



# Use of Artificial Intelligence (AI) Policy

STATUS: NON-STATUTORY

**Review Cycle:** Annual

**Governor Committee Responsible:** Education and FGB

**Date of Last Review:** 07/072026

**Date of Next Review:** Summer 2027

*Tiffin School's AI Policy is based upon The Key model AI Policy for schools (April 2026), adapted to reflect the school's local context, safeguarding procedures, Online Safety Policy and Student Digital Code of Conduct.*

## Contents

1. Aims and Scope
  2. Legislation and Guidance
  3. Roles and Responsibilities
  4. Approval and Risk Assessment of AI Tools
  5. Staff and Governor Use of AI
  6. Educating Students About AI
  7. Use of AI by Students
  8. AI and Formal Assessments
  9. Safeguarding and Online Safety
  10. Staff Training
  11. Breaches of this Policy
  12. Monitoring and Review
  13. Links with Other Policies
- Appendix 1 - Examples of Approved AI Uses
- Appendix 2 - AI Risk Assessment Framework

# 1. Aims and Scope

Tiffin School recognises the growing role of artificial intelligence (AI), including generative AI, in education and wider society. Used appropriately, AI technologies can enhance teaching, learning, accessibility, creativity and operational efficiency. However, AI also presents risks relating to safeguarding, misinformation, plagiarism and academic malpractice, data protection, bias, online abuse, deepfake content, and copyright or intellectual property.

This policy establishes clear expectations for the safe, ethical and responsible use of AI technologies by students, staff, governors, volunteers and visitors using school systems. It applies to all AI tools, including generative AI platforms, AI-assisted search tools, image generators, transcription and summarisation tools.

The policy aims to:

- support the responsible use of AI to enhance teaching, learning and operational efficiency;
- develop students' AI literacy, critical thinking and digital responsibility;
- promote academic honesty and integrity;
- protect personal data, privacy and safeguarding;
- ensure compliance with safeguarding and online safety expectations;
- prepare students for a future in which AI will play an increasingly significant role.

The school's approach to AI is underpinned by the following principles:

- AI should enhance, not replace, professional judgement, strong teaching and meaningful relationships;
- AI should support genuine learning rather than substitute for student thinking;
- safeguarding, wellbeing and data protection must remain central to all AI use;
- AI outputs should be reviewed critically for accuracy, bias and appropriateness;
- AI should promote inclusion, accessibility and equity;
- Human oversight and accountability remain essential.

The school's approach to AI is further informed by five overarching governance principles:

- Safety, security and robustness;
- Transparency and explainability;
- Fairness and equity;
- Accountability and governance;
- Contestability and human oversight.

These principles underpin all decisions relating to the approval, deployment and review of AI technologies.

For the purposes of this policy, the following definitions of AI apply:

**AI:** The theory and development of computer systems able to perform tasks normally requiring human intelligence, e.g. visual perception, speech recognition, decisionmaking

**Generative AI:** A category of AI algorithms that generate new digital content, such as text, images, videos or other data based on the data they have been trained on.

## 2. Legislation and Guidance

This policy is informed by:

- Department for Education (DfE) guidance on Generative Artificial Intelligence in Education
- DfE AI Product Safety Expectations
- Keeping Children Safe in Education (KCSIE)
- Joint Council for Qualifications (JCQ) guidance on AI use in assessments
- UK GDPR and the Data Protection Act 2018
- Ofsted guidance regarding AI use in schools
- Microsoft Responsible AI Principles and Approach
- Microsoft 365 Education AI Guidance
- Google for Education: AI in Education
- Gemini for Education / Google Workspace AI Guidance

This policy should also be read alongside:

- Online Safety Policy
- Student Digital Code of Conduct
- Behaviour and Pupil Discipline Policy
- Safeguarding and Child Protection Policy
- Data Protection Policy
- Acceptable Use of IT Policy
- Exams Policy
- Staff Code of Conduct
- Curriculum, Teaching & learning Policy
- Equality Statement and Objectives

## 3. Roles and Responsibilities

### 3.1 Governing Board

The Governing Board will:

- Monitor the implementation of this policy;
- Ensure the school's approach to AI is proportionate, ethical and legally compliant;
- Ensure appropriate safeguarding, filtering and monitoring systems are in place;
- Review AI-related risks and developments annually at least.

