PARMITER'S SCHOOL

Artificial Intelligence (AI) Policy

1. Purpose, Aims, and Scope

1.1 Purpose and Aims

This policy provides a framework for the safe, ethical and effective use of Artificial Intelligence (AI) across Parmiter's School. AI must always serve education and is intended to complement, not replace, the professional role of teachers, the integrity of learning, or human decision-making in educational and administrative contexts.

This policy aims to:

- Enhance educational outcomes for students and support staff in their professional duties.
- Promote equity in education by addressing learning gaps and providing personalised support, ensuring accepted AI resources are accessible to all students, irrespective of background or abilities.
- Prepare all stakeholders for a future in which AI technology will be an integral part of society.
- Uphold the highest standards of data privacy, security, transparency and accountability in AI usage.

1.2 Scope and Application

This policy applies to all staff, students, governors, contractors and visitors using AI-enabled systems or personal devices within Parmiter's School. It covers AI use in teaching, learning, assessment, administration and safeguarding. Safeguarding responsibilities are always prioritised ahead of any benefits of AI.

2. Legal and Regulatory Framework

2.1 Legal Compliance

AI use must comply with all relevant UK legislation and guidance, including:

- UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018.
- Keeping Children Safe in Education (KCSIE).
- Equality Act 2010.
- Online Safety Act 2023 and the ICO Children's Code (Age-Appropriate Design Code).
- Joint Council for Qualifications (JCQ) guidance on AI use in assessments.

2.2 Regulatory Principles

Parmiter's School follows the five principles set out in the AI regulation white paper:

- **Safety, Security and Robustness:** Ensure AI solutions are secure, safe and protect user data; identify and rectify bias or error; and anticipate threats such as hacking.
- **Appropriate Transparency and Explainability:** Be transparent about the use of AI and ensure that all stakeholders understand the suggestions and outputs it makes.
- **Fairness**: Only use AI solutions that are ethically appropriate, equitable and free from prejudice; closely monitor and correct bias, particularly regarding protected characteristics.
- **Accountability and Governance**: Ensure the governing board and staff have clear roles and responsibilities in the monitoring, evaluation, maintenance and use of AI.
- **Contestability and Redress**: Staff are empowered to correct and overrule AI suggestions (decisions must be made by the user, not the technology); respond appropriately to concerns where AI may have caused error or unfair treatment.

3. Key Definitions

- **Artificial Intelligence (AI):** Technologies that perform tasks requiring human-like reasoning or problem-solving.
- **Generative AI:** Tools that create new content (text, images, video, or audio) in response to prompts.
- **Open Generative AI Tools:** Tools accessible and modifiable by anyone, which may store, share, or learn from the information entered, including personal or sensitive information.
- **Closed Generative AI Tools:** Tools that are generally more secure, as external parties cannot access the data input.
- **Automated Decision-Making:** AI making determinations without human oversight
- **Agentic AI:** AI capable of planning and carrying out actions independently across systems.

- **Wearables/ Wearable technology:** AI-enabled devices worn on the body (such as glasses, pins, or clips) that capture and process data in real-time.
- **AI Literacy:** The ability to use, evaluate and understand AI critically and responsibly.

4. Governance, Oversight and Accountability

- **Accountability:** The Headteacher is accountable for AI governance, supported by the Deputy Head for Digital Strategy, the Designated Safeguarding Lead (DSL) and Data Protection Officer (DPO). The governing body holds ultimate oversight, approving and reviewing this and other relevant policies.
- **Tool Approval:** A Register of AI Digital Tools will record all AI systems approved for use, including their purpose, age appropriateness and data use. This will be maintained and overseen by the Deputy Headteacher, with responsibility for the Digital Strategy.
- **Staff Responsibility:** Staff must refer to the Register rating when considering the use of any AI tool. Staff must use the AI Software Approval form to request new applications or software (See appendix).
- **Consequences:** Individuals shall be held responsible for any misuse or negligence concerning AI systems, which may result in a disciplinary procedure.

5. Staff and Governor Use of AI

5.1 Professional Judgement and Review

AI may be used by staff and governors to prepare resources, adapt materials and improve operational efficiency (e.g., scheduling, summarisation). However, AI cannot replace the judgment and knowledge of a human expert.

- All outputs must be **reviewed and fact-checked** for accuracy, appropriateness, curriculum alignment and bias before use.
- The **quality and content** of any final plans, policies, or documents remain the professional responsibility of the person who produced it, regardless of the tools used.
- Staff must acknowledge or reference the use of Generative AI in their work.

5.2 Parmiter's Acceptable Use Parameters for AI (Red Lines)

Access to generative AI platforms is not restricted on staff devices. Staff are reminded to refer to the ICT & E-safety policy to ensure they are familiar with the acceptable use of AI alongside the following parameters (red lines for the use of AI):

- AI platforms can only be accessed using your school email / Google Account login.

