduced confidence or other negative impacts on pupil wellbeing.	Low	High	Medium	Set clear expectations around appropriate AI use and screen time. Monitor patterns of use and changes in pupil behaviour. Ensure pupils know how to access trusted adults and pastoral support. Work collaboratively with parents where AI use may be affecting a pupil's wellbeing.
Bias and Discrimination	AI systems may reproduce or amplify biases, stereotypes or discriminatory outcomes that affect pupil wellbeing, inclusion or educational opportunities.	Medium	High	Medium	Review AI tools and outputs for evidence of bias. Develop pupils' AI literacy through the curriculum, including understanding bias, stereotypes and representation in AI generated content. Ensure significant decisions are not made solely using AI outputs.
Misuse of AI	Learners may use AI tools for harmful, unethical or illegal purposes, including impersonation, harassment, cheating, deepfakes or the creation of sexualised/nudified images.	Medium	High	Medium	Establish clear expectations through AI/acceptable-use and behaviour policies. Explicitly teach safe, responsible and lawful AI use through the curriculum, including deepfakes, impersonation and AI-generated sexualised content where age appropriate. Restrict access to inappropriate tools where possible. Work with parents to reinforce expectations and respond to incidents. Treat serious misuse as a safeguarding matter where appropriate.

Risk Area	Risk Description	Likelihood	Impact	Risk Level	Mitigation Measures
Misinformation	AI may generate inaccurate, fabricated or misleading information which pupils or staff may accept or distribute as fact.	High	Medium	Medium	Teach pupils through the curriculum to critically evaluate and verify AI-generated information using reliable sources. Develop understanding of hallucinations, manipulated media and AI-generated misinformation. Provide staff training and share appropriate guidance with parents.
Digital Divide	Unequal access to devices, connectivity, paid AI services or digital skills may create disparities between pupils.	Low	Medium	Low	Ensure equitable access to school-approved AI resources where required for learning. Provide suitable alternatives where access is unavailable and avoid making paid AI services necessary for schoolwork. Consider parental circumstances and access when setting AI-supported activities outside school.
AI Ethics Awareness	Staff and learners may lack awareness of the ethical implications of AI, including privacy, copyright, bias, transparency and responsible use.	Medium	Medium	Medium	Develop a progressive, age-appropriate AI curriculum covering safe and responsible use, ethics, privacy, copyright, bias and critical evaluation. Provide regular staff training and appropriate information and guidance for parents. Consider an AI working/ethics group to review emerging issues.
Data Accuracy	AI systems may generate inaccurate, incomplete, fabricated or misleading recommendations and information.	High	Medium	Medium	Require appropriate human verification of AI-generated information. Staff remain accountable for decisions and professional judgements. Teach pupils to question, check and corroborate AI outputs as part of the curriculum. AI should not be the sole basis for significant

Risk Area	Risk Description	Likelihood	Impact	Risk Level	Mitigation Measures
					educational, safeguarding or administrative decisions.
Legal Compliance	AI use may result in non-compliance with data protection, copyright, safeguarding, equality or other relevant legal and regulatory requirements.	Low	High	Medium	Maintain awareness of current legal and regulatory requirements. Review school policies as guidance develops. Conduct DPIAs and other assessments where appropriate. Ensure staff training and curriculum content reflect changes to expectations around safe and lawful AI use.
Cyber-Security	AI tools may create additional opportunities for phishing, social engineering, malware, credential theft or other cyberattacks against school systems and users.	Medium	High	Medium	Maintain robust cybersecurity controls. Train staff and pupils to recognise AI-enhanced phishing, scams and social engineering. Incorporate emerging AI-related online threats into the computing/online-safety curriculum and provide parents with relevant guidance where appropriate. Only permit approved AI services on school systems.