### 3.2 Headteacher

The Headteacher is responsible for:

- Ensuring this policy is implemented consistently;
- Approving AI tools and use cases;
- Ensuring staff receive appropriate guidance, training and continuous professional development as it emerges;
- Ensuring students are educated about responsible AI use;
- Working with the DSL, DPO and IT team regarding safeguarding and compliance;
- Appointing an AI Lead (Digital Champion) to support the implementation of this policy, coordinate staff guidance, monitor developments in AI technologies and provide advice on approved educational uses of AI .

### 3.3 Designated Safeguarding Lead (DSL)

The DSL will:

- Monitor safeguarding concerns relating to AI;
- Respond to incidents involving harmful AI use;
- Ensure staff understand emerging AI safeguarding risks;

- Oversee filtering and monitoring processes linked to AI use.

This includes risks relating to deepfake content, AI-generated sexualised imagery, impersonation, cyberbullying, misinformation, harmful or extremist material, cognitive offloading that may reduce independent thinking or help-seeking, and emotional dependency on AI systems that may undermine trusted human relationships or safeguarding disclosures.

### **3.4 Head of IT**

The Head of IT will:

- Support the safe technical implementation of approved AI tools;
- Oversee filtering, monitoring and cybersecurity arrangements relating to AI;
- Support risk assessment and data protection processes;
- Work with the DSL and SLT regarding emerging AI-related risks.

### **3.5 Digital Champion**

The AI Lead will:

- Support the implementation of this policy;
- Advise SLT on emerging AI developments and educational opportunities;
- Support the evaluation and quality assurance of proposed AI tools;
- Work with the DSL, DPO and Head of IT to assess risks;
- Coordinate AI-related staff development;
- Maintain guidance on approved AI tools and uses;
- Act as a point of contact for staff seeking advice on AI.

### **3.6 Staff**

In teaching, staff must:

- Use only approved AI tools;
- Exercise professional judgement at all times;
- Fact-check and quality assure AI-generated content;
- Protect confidential and personal data;
- Report any data breaches to the DPO;
- Acknowledge AI use where appropriate.

With respect to students, staff must:

- Report safeguarding concerns immediately;
- Ensure where AI is used by pupils it is consistent with Section 7 and in the Student Digital Code of Conduct.

Staff must not:

- Input confidential student or staff or organisational information into any AI systems;
- Use AI to generate inappropriate or discriminatory material;
- Use AI to impersonate others;
- Rely solely on AI outputs without professional review.

### **3.6 Students**

Students must follow the expectations outlined in Section 7 and in the Student Digital Code of Conduct.

## **4. Approval and Risk Assessment of AI Tools**

All AI tools used within school must be risk assessed before approval.

Risk assessments will consider:

- safeguarding implications
- age restrictions

- filtering and monitoring compatibility
- data protection and GDPR compliance
- bias and misinformation risks
- educational value
- reputational risk

Where necessary, Data Protection Impact Assessments (DPIAs) will be completed.

The school reserves the right to prohibit the use of any AI platform deemed unsuitable or unsafe.

Given the rapidly evolving nature of AI technologies, approved uses may change regularly. See Appendix 1.

## 5. Staff and Governor Use of AI

Tiffin School encourages the thoughtful, ethical and proportionate use of AI to support teaching, learning and administrative efficiency. Appropriate uses may include lesson planning, quiz and resource generation, drafting communications, differentiation ideas, revision materials and retrieval practice activities.

Staff and governors should also be mindful of the environmental impact of AI technologies. AI should be used purposefully and proportionately, recognising that AI systems consume significant computing, energy and water resources. Where appropriate, users should consider whether AI adds genuine value to a task and avoid unnecessary or excessive use where simpler alternatives would be equally effective.