- Do not enter Personal or Sensitive data ***(including names)*** into unauthorised generative AI tools or chatbots. This will be treated as a data breach.
- Do not generate content to impersonate, bully, or harass another person.
- Do not generate explicit or offensive content, or input offensive, discriminatory, or inappropriate content as a prompt.
- Automated decision-making about individuals (admissions, support, discipline) is prohibited without human oversight.
- Students can use AI only within the Google Apps for Education Suite or on the Register of AI Digital Tools.
- Use of AI platforms with students must be directed and have a clear purpose.
- Students **MUST** be briefed each time it's used in learning on the ethical use of AI by the teacher.
- Any use of AI in creating materials must be acknowledged.
- Do not enter student work into any AI system ***(without prior student permission). When it is entered, it should be anonymised.***
- AI must not be used to mark student work, ***but it can be used to support feedback for students.***
- AI must not be used to write complete student reports/gradesheets.

6. Student Use, Teaching and Learning

6.1 AI Literacy and Curriculum

Parmiter's School will ensure the curriculum teaches students about the opportunities and risks posed by AI. Students will be taught to question outputs, recognise bias, understand limitations and use AI critically and responsibly. This will happen in all areas of the curriculum alongside discrete student workshops such as Year 7 Great Big Read Lessons, Year 12 EPQ AI and intellectual integrity sessions.

6.2 Student Use Rules

Student use of AI will be guided, supervised and age-appropriate.

- Students may only use AI tools approved by the school and listed in the Register of Digital AI Tools.
- Students may not create personal accounts, misrepresent their age, or use unapproved platforms.
- Students must adhere to school and JCQ guidance for using AI-generated content, including proper attribution and respect to creators.

6.3 Prohibited Misuse and Plagiarism

AI may not be used for dishonest purposes (e.g. plagiarism, impersonation, or generating work for submission).

- Unattributed use of AI-generated text or imagery is considered **plagiarism** and will be dealt with within our school's Malpractice Policy.
- Where AI use is permitted for preparatory work, students must acknowledge this transparently, including the tool, date and purpose.
- Students must not generate or share explicit or offensive content, including inappropriate or sexualised images.

7. Assessment and Malpractice

- **Assessment Integrity:** All work submitted must be the student's own. AI may support preparation but must not substitute for assessed work, including internal and external assessments and coursework.
- **Assessment Design:** Teachers will design tasks that encourage originality, process and higher-order thinking, avoiding over-reliance on repetitive or easily automated assessment opportunities.
- **Malpractice:** Misuse will be treated as malpractice in line with JCQ regulations and school malpractice procedures.

8. Data Protection, Consent and Intellectual Property

8.1 Data Protection and Consent

- **Lawful Basis:** The school will identify and record the lawful basis for AI-related processing of personal data.
- **Data Minimisation:** Only the minimum necessary data will be shared. Special category data (health, biometrics, SEND) will not be used without explicit authorisation.
- **Consent**: Parental consent will be sought where data use is not strictly necessary for education or safeguarding.
- **Transparency**: Parents and students will be informed how data is collected, stored and protected.

8.2 Intellectual Property (IP) and Procurement

- **Student IP:** Students own the IP rights to original content they create. Student work must not be used by staff to train generative AI models without appropriate consent or exemption.

- **Vendors**: Vendors must confirm that school data will not be used to train models for other customers.
- **Procurement**: Procurement will consider value, sustainability and ethics. Tools that monetise student behaviour or involve targeted advertising are prohibited. Free trials involving personal data must be DPO-approved.

9. Equity, Access, and Inclusion

- AI adoption must not disadvantage students because of digital poverty, SEND needs, or language barriers.
- Homework and assessments will never assume access to paid AI tools at home. Alternative routes to learning will always be provided.
- AI may be used to support accessibility (e.g. speech-to-text, translation) under staff supervision, but must not create new disparities in access or utilisation.

10. Agentic AI and Wearable Devices

10.1 Agentic AI

Agentic AI (systems that plan and act independently) must not be introduced without senior approval. All actions must be logged, transparent and reversible. Human oversight is required at all times. Agentic AI must not be used for pastoral monitoring, profiling, or discipline.

10.2 Wearable AI Devices (*including:* Glasses, Pins, Clips, etc.)

Wearable AI devices can present material risks to privacy, safeguarding, assessment integrity and data protection.

- These devices are **only permitted** on site or in lessons if they are authorised for a **defined educational or accessibility purpose**, with prior approval recorded in the Register of AI Digital Tools.
- **Recording:** Live recording, transcription, translation, or streaming is prohibited in classrooms and communal areas without written approval. Use is never permitted in toilets, changing rooms, medical rooms, or any other sensitive location.
- **Accessibility**: Where a student's needs suggest potential benefit, a case-by-case adjustment will be considered, requiring a risk assessment by the SEND lead and/or DPO, clear parameters for use and staff supervision.

