

Responsible Artificial Intelligence Use

Executive Summary

This Responsible AI Usage Policy outlines Epina Business & Enterprise School's ("Epina School") approach to implementing and using Artificial Intelligence (AI) technologies in our educational setting. Key points include:

1. Our commitment to safe, ethical, and effective use of AI in alignment with DfE guidance, Ofsted expectations and the DfE's Generative AI Product Safety Expectations;
2. Guidelines for selecting, implementing and monitoring AI tools with robust safeguarding measures;
3. Clear roles and responsibilities for staff, pupils and leadership in AI usage;
4. Comprehensive measures to protect data privacy, intellectual property and student welfare;
5. Strategies for preparing pupils for an AI-enhanced future while maintaining academic integrity; and
6. Recognition of environmental impact and sustainable AI practices;

This policy aims to harness the benefits of AI while mitigating potential risks, ensuring that our use of AI enhances teaching, learning, and administrative processes without compromising our educational values, safeguarding responsibilities or stakeholders' rights.

1. Introduction

At Epina School, we recognise the immense potential of Artificial Intelligence (AI), including generative AI and large language models (LLMs), to enhance school leadership, teaching, learning, and administrative processes. This policy outlines our approach to implementing and using AI technologies in a responsible, ethical and effective manner, in alignment with:

- Department for Education (DfE) Generative AI in Education guidance
- DfE Generative AI Product Safety Expectations
- Keeping Children Safe in Education statutory guidance
- Ofsted expectations
- Our school's values and educational philosophy

Key DfE Position: "If used safely, effectively and with the right infrastructure in place, AI can support every child and young person, regardless of their background, to achieve at school and college and develop the knowledge and skills they need for life."

2. Purpose

The purpose of this policy is to:

- Ensure the safe, secure, and appropriate use of AI technologies within our school in compliance with DfE Product Safety Expectations
- Promote transparency and accountability in AI implementation with robust human oversight
- Safeguard the wellbeing and rights of all pupils and staff, including protection from AI-generated harmful content
- Align our AI use with educational goals, DfE guidance, and OFSTED expectations
- Harness the potential of AI to reduce workload and enhance leadership, teaching, and learning
- Protect intellectual property rights and ensure compliance with UK GDPR
- Prepare our pupils for a future where AI is increasingly prevalent while maintaining academic integrity
- Address emerging safeguarding risks specific to AI technologies

3. Scope

This policy applies to all AI technologies used within Epina School, including but not limited to:

- **Generative AI tools** (e.g., ChatGPT, Google Gemini, Microsoft Copilot, SLT AI)
- **Administrative and productivity tools** with AI features
- **Learning management systems** incorporating AI functionality
- **Assessment and feedback** tools using AI processing

- **Personalised learning platforms** with AI adaptation
- **Data analysis and decision-support systems**
- **AI-integrated educational software and applications**

It covers use by all staff, pupils and any third parties acting on behalf of the school.

Critical Distinction: This policy distinguishes between:

- **Staff use of AI tools** for professional purposes
- **Pupil use of AI tools** (which requires additional safeguards and permissions)

4. Understanding Generative AI

Generative AI refers to technology that can create new content based on large volumes of data. This includes tools that can:

- Answer questions and complete written tasks
- Respond to prompts in a human-like way
- Produce audio, code, images, text, simulations, and videos
- Adapt content for different reading levels and learning needs

Important Limitations to Understand:

- AI systems can produce **hallucinations** (convincing but inaccurate information)
- AI outputs may contain **bias** from training data or system design
- AI cannot **think, understand, or have intentions** - it predicts responses based on patterns
- AI requires **human oversight** and critical evaluation of all outputs
- AI systems are "**black box**" technologies where the decision-making process is not transparent

While these tools offer significant opportunities, it's crucial to understand their limitations and maintain the principle that humans must always remain in the loop.

