# ONE49: AI Risk Register (updated 18.12.25)

As the use of artificial intelligence (AI) in educational practice continues to expand, it is essential to identify, assess, and manage potential risks to ensure ethical, effective, and responsible implementation. This risk log provides a structured approach to documenting risks associated with AI in our schools, including concerns related to data privacy, bias, transparency, and the impact on teaching and learning. By maintaining this log, we aim to support informed decision-making, safeguard stakeholders, and promote the responsible use of AI technologies within educational settings.

| **AIs covered by this risk log:** |
| --- |
| • Chat GPT<br>• Chalkie AI<br>• Canva<br>• Perplexity<br>• Teachmate AI<br>• CoPilot<br>• Gemini<br>• Ideogram<br>• Diffit<br>• Brisk<br>• Almanac<br>• Twinkle – Ari<br>• SLT AI<br>• Flint AI<br>• KeyGPT |

| Use Case | Risk Rating | Use Description | Risks Associated | Mitigations |
|---|---|---|---|---|
| Pupil interactions | High | Implementing generative AI software to interact with pupils, e.g. providing feedback, assistance | Inaccuracy of responses, lack of empathy, data privacy concerns, potential for bias, alignment with sound pedagogical practice, lack of consent and intellectual property risks | 1. Avoid. AI is not permitted for interactions with pupils. |
| Assessment | High/medium | Using AI to mark assessments | Potential bias in assessment, Inaccuracy, data privacy concerns, consent and intellectual property risks, transparency and acceptance of using AI in the process of assessment, loss of teacher value in the process | 1. Review AI designed assessments for bias and accuracy.<br>2. Ensure student data privacy is maintained by anonymising names and other personal details within the prompt.<br>3. Use AI tools with data protection measures such as Copilot enterprise.<br>4. Clear human moderation process to validate and review AI output. |
| Creating curriculum resources or activities | Low | Using AI to generate lesson activities, lesson plans, presentations and generic educational materials | Inaccuracy of generated content, lack of personalisation for student group, potential bias in resources, pedagogical rigour | 1. Human check on material validity and generated content<br>2. Customisation and adaptation of resources to suit specific classroom needs<br>3. Use educational/workplace logins |
| Parent communications, including emails, letters and postings | Low/medium | Using AI to help draft parent emails or complete student reports. | Over reliance on AI leading to loss of personal touch and empathy, potential data privacy issues | 1. Review and personalise all AI generated materials<br>2. Ensure parent data privacy is maintained by anonymising names and personal details<br>3. Use AI tools with GDPR compliance and strong data protection measures, such as Co-pilot<br>4. Use AI tools that do not train models on your data such as Co-pilot or models that have an option to turn off training data, such as ChatGPT<br>5. Do not synchronise the AI tools with your account<br>6. Use educational/workplace logins |

| Use Case | Risk Rating | Use Description | Risks Associated | Mitigations |
|---|---|---|---|---|
| Data Analysis | Medium/High (Dependent on nature of data being processed) | Analysing performance data and other educational metrics | Misinterpretation of data, potential bias in analysis, data privacy concerns, poor decision making based on lack of understanding of analysis and results | 1. Avoidance. Use Trust/school approved data analysis tools<br>2. Avoid using special category data. This data is subject to strict controls, and therefore schools need to adhere to GDPR regulation and protect this information efficiently<br>3. Cross check AI analysis with manual data review<br>4. Ensure data used is anonymised and privacy compliant<br>5. Use AI tools with data protection measures<br>6. Use AI tools that do not train models on your data or models that have an option to turn off training data |
| Creating notes, minutes and summaries of meetings | Medium/High (Dependent on nature of data being processed) | Using AI to help draft notes/minutes of meetings | Potential for confidential information to be shared in the public domain<br>Inaccuracies arising from error in documentation and interpretation. | 1. Use AI tools with data protection measures such as Copilot enterprise.<br>2. Ensure no information is shared inappropriately either inside or outside the organisation and confidentiality is maintained (subject matter and personal data).<br>3. Review and edit all AI generated materials to ensure accuracy and information for inclusion is appropriately selected and formatted.<br>4. Ensure all parties are notified and are agreeable that AI will be used and meetings recorded for this purpose. |
| All work use | Medium/High | All types of use | Increased risk of data breaches and cyber security attacks | 1. Training for staff in the use of AI and awareness of the risks<br>2. Clear instructions to staff on what AI Tools are approved for use and the importance of setting these up correctly<br>3. Clear instructions to staff not to utilise any tool in such a way that personal and/or confidential information can enter the public domain<br>4. Privacy Assessments and DPIAS carried out on all 'approved' tools and shared with staff. |