

Artificial Intelligence (AI) Policy

This policy sets out how Innovate2Educate Partnership uses artificial intelligence safely, ethically and effectively to support learning, reduce workload and protect pupils, staff and Trust data.

This policy was approved as follows:

Approver:	Trust Board	Date:	Aug 2026
Owner:	Trust AI Lead / Digital Strategy	Version:	V1.0
LAC adoption date:	Trust-wide policy	Review frequency:	Annual
Status:	Non-statutory	Next review date:	August 2027

This policy applies to all Innovate2Educate Partnership schools, central team employees, Trustees, local governors, workers, volunteers, contractors and pupils when using AI in connection with Trust activity.

Document History

Version	Version Date	Author	Summary of Changes
V1.0	Aug 2026	Trust AI Lead / Digital Strategy	New Trust-wide AI policy. Incorporates current DfE, JCQ, data protection, safeguarding, filtering and monitoring, product safety and assessment guidance.



Contents

1. Statement of intent, aims and scope	6
2. Definitions	6
3. Legal, statutory and guidance framework	7
4. Trust principles for AI use	7
5. Governance, roles and responsibilities	8
6. Approved AI tools, procurement and risk assessment	8
7. Data protection, privacy and cyber security	9
8. Safeguarding, filtering and monitoring	10
9. Fairness, bias, transparency and human oversight	10
10. Intellectual property and copyright	10
11. Use of AI by staff, Trustees and local governors	11
12. Use of AI by pupils	11
13. Assessments, examinations and academic integrity	11
14. AI-enabled wearable and recording-capable devices	12
15. Training and curriculum education	12
16. Concerns, complaints, incidents and breach of policy	13
17. Monitoring and review	13
18. Links with other policies and documents	13
Appendix 1: Approved AI tools and permitted uses	13
Appendix 2: AI tool approval checklist	14

1. Statement of intent, aims and scope

Innovate2Educate Partnership recognises that artificial intelligence (AI), including generative AI, can support excellent education, reduce unnecessary workload, improve access to learning and help pupils develop the knowledge and skills they need for future study, employment and civic life.

We also recognise that AI can create significant risks if it is used without appropriate safeguards. These include risks relating to safeguarding, data protection, cyber security, intellectual property, equality, bias, misinformation, academic integrity, over-reliance, emotional and social development, and the creation or sharing of harmful content.

The aim of this policy is to provide a Trust-wide framework for the safe, ethical, transparent and effective use of AI. It applies to all AI use connected with Trust activity, including teaching and learning, assessment, administration, communications, governance, safeguarding, HR, operational work and pupil use of AI in school.

This policy applies to all Innovate2Educate Partnership schools, the central team, Trustees, local governors, employees, workers, agency staff, volunteers, contractors and pupils. It applies whether AI is accessed through Trust systems, school devices, personal devices, online platforms, applications, browser extensions, embedded features within existing software, or AI-enabled wearable or recording-capable devices.

AI is a tool to support people. It must not replace professional judgement, teacher expertise, safeguarding judgement, accountable leadership, or meaningful human involvement in decisions that affect individuals.

Core position

AI may be used where there is a clear educational, operational or workload benefit, the risks have been assessed, the tool is approved for the intended use, and appropriate human oversight is maintained.

2. Definitions

Term	Meaning
Artificial intelligence (AI)	Computer systems or tools that can perform tasks which normally require human intelligence, such as generating text, analysing information, recognising images or speech, making predictions, identifying patterns or supporting decision-making.
Generative AI	AI that creates new content, such as text, images, audio, video, code, lesson materials, summaries or feedback, based on prompts and training data.
Open AI tool	A tool or service that is publicly available and may store, learn from, share or otherwise use prompts and outputs entered by users. These tools must not be used with identifiable Trust personal data unless specifically approved.
Closed or approved AI tool	A tool approved by the Trust for specified uses after proportionate review of safeguarding, data protection, cyber security, intellectual property, equality and educational risks. Approval may be limited by role, school, age group, subject or purpose.
Personal data	Information relating to an identified or identifiable living person, including pupils, parents/carers, staff, governors, Trustees and others.
Term	Meaning
Special category data	More sensitive personal data requiring additional protection, including information about health, ethnicity, religion, biometric data, sexual orientation and certain other protected information.
AI misuse	Use of AI that breaches this policy or means a pupil, member of staff or other user presents AI-generated output as their own unaided work, uses AI to deceive, cause harm, circumvent safeguarding or security, or process data unlawfully.