5. Guiding Principles

Our use of AI technologies is guided by the following principles, aligned with DfE Product Safety Expectations:

5.1 Safety, Security, and Robustness

We are committed to prioritising the safety and security of all users when implementing AI systems:

- **Content Filtering:** All AI tools must include robust content filtering to prevent generation of harmful, inappropriate, or illegal content
- **Activity Monitoring:** AI tool usage is monitored and logged for safeguarding purposes
- **Regular Risk Assessments:** Continuous evaluation of AI tools and their applications
- **Security Standards:** Compliance with cyber security standards for schools and colleges
- **Age-Appropriate Access:** Strict enforcement of minimum age requirements for AI tools

5.2 Transparency and Explainability

We maintain clear communication about how and why AI is used in our school:

- **Clear Documentation:** All AI use is documented and communicated to stakeholders
- **Output Attribution:** When AI is used to create content, this is clearly disclosed
- **Decision Transparency:** AI-assisted decisions can be explained and justified
- **Regular Updates:** Stakeholders receive regular information about AI implementations

5.3 Fairness and Non-Discrimination

We actively work to prevent and address any biases in our AI systems:

- **Bias Monitoring:** Regular evaluation of AI outputs for potential bias
- **Inclusive Design:** Consideration of diverse learner needs in AI implementation
- **Corrective Action:** Prompt response to identified biases or unfair treatment

- Representation: Ensuring AI tools represent diverse perspectives and communities

5.4 Human Oversight and Accountability

We maintain human oversight of all AI systems and their outputs:

- Professional Responsibility: All AI outputs are reviewed by qualified professionals
- Decision Authority: Humans retain final decision-making authority
- Override Capability: Staff can override AI suggestions when professional judgement deems necessary
- Continuous Supervision: No AI system operates without human monitoring

5.5 Data Protection and Privacy

We adhere to all relevant data protection regulations:

- UK GDPR Compliance: Strict adherence to data protection legislation
- Lawful Basis: Clear legal basis for all data processing through AI systems
- Data Minimisation: Only necessary data is processed by AI tools
- Consent Management: Appropriate consent obtained where required
- Right to Erasure: Systems that support data subject rights

5.6 Intellectual Property Protection

We respect and protect intellectual property rights:

- Copyright Compliance: Ensuring all AI use respects copyright law
- Student Work Protection: Safeguarding pupils' intellectual property rights
- Permission Protocols: Clear processes for obtaining necessary permissions
- Secondary Infringement Prevention: Avoiding use of potentially infringing AI outputs

6. Roles and Responsibilities

6.1 School Leadership

- Overall responsibility for AI strategy and policy compliance
- Ensuring alignment with DfE guidance and Product Safety Expectations
- Resource allocation for safe AI implementation
- Regular policy review and updates
- Designated Senior Leader responsible for digital technology strategy

6.2 Data Protection Officer (Chapman)

- Conducting Data Protection Impact Assessments for AI tools
- Ensuring UK GDPR compliance
- Advising on lawful basis for AI data processing
- Managing data subject rights regarding AI use

6.3 Designated Safeguarding Lead (DSL)

- Monitoring AI-related safeguarding risks
- Responding to AI-related safeguarding concerns
- Ensuring filtering and monitoring systems address AI risks
- Training staff on AI safeguarding considerations

6.4 IT in Schools

- Technical implementation and maintenance of AI systems
- Ensuring security and robustness of AI tools
- Managing access controls and monitoring systems
- Providing technical support and training

6.5 Teaching and Support Staff

- Responsible use of approved AI tools
- Critical evaluation of all AI outputs
- Maintaining human oversight of AI-assisted work
- Reporting concerns or issues with AI systems
- Participating in required training

6.6 Pupils

- Ethical use of approved AI tools (where permitted)
- Understanding limitations and responsible use
- Reporting concerns to staff

- Respecting intellectual property and academic integrity rules

7. Implementation Guidelines

7.1 Selection and Procurement

We carefully select AI tools that align with DfE Product Safety Expectations:

Enterprise vs. Free Tools:

