

Responsible AI & Online Safety Policy

Maxwell and other AI-enabled services operated by Sunbury Education Limited

Document owner	Founder & Director (AI and online-safety accountable owner)
Applies to	Maxwell, AI-assisted education, assessment, tutoring, content generation, school pilots, staff use of AI and learner-facing AI interactions
Status	Draft for formal adoption
Proposed effective date	15 October 2026
Review cycle	At least annually and after material legal, safeguarding, security or product changes
Next review	October 2027
Approval	To be approved and signed by the Founder & Director before reliance on this policy

1. Purpose

This policy governs the safe, responsible and educationally appropriate use of artificial intelligence by Sunbury Education Limited (SEL), including Maxwell. It is intended to protect learners, support teachers and ensure that AI complements - rather than replaces - professional judgement and the teacher-learner relationship.

2. Core principles

- Learner safety and the best interests of the child come before speed, novelty or commercial benefit.
- AI is assistive. Humans remain accountable for consequential educational, safeguarding and disciplinary decisions.
- AI outputs may be inaccurate, biased, incomplete or inappropriate and must be treated as fallible.
- Learner-facing AI must be age-appropriate, privacy-conscious and designed to discourage unnecessary disclosure of personal information.

- Assessment claims must be evidence-based; absence of evidence must not automatically be treated as failure.
- Accessibility, SEND and language needs should be considered in design and evaluation.
- AI use must be transparent enough for users and partner schools to understand its role and limitations.

3. Permitted uses

Subject to role, configuration and school agreement, AI may be used to:

- provide explanations, guided questions, hints and practice;
- support formative assessment and identify possible misconceptions for teacher review;
- assist teachers with preparation, differentiation, feedback drafts and administrative summaries;
- generate or adapt learning materials subject to review;
- support multilingual or accessibility features where quality and safety are monitored;
- analyse de-identified or appropriately protected evidence for evaluation and improvement.

4. Prohibited or restricted uses

- AI must not make final safeguarding decisions, statutory referrals, diagnoses, disciplinary exclusions or other high-impact decisions about a child.
- AI must not represent itself as a doctor, therapist, emergency service, safeguarding professional or substitute for a teacher.
- AI must not be used to manipulate, shame, coerce or unfairly profile learners.
- Staff and learners must not enter passwords, payment credentials, unnecessary health data, detailed safeguarding records or other highly sensitive information into unapproved AI tools.
- AI-generated content must not be treated as automatically accurate, authoritative or suitable for publication or assessment.
- AI must not be used to circumvent examination rules, awarding-body requirements, copyright restrictions or school policies.

5. Human oversight and assessment

Teachers and authorised staff retain professional judgement. Maxwell may provide evidence, suggestions, classifications or draft feedback, but high-stakes conclusions require human review. Where AI supports formative assessment, the system should distinguish evidence gathered from inference and preserve appropriate provenance.

For pilots, schools should know what AI is doing, what data is used, what outputs teachers will see, and which decisions remain exclusively human.

6. Safeguarding and online safety

- Learner-facing AI should use safety controls, age-appropriate interaction patterns and monitoring proportionate to risk.

- Users should be encouraged not to disclose unnecessary personal or sensitive information.
- Potential safeguarding content must be routed to an authorised human process; AI must not determine whether a child is safe.
- If a learner indicates immediate danger or a serious safeguarding concern, the service should direct them to an appropriate trusted adult or emergency route and trigger any agreed human escalation available in the deployment.
- Schools' safeguarding policies and DSL procedures take precedence during school deployments.

7. Accuracy, bias and quality assurance

SEL will test important AI-assisted workflows for accuracy, consistency, bias, age appropriateness and failure modes. New or materially changed features should be evaluated before broad learner use. Where confidence is inadequate or evidence is unavailable, the system should avoid unsupported claims and enable review or escalation.

8. Privacy and provider controls

- Personal data sent to AI providers must be limited to what is necessary for the authorised function.
- Provider contracts and settings should, where available, restrict training on SEL/customer content and unnecessary retention.
- Sensitive domains such as safeguarding, health and special-category data require explicit authority and tighter controls.
- Logs and evaluation datasets should be minimised, access-controlled and retained only as long as necessary.
- Any material change in provider, model or data flow must be reviewed for privacy, security and safety impact.

9. Learner transparency and academic integrity

Learners should understand when they are interacting with AI, its limitations, and when a teacher will review their work. SEL will promote legitimate learning use and discourage use that replaces the learner's own thinking or breaches school or examination rules.

10. Accessibility and inclusion

AI features should be designed and evaluated with diverse learners in mind, including SEND, working-memory, attention, numeracy, literacy and language needs. Accessibility support should not reduce academic expectations unfairly; it should remove avoidable barriers while preserving valid evidence of learning.

11. Incident management and complaints

Unsafe, discriminatory, privacy-invasive or materially incorrect AI behaviour should be reportable. SEL will document significant incidents, investigate root causes, apply mitigations and, where necessary, suspend affected functionality until risks are controlled.

12. Governance and change control

The Founder & Director is accountable for this policy unless responsibility is formally delegated. Material learner-facing AI changes should have an identified owner, purpose, risk assessment, test evidence and release decision. AI deployment does not override safeguarding, privacy, curriculum, assessment or school governance.

References and related documents

DfE - Generative artificial intelligence in education:

<https://www.gov.uk/government/publications/generative-artificial-intelligence-in-education/generative-artificial-intelligence-ai-in-education>

DfE - Safe use of generative AI in education: <https://www.gov.uk/government/publications/safe-use-of-generative-ai-in-education-module-3>

Keeping Children Safe in Education 2026:

<https://www.gov.uk/government/publications/keeping-children-safe-in-education--2>

ICO - Children's Code: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/>

Sunbury Safeguarding & Child Protection Policy: Internal SEL policy

Sunbury Data Protection & Privacy Policy: Internal SEL policy

Approval

Name	Seyed Mostafa Owji
Role	Founder & Director
Signature	
Date	

This policy becomes effective when approved and dated by the authorised signatory.