| **Introduction** | |
| --- | --- |

[School Name] recognises that Artificial Intelligence (AI)-powered tutoring (voice-based or text-based) can provide personalised support and reduce staff workload. This policy outlines how AI tutoring systems may be used safely, ethically, and effectively, ensuring compliance with safeguarding, data protection, and educational best practices.

| **2. Purpose and Scope** | |
| --- | --- |

**Purpose**

* Ensure AI tutoring aligns with curriculum standards and legal/ethical guidelines.
* Protect students from harm or exploitation in AI tutoring contexts.
* Comply with data protection laws (e.g., UK GDPR).
* Clarify lines of accountability so that qualified staff oversee AI tutoring systems.

**Scope**

* Applies to all AI tutoring tools, platforms, or software used with [School Name] students.
* Covers all staff, volunteers, and external providers who develop, manage, or use AI tutoring on behalf of the school.

| **3. Roles and Responsibilities** | |
| --- | --- |

1. **Governing Body / Trust Board**

* Approves and reviews this policy.
* Monitors safeguarding, data protection, and educational impact.

1. **Headteacher / Principal**

* Oversees implementation of AI tutoring.
* Ensures staff have time and training to comply with this policy.

1. **Designated Safeguarding Lead (DSL)**

* Monitors safeguarding incidents involving AI tutoring.
* Advises on risk assessments for new AI features.
* Oversees flagged or concerning content as per the school’s safeguarding procedures.

1. **Data Protection Officer (DPO)**

* Ensures all AI tutor data processing aligns with UK GDPR.
* Oversees Data Protection Impact Assessments (DPIAs) and data sharing agreements.

1. **AI/EdTech Lead**

* Evaluates AI tutoring platforms in consultation with the DSL and DPO.
* Coordinates staff training on AI usage.
* Leads any AI tutoring re-audits or risk assessments.

1. **Teachers and Support Staff**

* Use only approved AI tutoring solutions.
* Remain responsible for final teaching quality and pupil progress decisions.
* Report technical, data, or safeguarding concerns to the DSL, DPO, or AI/EdTech Lead.

| **4. Approval Process** | |
| --- | --- |

**Platform Vetting**

All AI tutoring platforms, including free trials, must be reviewed by the AI/EdTech Lead in consultation with the DSL and DPO before use. Any provider must demonstrate suitable data protection measures and robust safeguarding features.

**Contracts & Agreements**

[School Name] must enter into a written contract and appropriate annexures if necessary (i.e. Data Sharing Agreement or Data Processing Agreement if not covered within the contract), outlining:

* How data is stored, processed, and secured.
* Any relevant third-party data sharing.
* Breach notification obligations.

**Teacher Oversight**

1. Curriculum Lesson Development

* Lessons used by an AI tutor should not be fully machine-generated.
* [School Name] requires the involvement of teaching and curriculum experts in lesson creation and review. This applies to external providers and any teacher-created lessons aided by AI tools.

1. **Educational Outcomes**

* Where AI tutoring providers set goals for each student’s AI tutoring, it is the responsibility of the class teacher to ensure they align with curriculum objectives.
* AI recommendations do not override teacher professional judgment; staff remain accountable for pupils’ academic progress and well-being.

| **5. Safeguarding** | |
| --- | --- |

**Session Supervision**

* AI tutoring sessions should be conducted through school-managed logins; all sessions should be recorded with staff able to request transcripts.

**Flagging & Alerts**

* The AI system must have filters or detection features for harmful or explicit content, automatically flagging concerns.

**Disclosure Handling**

* If a pupil discloses potential abuse or harm within AI tutoring, staff respond as they would to any in-person disclosure, escalating to the DSL immediately.

**Teacher Oversight**

* Staff cannot assume the AI will catch all risks; human vigilance remains vital for spotting bullying, grooming, or other unsafe behaviour.

**Tutoring at Home**

* If AI tutoring is provided off-site or at home, the same safeguarding and data standards apply.
* Providers must give the school the same access to session records or transcripts on request
* Parents/carers should be informed about how sessions work, data collection, and the nature of any possible disclosures.

**Session Records**

* Any AI tutoring platform used by [School Name] must record sessions (or keep transcripts) and have an automated flagging system for harmful content.
* Any AI tutoring platform used by [School Name] must record and transcribe sessions and include an automated red flag system for identifying inappropriate, harmful or safeguarding-related content.
* Flagged interactions should trigger alerts to designated staff for timely review.
* The DSL decides on a monitoring schedule for these records and how any disclosures are handled.

| **6. Equity and Inclusion** | |
| --- | --- |

**SEND / EHC Plans**

* If an AI tutor’s format, pacing, or scaffolding is unsuitable for a SEND/EHC learner, staff consult with the provider to adapt content (e.g., difficulty level, text vs. voice).
* If no suitable adaptation is possible, staff use more specialised human-led support or an alternative intervention.

**Equality and Diversity**

* Teachers must watch for biased or culturally insensitive outputs from the AI.
* Repeated or concerning patterns of bias should be escalated to the AI/EdTech Lead and the provider.

**Digital Divide**

* Where AI tutoring extends beyond school hours, the school attempts to loan devices or provide onsite sessions for pupils lacking reliable hardware or connectivity.
* Staff confirm platform compatibility with mobile/tablet devices to maximise access.

| **7. Data Protection and Privacy** | |
| --- | --- |

**Lawful Basis**

* The school defines a lawful basis (e.g., “public task”) for AI tutoring. If usage extends beyond normal educational provision, parental consent may be needed.

**Data Minimisation**

* AI tutors must collect only minimal personal data needed for effective support (e.g., first name, year group).
* No sensitive data (e.g. health info, EHCP details) may be uploaded into generative AI services unless explicitly anonymised.
* Any data collected for platform development or analysis (e.g. SEND flags) must be anonymised and used solely for internal improvement, not shared externally.

**DPIA & Agreements**

* A Data Protection Impact Assessment (DPIA) is completed for each AI tutoring platform, identifying any high-risk data practices.
* Platforms should adhere to safeguarding and data protection standards equivalent to those audited under national frameworks such as the Department for Education’s National Tutoring Programme.
* The school keeps a record of data sharing agreements.

**Security & Breach Reporting**

* Providers must not share pupil data with unauthorised third parties.
* If voice data is stored or biometric identifiers are used, the school must obtain consent from parents or carers unless an existing agreement permits the school to provide consent on their behalf.
* Providers must promptly report data breaches to [School Name], enabling the school to follow ICO notification procedures if necessary.

| **8. Monitoring and Review** | |
| --- | --- |

**Ongoing Monitoring**

* The SLT and AI/EdTech Lead regularly collect feedback from staff, pupils, and parents on the AI tutor’s educational efficacy, safeguarding reliability, and data compliance.

**Risk Matrix & Re-Audit**

* The school maintains an “AI Tutoring Risk Matrix” to identify issues (e.g., data misuse, negative learning experiences). The AI/EdTech Lead, DSL, and DPO will re-audit the system every [6 or 12] months or after significant platform updates.

**Annual Policy Review**

* The Governing Body (or Trust Board) reviews this policy annually or sooner if major AI or legal changes occur.

| **9. Breaches and Non-Compliance** | |
| --- | --- |

**Staff Disciplinary**

* Failure to follow this policy may result in disciplinary action, up to termination of employment.

**Provider Violations**

* Non-compliant providers risk contract termination or suspension.

**Safeguarding & Data Breaches**

* Severe safeguarding concerns are referred to external agencies in accordance with statutory guidance.
* Data breaches follow the school’s Data Breach Policy and ICO guidelines.