However:

- AI must not replace professional expertise or judgement;
- all AI-generated outputs must be reviewed critically;
- responsibility for final content always remains with the member of staff or governor using the tool.

In addition, staff and governors must not:

- use AI in a manner that breaches safeguarding, data protection, copyright or professional conduct requirements;
- use AI to generate, access or distribute harmful, offensive, discriminatory or inappropriate content; use AI to make consequential decisions about students, staff or families without appropriate human oversight and professional judgement;
- use AI in any way that would be inconsistent with the Staff Code of Conduct or other school policies.

Any AI-generated content shared internally or externally should be checked carefully for factual accuracy, bias, safeguarding concerns, inappropriate tone or content, and potential copyright issues.

### 5.1 Data Protection

Staff and governors must not enter personally identifiable student information, photographs, safeguarding information, confidential HR information or sensitive parental communications into AI tools unless explicitly approved and compliant with data protection requirements.

AI must not be used to process personal data through public or unapproved AI systems. This includes, but is not limited to, names, contact details, photographs, safeguarding information, SEND records, medical information, assessment data, admissions information, parental communications and personnel records.

Any accidental disclosure may constitute a data breach and will be managed in accordance with the school's Data Protection Policy.

Any actual or suspected data breach involving the use of AI must be reported immediately to the Headteacher, DPO and Head of IT.

Examples may include:

- entering personal, safeguarding, medical, SEND or assessment information into an unapproved AI platform;
- uploading documents containing personally identifiable information;
- AI-generated outputs that inadvertently disclose confidential information;
- unauthorised sharing of AI-generated content containing personal data.

The school will investigate all reported incidents promptly and take appropriate action in accordance with the UK GDPR, Data Protection Act 2018 and the school's Data Protection Policy. Where required, breaches will be reported to the Information Commissioner's Office (ICO) and affected individuals will be informed.

## **5.2 Intellectual Property and Copyright**

Students and staff retain intellectual property rights over original work they create. AI tools must not be used in ways that breach copyright, licensing or intellectual property requirements.

Users should also be aware that:

- AI outputs may reproduce copyrighted material;
- AI-generated content may not always be original;
- prompts and uploaded materials may be retained by some providers;
- AI-generated content should not be published externally without appropriate human review;
- the use of AI should be acknowledged and cited appropriately where required, in accordance with principles of academic integrity, transparency and any relevant school, examination board or awarding body guidance.

## **5.3 Bias and Critical Evaluation**

AI systems may reflect or amplify societal biases. Users should critically evaluate AI outputs for inaccuracies, misinformation, stereotypes and discriminatory assumptions.

Examples may include:

- gender stereotypes in subject, career or leadership recommendations;
- racial, ethnic, cultural or religious bias
- assumptions about disability, SEND or neurodiversity;
- socioeconomic bias and assumptions about family background;
- biased representations of historical events, individuals or communities;
- unequal treatment of different groups in recommendations, assessments or generated content.

Staff and students should not assume that AI-generated content is neutral, objective or free from prejudice. Human review and professional judgement remain essential.

## **5.4 Human Oversight**

AI may support administrative processes and decision-making but must not be used to make consequential decisions about students without substantive human review and professional judgement.

This includes decisions relating to safeguarding, behaviour sanctions, academic outcomes, references, SEND provision, admissions and pastoral support. AI must not be used to determine safeguarding thresholds, assess risk, make child protection decisions, or draft safeguarding records without

substantive human review. Professional judgement and accountability remain essential in all safeguarding matters.

### **5.5 AI Incidents and Data Breaches**

Any actual or suspected AI-related data breach, cybersecurity incident or unauthorised disclosure of confidential information must be reported immediately to the Headteacher, DPO and Head of IT and managed in accordance with the school's Data Protection Policy.

Incidents may include:

- uploading personal or sensitive information to an unapproved AI tool;
- disclosure of safeguarding, SEND, medical or assessment information through AI systems;
- unauthorised sharing of AI-generated content containing personal data;
- compromise of school accounts through AI-related phishing or cyber attacks;
- use of AI tools in a manner that breaches UK GDPR or school policies.