11. Safeguarding, Online Safety and Wellbeing

- **Safeguarding**: AI-related risks (deepfakes, impersonation, grooming, harmful content) are safeguarding concerns and must be reported immediately to the DSL.
- **Online Safety:** Staff will supervise the use of AI tools embedded in digital platforms and ensure students are protected from harmful or inappropriate outputs.
- **Wellbeing**: AI will not be used as a substitute for pastoral care. Students will be taught that AI cannot provide emotional care or wellbeing support. Staff will monitor for signs of dependency or overuse.

12. Training and Professional Development

All staff, governors and parents will be provided with role-specific training and information where appropriate and when available to ensure they understand the opportunities and risks posed by AI and can use applications appropriately.

13. Incident Response and Breach of Policy

13.1 Incident Response

AI-related incidents will be reported through existing procedures:

- **Academic Malpractice:** Identify the concern, discuss it with the student, log evidence and escalate to the Deputy Headteacher overseeing Examinations/DSL, and they will follow the Exams Malpractice policy.
- **Harmful or Inappropriate Content:** Close the tool, screenshot evidence and report to the DSL and Network Resources.
- **Data Breach via AI Platform:** Report immediately to the DPO, who will investigate, contain and log the breach.
- **Deepfakes or Impersonation:** Secure evidence and report immediately to the DSL/DPO for escalation to leadership and, if needed, the police.

14. Review and Evaluation

This policy will be reviewed annually, or sooner if law or risk changes. The governing body will be asked to review this policy. Feedback from students, staff and parents will be used to inform updates and the ongoing evaluation of AI use in school.

Appendix:

*Appendices 1 and 2 are combined to form our **AI Software Approval form**, which in turn makes our **Register of AI Digital Tools.***

Appendix 1: AI Tool Risk Assessment Checklist

A one-page guide for staff and leaders considering a new AI tool.

Step 1: Educational Purpose

- Does the tool clearly support learning or workload reduction?
- Is it aligned with curriculum or safeguarding priorities?

Step 2: Safeguarding and Age Appropriateness

- Does the tool meet age restrictions (13+, 18+)?
- Could students encounter harmful or unmoderated content?
- Does it allow unsupervised chat or sharing?

Step 3: Data Protection

- What personal data does it collect (names, images, voice, location)?
- Where is data stored (UK/EU/elsewhere)?
- Has the vendor confirmed data will not be used to train models for others?

Step 4: Inclusion and Access

- Can all students access it fairly (SEND, EAL, digital poverty)?
- Is there a non-AI alternative for homework?

Step 5: Practicalities

- Is it affordable and sustainable?
- Is there environmental disclosure on energy use?

Decision:

- Approved by [insert role]
- Referred to DSL/DPO for review
- Not approved

Note: These questions will be asked on the AI platform request form before approving any AI tool.

Appendix 2: Vendor Due Diligence Questions

Questions to ask when evaluating an AI platform.

Company and Contracts

- Who is the contracting organisation?
- Where is it based and who are its data processors?
- Is there a Data Processing Agreement?

Data Protection

- Where is student data stored?
- Will data be used to train models for others?
- What is the deletion process when the contract ends?

Safeguarding

- Minimum age for use?
- Content moderation and safety measures in place?

Inclusion and Environment

- Is it accessible to SEND and EAL students?
- Is it affordable and sustainable?
- What is the environmental impact?

Accountability

- Does the vendor provide transparency reports or audit logs?
- Breach notification within 72 hours?

Note: These questions will be asked on the AI platform request form before approving any AI tool.

Appendix 3: AI Incident Response *(Any incidents should initially be reported to ABA via this form).* ***ALL Safeguards concerns MUST be reported via CPOMS!***

A quick reference for staff when things go wrong.

A. Academic Malpractice

- Identify concern (suspicious work).
- Compare with student's known work; discuss with student.
- Log evidence and escalate to the Deputy Headteacher (ABA) overseeing Exams.
- DSL informed if safeguarding concern arises.

B. Harmful or Inappropriate Content

- Close the tool; screenshot evidence if safe.
- Report to DSL.
- DSL assesses risk, informs parents as appropriate.
- Deputy Headteacher (ABA) lead reviews tool approval.

C. Deepfakes or Impersonation

- Secure evidence (files, URLs).
- Report immediately to DSL and Network Resources.
- DSL/DPO escalate to leadership and, if needed, police.
- Communications agreed to protect wellbeing and reputation.

D. Data Breach via AI Platform

- Report immediately to DPO.
- DPO investigates, contains and logs breach.
- Decide if ICO notification is needed.
- Parents/Carers informed if there is risk of harm.

E. Wearable AI Misuse

- Device removed and stored securely.
- Incident logged; DSL and DPO informed.
- Repeated breaches handled under behaviour and safeguarding policies.

F. Student Wellbeing Concern

- Teacher notices dependency or misuse.
- Raise with the Form Tutor/Head of Year.
- DSL assesses safeguarding concerns.
- Parents/Carers engaged to support balanced use.