AI RISK ASSESSSMENT

2025/26

askKira.com

AI RISK ASSESSMENT TEMPLATE

Sample document for UK Primary & Secondary Schools / Multi-Academy Trusts (MATs)
Aligned with DfE, Ofsted, KCSIE, GDPR, NCSC

This risk assessment, prepared by askKira.com, is designed to help schools assess the risks of AI adoption before implementation. It aligns with DfE guidance, UK GDPR, and best practices in data protection and safeguarding.

SECTION 1: RISK ASSESSMENT OVERVIEW

MAT/School Name	
School(s) Involved	
AI Tool Name	
AI Tool Provider	
AI Tool Purpose	
Date of Assessment	
Assessor's Name & Role	
Final Approval Required By	

SECTION 2: RISK SCORING SYSTEM

This risk assessment follows a standard school risk matrix, helping decision-makers evaluate the likelihood and impact of AI-related risks.

Risk Level	Likelihood	Impact	Score Range	Required Action
Low Risk (1-5)	Rare (1-2)	Minimal (1-2)	1-5	Acceptable with monitoring
Medium Risk (6-10)	Possible (3)	Moderate (3)	6-10	Mitigation plan must be created and signed off by SLT/DPO before deployment
High Risk (11-15)	Likely (4)	Significant (4)	11-15	Immediate action needed
Critical Risk (16-25)	Very Likely (5)	Severe (5)	16-25	AI deployment paused until risk addressed.

Colour Coding

- Green - Low Risk
- Amber - Medium Risk
- Red - High Risk
- Dark Red - Critical Risk

Likelihood:
1 = Rare, 5 = Very Likely

Impact:
1 = Minimal, 5 = Severe

SECTION 3: LEGAL & COMPLIANCE CHECKLIST

- □ Does the AI tool comply with UK GDPR and ICO guidance?
- □ Has a Data Protection Impact Assessment (DPIA) been completed?
- □ Has the school's Data Protection Officer (DPO) reviewed and approved this AI tool?
- □ Does the AI provider follow DfE AI guidance (Jan 2025) and Ofsted EIF?
- □ Does the provider meet Cyber Essentials/NCSC standards?
- □ Are Data Processing Agreements (DPAs) in place?
- □ Is data stored on UK/EU-compliant servers?
- □ Reviewed against KCSIE (2025) for safeguarding?
- □ Is there a process for ongoing compliance checks when regulations change?

SECTION 4: DATA PROTECTION & PRIVACY RISKS

Risk Factor	Yes/No	Risk Level (1-5)	Control Measures / Mitigation
Does the AI tool collect student or staff personal data?			
Is data stored securely on UK-based servers?			
Is access role-based and auditable?			
Are there clear retention and deletion policies?			
Does the provider share data with third parties?			
Are staff, parents, and governors informed?			
Are cybersecurity controls in place (encryption, MFA, breach reporting)?			
Is there an incident response plan including ICO and stakeholder notification?			

SECTION 5: SAFEGUARDING & ETHICAL RISKS

Risk Factor	**Yes/No**	**Risk Level (1-5)**	**Control Measures / Mitigation**
Has the Designated Safeguarding Lead (DSL) reviewed this tool?			
Does it analyse or store safeguarding/behavioural data?			
Has the AI been tested for bias related to SEND, ethnicity, gender, or other protected characteristics?			
Are outputs explainable and teacher-controlled?			
Does the AI support teachers rather than replacing professional judgment?			
Does it consider different learning needs?			

SECTION 5: SAFEGUARDING & ETHICAL RISKS

Risk Factor	Yes/No	Risk Level (1-5)	Control Measures / Mitigation
Does the AI reinforce or potentially amplify cultural or socioeconomic biases relevant to your specific school context?			
How transparent are the AI's decision-making processes to teachers, pupils, and parents?			
Has the AI been tested with a diverse sample representing your school's demographic profile?			

SECTION 6: CYBERSECURITY & TECHNICAL RISKS

Risk Factor	Yes/No	Risk Level (1-5)	Control Measures / Mitigation
Does the AI tool meet UK cybersecurity standards (Cyber Essentials, NCSC guidance, etc.)?			
Has a security vulnerability assessment (IT Health Check) or penetration test (Ethical Hacking) been conducted?			
Who can access the data (teachers, students, third parties)?			
Does the tool integrate securely with existing school systems (MIS, safeguarding software)?			
What happens if the tool is hacked or suffers a data breach?			
What backup and contingency plans are in place if the AI system becomes unavailable during critical education periods?			

SECTION 7: TRAINING & AI GOVERNANCE IN SCHOOLS

Risk Factor	Yes/No	Risk Level (1-5)	Control Measures / Mitigation
Have staff been trained on safe and responsible AI use? (Onboarding & CPD)			
Are feedback and issues reported easily?			
Is an AI policy in place covering responsible use, bias, and security?			
Who is responsible for monitoring the AI's effectiveness and addressing any issues that arise?			
How often will the AI tool be reviewed for effectiveness and risks?			

SECTION 8: STAKEHOLDER CONSULTATION

Risk Factor	Yes/No	Risk Level (1-5)	Control Measures / Mitigation
Have school governors been briefed and consulted on this AI implementation?			
Have parents been informed about the Introduction of this AI tool and how it may interact with their children's education?			
Have relevant teaching unions been consulted regarding any potential impact on staff workload or assessment practices?			
Have pupils been engaged in age- appropriate discussions about how the AI will be used in their learning?			
Are staff clear on when and why AI is used?			
Are outputs acknowledged when used in reports?			

SECTION 9: COST BENEFIT ANALYSIS

Risk Factor	Yes/No	Risk Level (1-5)	Control Measures / Mitigation
What specific educational or administrative problems will this AI tool solve?			
What measurable benefits are expected against the identified risks?			
How does the cost (financial and time) of implementing this AI tool compare to alternative non-AI solutions?			
What is the expected return on investment in terms of staff time saved or educational outcomes improved?			

SECTION 10: AI EXIT STRATEGY

Risk Factor	Yes/No	Risk Level (1-5)	Control Measures / Mitigation
What happens if the AI provider shuts down or discontinues the tool?			
How will data be deleted if the school stops using the tool?			
Are there alternative AI solutions if this tool fails?			

SECTION 11: FINAL RISK ASSESSMENT DECISION

Low Risk (1-5)	Approved for deployment with monitoring
Medium Risk (6-10)	Approved with required mitigation
High Risk (11-15)	Requires further action before deployment
Critical Risk (16-25)	Rejected – AI not suitable for deployment

SECTION 12: REVIEW & SIGN-OFF

Review Stage	Reviewer Name & Role	Signature	Date
Assessor (IT Lead / SLT / Digital Lead)			
Data Protection Officer (DPO)			
Safeguarding Lead (DSL)			
Headteacher / MAT CEO			

This risk assessment should be reviewed annually or whenever significant changes occur to ensure it remains relevant and effective. Regular updates will help schools stay ahead of emerging risks and maintain best practices in AI governance.

REFERENCES

- DfE Generative AI in Education (Jan 2025)
- NCSC Guidelines for Secure AI
- Ofsted EIF (2023)
- KCSIE (2025)
- ICO GDPR Guidance for Schools

This document ensures UK schools and MATs adopt AI safely, ethically, and effectively.