The school will investigate all incidents promptly and take appropriate remedial action. Where necessary, the school will notify the Information Commissioner's Office (ICO), affected individuals and other relevant authorities in accordance with statutory requirements.

Lessons learned from AI-related incidents will inform future risk assessments, staff training and approval processes.

## **6. Educating Students About AI**

Tiffin School believes students should develop strong AI literacy alongside broader digital literacy and critical thinking skills.

Students will be taught:

- how AI works in broad terms;
- the opportunities and limitations of AI;
- how to evaluate AI-generated information critically;
- online safety and misinformation awareness;
- ethical and responsible AI use;
- academic integrity expectations;
- risks associated with deepfakes and manipulated media;
- the risks of over-reliance on AI and the importance of independent thinking;
- the risks of emotional dependence on AI systems and the value of trusted human relationships;
- the importance of human oversight ("human in the loop") when using AI tools and the need to review, question and improve AI-generated outputs;
- the environmental and sustainability implications of AI technologies, including the energy, water and computing resources required to train and operate AI systems.

Students should understand that AI-generated content may contain inaccuracies, bias, fabricated references or misleading information presented confidently. They should therefore evaluate AI outputs critically rather than assuming they are accurate or reliable. Students should understand that responsibility for decisions, actions and submitted work always remains with the human user. AI outputs should be reviewed, challenged and refined through human judgement rather than accepted uncritically.

Students should understand that responsible AI use includes consideration of its environmental impact. AI should be used purposefully to support learning and problem-solving, rather than as a substitute for effort, curiosity or independent thinking. Students will be encouraged to consider whether AI is the most appropriate tool for a given task and to use digital technologies responsibly and sustainably.

Students will also learn:

- that AI should support learning rather than replace thinking;
- that AI-generated content may be inaccurate or biased;
- how to acknowledge or reference AI use appropriately where permitted;
- that responsibility for learning, decision-making and final work remains with the student, not the AI system.

AI education may take place through Computing, PSHE and Twenty First Century Life lessons, assemblies, tutor time, online safety education and subject-specific discussions.

## 7. Use of AI by Students

The school recognises that AI may support learning appropriately in some contexts. Students may use approved AI tools:

- for research and exploration
- for revision support
- to generate practice questions
- to support understanding of difficult concepts
- where specifically directed by a teacher

Any use of AI must:

- support genuine learning
- be age appropriate
- be transparent
- comply with school expectations regarding academic honesty
- comply with the Student Digital Code of Conduct and all other relevant school policies

Students must not use AI:

- during assessments unless explicitly permitted
- to complete homework dishonestly
- to generate coursework presented as entirely their own
- to bypass learning processes
- to impersonate or harass others
- to create harmful, explicit or offensive content

Students should understand that AI systems are tools rather than trusted companions. They should not be relied upon in place of independent thinking, learning, or support from trusted adults and peers. AI systems may sometimes generate inaccurate, manipulative, misleading, sexualised or otherwise inappropriate responses.

Students must not engage with AI systems in ways that involve:

- sexualised conversations or roleplay
- harmful or exploitative scenarios
- sharing personal, sensitive or intimate information
- emotionally dependent or inappropriate interactions

The following are strictly prohibited:

- AI-generated bullying or harassment
- creation or sharing of deepfake material
- AI-generated pornography or sexualised imagery
- use of AI to deceive staff or students
- attempts to bypass school filtering or monitoring systems

Students should always reference AI tools appropriately.

Unattributed AI-generated work may be treated as plagiarism and sanctioned under the Behaviour and Pupil Discipline or Exams Policies.

Students must only use AI tools that have been approved by the school and must comply with any minimum age requirements specified by the provider. Students must not create accounts, access services or otherwise use AI platforms where they do not meet the provider's age requirements or where use has not been authorised by the school.