- **Preference for Enterprise Tools:** Professional AI tools with organisational controls
- **Prohibition of Free Personal Accounts:** Staff must not use personal AI accounts for school work
- **Safety Features Required:** Content filtering, activity monitoring, data protection controls
- **Educational Suitability:** Tools designed for or adapted to educational contexts

Evaluation Criteria:

- Compliance with DfE Product Safety Expectations
- Alignment with educational objectives
- Data protection and security features
- Age-appropriate safeguards
- Evidence of effectiveness in educational settings

7.2 Data Management and Protection

Critical Requirements:

- **Avoid Identifiable Data:** Staff must not input personally identifiable pupil or staff information into AI tools unless the tool is explicitly approved for such use by the school and meets all data protection requirements.
- **Approved Tools Only:** Only use AI systems that have been reviewed and approved by the school, with appropriate data privacy and security measures in place.
- **No Unauthorised Training:** Ensure AI tools do not use school data for model training unless explicit consent and contracts are in place.
- **Data Retention Awareness:** Staff must understand how long data is stored by any AI tool used and ensure this aligns with school policy and legal obligations.

Safe Practice Guidelines:

- Remove or anonymise identifiable data before using AI tools unless the tool has been verified as safe for processing such data.
- Use pseudonyms or generalised examples where appropriate.
- Conduct regular audits of AI tool data practices to ensure ongoing compliance.
- Maintain and follow clear protocols for responding to any data breaches involving AI tools.

7.3 Training and Support

Mandatory Training Requirements:

- **Foundation Training:** All staff must complete AI CPD
- **Role-Specific Training:** Tailored training for different staff roles
- **Ongoing Professional Development:** Regular updates on AI best practices
- **Critical Thinking Skills:** Training on evaluating AI outputs

Training Components:

- Understanding AI capabilities and limitations
- Recognising hallucinations and bias
- Data protection and intellectual property awareness
- Safeguarding considerations specific to AI
- Practical skills for effective AI use

7.4 Monitoring and Evaluation

Systematic Monitoring:

- Regular assessment of AI tool effectiveness
- Monitoring for misuse or inappropriate outputs
- Gathering feedback from staff, pupils, and parents
- Annual review of AI implementation

Key Performance Indicators:

- Staff confidence in using AI tools safely
- Reduction in administrative workload
- Quality of AI-generated resources
- Safeguarding incident tracking

Use the AI Implementation Plan Template in Appendix B to guide new AI tool introduction.

8. AI in Teaching and Learning

8.1 Opportunities

When used appropriately, AI has the potential to:

- **Reduce Administrative Workload:** Streamlining planning, assessment, and communication tasks
- **Enhance Personalised Learning:** Adapting content for different abilities and needs
- **Support SEND Provision:** Creating accessible resources and alternative formats
- **Improve Resource Quality:** Generating high-quality, curriculum-aligned materials
- **Free Teacher/Leader Time:** Allowing focus on direct teaching and pupil interaction

8.2 Limitations and Safeguards

Key Limitations:

- AI may produce inaccurate, inappropriate, biased, or outdated information
- AI cannot replace human expertise, judgement, or subject knowledge
- AI-generated content requires professional review and adaptation
- AI tools may not understand local context or specific pupil needs

Required Safeguards:

- **Human Oversight:** All AI outputs must be reviewed by qualified staff
- **Professional Judgement:** Teachers and leaders retain authority over educational decisions
- **Quality Assurance:** Regular checking of AI-generated resources
- **Pedagogical Alignment:** Ensuring AI use supports effective teaching practices

8.3 Use in Assessments

Formal Assessments:

- Compliance with Joint Council for Qualifications (JCQ) guidance
- Clear procedures for preventing AI malpractice
- Student education about appropriate AI use in assessments
- Detection and response protocols for suspected misuse

Formative Assessment:

- AI tools may support assessment creation and feedback generation
- All assessment decisions remain with teaching professionals
- Transparency required when AI assists in assessment processes

8.4 Homework and Independent Study

Policy Requirements:

- Clear guidance to pupils about when AI use is/isn't permitted
- Regular review of homework policies to account for AI availability
- Focus on tasks that promote genuine learning rather than AI completion
- Education about over-reliance risks

9. Data Protection and Intellectual Property

9.1 UK GDPR Compliance

Lawful Basis Requirements: Before using AI tools with personal data, we must establish one of the following lawful bases:

- Consent (with clear understanding of AI processing)
- Contract (where AI processing is necessary for service delivery)
- Legal obligation (compliance with statutory requirements)
- Public task (performing official functions)
- Legitimate interests (where balanced against individual rights)

Special Category Data:

- Enhanced protections for sensitive personal data
- Additional consent requirements
- Careful consideration of necessity and proportionality

9.2 Intellectual Property Protection

Student Work Rights:

- Students automatically own copyright to their original work
- Permission required before using student work with AI tools
- Parental consent needed for students under 18
- Clear opt-out mechanisms for data use
- Copyright Compliance:
 - No use of copyrighted material without permission
 - Awareness of secondary copyright infringement risks
 - Avoiding public sharing of largely AI-generated content
 - Respecting licensing terms of educational resources

Staff-Created Content:

- Clear ownership agreements for AI-assisted work
- Protection of school intellectual property
- Guidelines for sharing AI-generated resources

9.3 Consent and Permissions

Student Consent Framework:

- Age-appropriate consent processes
- Clear explanation of AI use and implications
- Easy withdrawal mechanisms
- Regular review of consent status

Transparency Requirements:

- Clear privacy notices explaining AI data processing
- Information about AI training data use
- Details of data retention and deletion policies
- Contact information for data protection queries

10. Safeguarding Considerations

10.1 Emerging AI-Specific Risks

Critical Safeguarding Risks:

- **AI-Generated Child Sexual Abuse Material:** Using AI to create, manipulate, or distribute illegal content
- **Deepfakes and Manipulation:** Creating false content that could harm reputation or wellbeing
- **Grooming and Exploitation:** AI avatars or chatbots used for harmful purposes
- **Misinformation and Radicalisation:** AI-generated extremist or misleading content
- **Over-reliance and Social Isolation:** Excessive dependence on AI rather than human interaction

10.2 Preventive Measures

Robust Filtering and Monitoring:

- AI tools must include content filtering capabilities
- Real-time monitoring of AI tool usage
- Regular review of filtering and monitoring reports
- Integration with existing safeguarding systems

Staff Training Requirements:

- Recognition of AI-generated harmful content
- Understanding of AI-specific grooming techniques
- Response protocols for AI-related safeguarding concerns
- Regular updates on emerging threats

Pupil Education:

- Age-appropriate education about AI risks
- Critical thinking skills for evaluating AI content
- Understanding of digital footprints and privacy
- Promotion of healthy relationships with technology

10.3 Response Protocols

Incident Management:

- Clear reporting procedures for AI-related concerns
- Integration with existing safeguarding processes
- Liaison with external agencies where appropriate
- Support for affected pupils and families

Policy Updates:

- Regular review of safeguarding policies to address AI risks
- Coordination with behaviour and online safety policies
- Integration with child protection procedures

11. Academic Integrity

11.1 Clear Expectations

Academic Honesty Standards:

- Students must submit work that represents their own thinking and effort
- Any AI assistance must be appropriately acknowledged
- Clear boundaries between acceptable and unacceptable AI use
- Understanding that AI use without disclosure constitutes academic misconduct

11.2 Detection and Prevention

Professional Judgement Approach:

- Staff knowledge of students' typical work patterns
- Inconsistencies in writing style, vocabulary, or complexity
- Unreferenced claims or unusual factual content
- Manual checking prioritised over automated detection tools

Limitation of Detection Tools:

- AI detection tools are unreliable and may discriminate
- False positives can unfairly impact students
- Professional judgement remains the primary detection method
- No automated AI detection without human verification

11.3 Educational Response

Teaching Academic Integrity:

- Embedding discussions about AI and academic honesty
- Helping students understand learning processes
- Designing assignments that are difficult to complete with AI alone
- Promoting intrinsic motivation for learning