3. Legal, statutory and guidance framework

This policy has been written with regard to current legislation, statutory guidance and national guidance relevant to schools and academy trusts. The Trust will keep this policy under review as the law and guidance on AI develops.

- UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 and the Data (Use and Access) Act 2025.
- Keeping Children Safe in Education 2025 and Keeping Children Safe in Education 2026 from 1 September 2026.
- DfE guidance on Generative artificial intelligence (AI) in education.
- DfE Generative AI: product safety standards, including the January 2026 updates on cognitive development, emotional and social development, mental health and manipulation.
- DfE safe use of generative AI in education support materials for schools and colleges.
- DfE Meeting digital and technology standards in schools and colleges, including filtering and monitoring and cyber security standards.
- Online Safety Act 2023 and associated online safety requirements relevant to AI services and harmful content.
- Equality Act 2010 and the Public Sector Equality Duty.
- Copyright, Designs and Patents Act 1988 and relevant intellectual property law.
- Joint Council for Qualifications (JCQ) guidance on AI use in assessments and suspected malpractice, where applicable.

Where guidance changes during the life of this policy, the Trust will apply the most current statutory guidance and will update the policy where required.

4. Trust principles for AI use

- Safety first: AI use must be carefully planned, risk assessed and aligned with safeguarding, online safety, data protection and cyber security requirements.
- Human-centred: AI supports, but does not replace, professional judgement, teacher expertise, safeguarding decisions or accountable leadership.
- Beneficial and proportionate: AI should only be used where the intended use has a clear educational or operational benefit that outweighs the risks.
- Transparent and explainable: staff, pupils and parents/carers should understand when AI is being used in a meaningful way and what its limits are.
- Fair and inclusive: AI use must not discriminate, reinforce bias, disadvantage protected groups or widen inequality of access or outcomes.
- Private and secure: personal data and special category data must not be entered into unapproved AI tools. Data must be processed lawfully, securely and minimally.
- Accurate and checked: AI outputs must be fact-checked, sense-checked and quality assured by an appropriate person before they are relied upon or shared.
- Age-appropriate: pupil-facing AI must be suitable for the pupil's age, needs, vulnerability and educational context, with appropriate supervision.

- **Accountable:** the person using AI remains responsible for the final output, decision, communication or action.

5. Governance, roles and responsibilities

The Trust Board has overall responsibility for ensuring that the Trust has appropriate governance for AI use and that this policy is reviewed at least annually and sooner where there are significant changes in law, guidance, technology or risk.

The Executive Team will oversee strategic implementation of AI across the Trust and ensure that AI use aligns with the Trust's digital strategy, safeguarding expectations, data protection duties, cyber security standards and educational aims.

The Trust AI Lead, or other person designated by the Executive Team, is responsible for coordinating the Trust's approach to AI, maintaining the approved AI tools register, supporting risk assessment and procurement processes, and sharing practice and guidance across schools.

Head Teachers are responsible for the day-to-day leadership of AI use in their schools, ensuring that staff understand this policy, that pupil use is appropriately supervised, and that concerns are reported through the correct channels.

The Data Protection Officer advises on data protection compliance, DPIAs, lawful bases, privacy notices, data sharing and personal data incidents involving AI. The DPO must be consulted before AI tools are approved for processing personal data or where the proposed use is likely to be high risk.