Some AI platforms have minimum age requirements within their own terms of service. The school will ensure that any approved student-facing AI tools are age-appropriate and compatible with safeguarding expectation

## **8. AI and Formal Assessments**

The school follows current JCQ guidance regarding AI use in assessments.

Students must not use AI in any assessment where it is prohibited.

Any misuse of AI in:

- coursework
- controlled assessments
- mock examinations
- public examinations

will constitute malpractice.

The school will take reasonable steps to prevent and investigate AI-related malpractice in accordance with the Exams Policy, NEA Policy, JCQ Regulations and the Student Digital Code of Conduct.

## **9. Safeguarding and Online Safety**

The school recognises that AI technologies may create safeguarding risks including:

- cyberbullying
- harassment
- impersonation
- deepfake abuse
- grooming
- harmful content generation
- extremist material
- misinformation
- sexual exploitation
- harmful, manipulative or sexualised AI chatbot interactions
- over-reliance on AI that may reduce independent thinking or help-seeking
- emotional dependency on AI systems that may undermine healthy relationships or safeguarding disclosures

Any safeguarding concern involving AI must be reported immediately to the DSL.

The school's filtering and monitoring systems, including GoGuardian, Smoothwall and other safeguarding systems, support the monitoring of online activity on school-managed devices.

The school will respond to AI-related incidents in line with:

- the Safeguarding and Child Protection Policy
- the Behaviour and Pupil Discipline Policy including Anti Bullying Approach
- the Online Safety Policy

## **10. Staff Training**

Staff will receive regular training and updates regarding:

- AI developments
- safeguarding risks
- data protection
- ethical use of AI
- academic integrity concerns
- practical classroom applications

AI guidance may be delivered through:

- safeguarding training
- CPD sessions
- staff briefings
- Staff Portal notices
- departmental discussions

The school will continue to review emerging good practice and national guidance.

## **11. Breaches of this Policy**

### **11.1 Staff**

Breaches by staff will be managed under the Staff Code of Conduct and disciplinary procedures.

Serious breaches may include:

- misuse or unauthorised disclosure of confidential information;
- entering safeguarding, SEND, medical, assessment or personnel data into unapproved AI systems;
- failure to report an AI-related data breach or safeguarding concern;
- unsafe or inappropriate use of AI with students;
- generation, sharing or publication of inappropriate, discriminatory or misleading material;
- use of AI to impersonate another individual;
- use of AI in a manner that undermines academic integrity or examination regulations;
- inappropriate reliance on AI in professional decision-making without adequate human oversight;
- use of AI in safeguarding processes in a manner contrary to this policy;
- use of AI to generate inappropriate, offensive or harmful content using school systems or devices.
- breaches of the Staff Code of Conduct, safeguarding requirements, data protection legislation or professional standards.

Depending on the nature and seriousness of the breach, this may result in management action, formal disciplinary procedures, referral to external agencies, or other sanctions as appropriate.

### **11.2 Students**

Breaches by students will be managed in line with:

- the Behaviour and Pupil Discipline Policy including Anti Bullying Approach
- the Online Safety Policy
- the Exams Policy
- safeguarding procedures where relevant

Sanctions may include:

- detention
- withdrawal of device/network privileges
- internal suspension, external suspension or permanent exclusion
- safeguarding intervention
- examination malpractice procedures

## **12. Monitoring and Review**

AI technologies evolve rapidly. This policy will therefore:

- be reviewed at least annually and more frequently if deemed necessary
- remain under ongoing review as guidance and technologies develop

The school will continue to evaluate:

- educational effectiveness
- safeguarding implications
- staff and student feedback
- legal and regulatory developments

## **13. Links with Other Policies**

This policy should be read alongside:

- Safeguarding and Child Protection Policy
- Online Safety Policy
- Student Digital Code of Conduct
- Behaviour and Pupil Discipline Policy including Anti Bullying Approach
- Data Protection Policy
- Exams Policy
- Acceptable Use of IT Policy
- Staff Code of Conduct

## Appendix 1 – Approved AI Tools (as at May 2026)

The following AI tools have been reviewed and approved for use at Tiffin School (by the HT, DPO, Head of IT, CS Department) at the date of publication of this policy.