Assessment Design:

- Tasks requiring personal reflection and reasoning
- Process-based assessments showing working

- Practical applications and real-world problem-solving
- Oral assessments and presentations

12. Environmental Considerations

12.1 Sustainability Awareness

Environmental Impact Recognition:

- AI systems require significant energy for training and operation
- Data centres consume substantial water resources
- Carbon footprint considerations for frequent AI use
- Preference for smaller, more efficient AI models where appropriate

12.2 Responsible Usage

Sustainable Practice Guidelines:

- Consider whether AI is the most appropriate tool for each task
- Avoid unnecessary generation of multiple images or lengthy outputs
- Use existing resources before generating new AI content
- Balance educational benefits against environmental costs

13. Preparing Pupils for the Future

13.1 AI Literacy Development

Core Competencies:

- Understanding how AI systems work at an age-appropriate level
- Recognising AI-generated content and its limitations
- Critical evaluation of AI outputs for accuracy and bias
- Ethical considerations in AI use and development

Curriculum Integration:

- Computing curriculum enhanced with AI understanding
- Cross-curricular applications of AI concepts
- Career exploration in AI-related fields
- Real-world examples of AI impact on society

13.2 Digital Citizenship

Responsible Technology Use:

- Understanding privacy and data protection in AI context
- Respecting intellectual property in the age of AI
- Recognising manipulation and misinformation
- Developing healthy relationships with AI technologies

13.3 Future Skills Preparation

Essential Capabilities:

- Critical thinking and source verification
- Human-AI collaboration skills
- Creative problem-solving that complements AI
- Emotional intelligence and interpersonal skills
- Adaptability to technological change

14. Complaint and Redress Procedures

14.1 Reporting Mechanisms

Multiple Reporting Channels:

- Standard school complaints procedure for AI-related concerns
- Dedicated process for urgent AI safety issues
- Anonymous reporting options for sensitive matters
- Clear escalation procedures for serious incidents

14.2 Response Framework

Investigation Process:

- Prompt acknowledgement of all AI-related complaints
- Thorough investigation by appropriately trained staff
- Clear communication with complainants about progress
- Documentation of all investigations and outcomes

Resolution and Learning:

- Appropriate remedial action where issues are identified
- Learning from incidents to improve policies and procedures
- Communication of changes to relevant stakeholders
- Regular review of complaint patterns and trends

15. Monitoring and Review

15.1 Regular Policy Review

Review Schedule:

- Annual comprehensive policy review
- Quarterly updates from ICT In Schools for emerging issues
- Immediate review following significant AI developments
- Integration with broader school policy review cycles

Review Criteria:

- Compliance with updated DfE guidance
- Effectiveness in managing identified risks
- Staff, pupil, and parent feedback
- Technological developments and new tools

15.2 Continuous Improvement

Data-Driven Evaluation:

- Regular monitoring of AI tool usage and effectiveness
- Analysis of safeguarding incidents and complaints
- Assessment of educational outcomes and workload impact
- Benchmarking against sector best practices

Stakeholder Engagement:

- Regular consultation with staff on AI policy effectiveness
- Pupil voice in AI policy development and review
- Parent and community feedback on AI implementation
- Professional network sharing and learning

16. Related Policies and Documents

This policy should be read in conjunction with the following:

Core School Policies:

- Data Protection Policy
- Safeguarding and Child Protection Policy
- Teaching and Learning Policy
- Assessment Policy
- Online Safety Policy
- Acceptable Use Policies (Staff and Pupils)
- Behaviour Policy
- SEND Policy

External Guidance:

- [DfE Generative AI in Education](#)
- [DfE Generative AI Product Safety Expectations](#)
- [Keeping Children Safe in Education](#)
- [JCQ AI Use in Assessments](#)
- [UK GDPR and Data Protection Act 2018](#)
- [Meeting Digital and Technology Standards in Schools and Colleges](#)

Policy approved by Governors: June 2026

Date of next review by Governors: June 2027