| Tool                                                                                         | Approved Users | Approved Uses                                                                                                                                                         |
|----------------------------------------------------------------------------------------------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ChatGPT (Open AI)                                                                            | Staff          | Lesson planning, retrieval practice, quiz generation, drafting communications, policy development, administrative support, curriculum planning and revision resources |
| Claude (Anthropic)                                                                           | Staff          | Drafting, summarisation, curriculum planning, policy development, research support and administrative tasks                                                           |
| Google Gemini for Education (via Tiffin Google Workspace)                                    | Staff          | Lesson planning, resource generation, drafting communications, summarisation, retrieval practice, administrative support                                              |
| Microsoft Copilot for Education (where available through the school's Microsoft environment) | Staff          | Drafting documents, summarisation, administrative support, presentation development                                                                                   |
| Google NotebookLM (school-approved accounts only)                                            | Staff          | Summarising documents, curriculum planning, revision resource development                                                                                             |

The school does not currently approve the use of public AI platforms for the processing of personal, safeguarding, SEND, medical, assessment, admissions or personnel data.

The use of any AI platform not listed above requires prior approval in accordance with Section 4 of this policy.

## Appendix 2 – AI Risk Assessment Framework

| Risk Area                          | Example Risks                                                                                                          | Potential Impact                                         | Mitigation / Controls                                                                                                        | Lead Responsib                       |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
| Safeguarding & Student Safety      | Exposure to harmful/inappropriate AI-generated content; unsafe advice; grooming/manipulation risks through AI chatbots | Safeguarding concerns; emotional harm; reputational risk | Filtering/monitoring systems; supervised use; Digital Code of Conduct; staff training; reporting procedures                  | DSL / IT                             |
| Data Protection & GDPR             | Staff/students uploading personal, safeguarding or assessment data into public AI tools                                | GDPR breach; confidentiality breach                      | Clear prohibition on uploading personal/confidential data; approved platforms only; DPIA where required                      | DPO / IT                             |
| Assessment Integrity & Malpractice | AI-generated coursework; plagiarism; unauthorised AI assistance in homework/NEA                                        | Malpractice; invalid assessment evidence                 | Clear assessment guidance; staff vigilance; oral questioning; version histories; sanctions aligned to behaviour/exams policy | Deputy Head Academic / Exams Officer |
| Accuracy & Reliability             | AI hallucinations; fabricated sources; inaccurate academic content                                                     | Misinformation; poor-quality learning                    | Human checking expectations; teacher oversight; critical literacy teaching                                                   | Curriculum Leaders                   |
| Bias & Equality                    | AI outputs reflecting stereotypes or bias                                                                              | Discriminatory outcomes; equality concerns               | Staff awareness training; human oversight; review processes                                                                  | SLT / Inclusion                      |
| Online Safety & Cybersecurity      | Unsafe AI platforms; phishing or malicious AI-generated content                                                        | Cybersecurity incidents                                  | Approved software lists; IT oversight; staff guidance                                                                        | Network Manager                      |
| Staff Professional Conduct         | Over-reliance on AI for reports, references or parent communication                                                    | Reduced professional judgement; reputational risk        | Human accountability retained; review expectations; policy guidance                                                          | SLT                                  |

|                                   |                                                              |                                   |                                                           |                           |
|-----------------------------------|--------------------------------------------------------------|-----------------------------------|-----------------------------------------------------------|---------------------------|
| Intellectual Property & Copyright | Unauthorised use of copyrighted AI-generated content/images  | Copyright infringement            | Staff guidance on licensing and attribution               | IT / Deputy Head Academic |
| Operational & Reputational Risk   | Inconsistent AI use across departments; public complaints    | Loss of confidence; inconsistency | Central policy; governor oversight; phased implementation | Headteacher / Governors   |
| SEND & Accessibility              | AI tools used inconsistently for access arrangements/support | Inequitable provision             | SEND oversight; approved accessibility tools              | SENCo                     |