Designated Safeguarding Leads are responsible for advising on safeguarding risks related to AI, recording and responding to AI-related safeguarding concerns, and ensuring that AI risks are reflected in online safety, filtering and monitoring and child protection arrangements.

IT and digital support staff are responsible for advising on technical implementation, access controls, filtering and monitoring, cyber security, device management, logging, account security and system integration.

All staff, Trustees and local governors must use AI only in accordance with this policy, approved uses, data protection and safeguarding requirements, and must report concerns or incidents promptly. Pupils must follow this policy, school rules and acceptable use arrangements when using AI.

6. Approved AI tools, procurement and risk assessment

Only approved AI tools may be used for Trust work where personal data, pupil work, safeguarding information, confidential information or Trust operational information is involved. Open public tools may only be used for low-risk tasks that do not involve identifiable, confidential or sensitive information, unless specifically approved.

Before a new AI tool or AI-enabled feature is approved for Trust use, a proportionate review must be completed. The level of review will depend on the nature of the tool, the users, the data processed, whether pupils use it directly, whether it supports decisions about individuals and whether it introduces safeguarding, bias, cyber or assessment risks.

For pupil-facing or high-risk AI tools, the review must consider the DfE's generative AI product safety standards. In particular, the Trust will seek assurance on filtering, monitoring and reporting, security, privacy and data protection, governance, accountability, fairness, the avoidance of manipulation, and safeguards relating to cognitive, emotional, social and mental health development.

The Trust will maintain an approved AI tools register, setting out each approved tool, approved users, approved purposes, restrictions, data protection status, age restrictions, review date and any required mitigations.

- No AI tool may be used with pupils unless it is age-appropriate, complies with provider terms of use and has appropriate supervision, filtering and monitoring arrangements.
- No AI tool may be procured or enabled for Trust-wide use without considering data protection, cyber security, safeguarding, equality, intellectual property and contractual terms.
- AI tools must not be used for high-stakes decisions about individuals unless a specific lawful process, safeguards and meaningful human oversight have been approved.
- Approval for one purpose does not mean approval for every purpose. Staff must use tools only for the approved use cases.

7. Data protection, privacy and cyber security

AI use must comply with the Trust's Data Protection Policy, ICT and cyber security requirements, acceptable use arrangements and any instructions issued by the DPO, IT team or senior leaders.

Personal data, special category data, safeguarding information, assessment information, confidential staff information and confidential Trust information must not be entered into open or unapproved AI tools. If such information is entered into an unapproved AI tool, it must be reported immediately as a potential personal data breach.

Where AI processing involves personal data, the Trust will identify a lawful basis, provide appropriate privacy information, minimise the data used, apply access controls, ensure appropriate contractual arrangements and consider whether a DPIA is required. The Data (Use and Access) Act 2025 strengthens and refines expectations around lawful, transparent and secure use of personal data, complaints handling and automated decision-making; the Trust will reflect those requirements in AI governance.

Staff must be alert to AI-enhanced cyber risks, including more convincing phishing emails, deepfake audio or video, impersonation, fake payment requests, malicious prompts, data leakage, hallucinated instructions and unverified links or attachments.

- AI-generated emails, letters, reports, resources or code must be checked before use and must not be relied on for legal, safeguarding, financial or HR decisions without appropriate professional review.
- AI-generated content must not be used to bypass Trust security controls, filtering, monitoring, password requirements or approval processes.
- Staff must not use personal accounts, personal devices or personal cloud services to process Trust data through AI unless expressly authorised.
- Any suspected cyber incident, data breach or unsafe AI behaviour must be reported immediately through Trust reporting routes.

8. Safeguarding, filtering and monitoring

AI use must align with the Trust's safeguarding, child protection, online safety and filtering and monitoring arrangements. Safety must be the top priority when deciding whether AI should be used with pupils.

The Trust recognises that AI may create or amplify safeguarding risks, including exposure to harmful or inappropriate content, sexualised or abusive generated images, grooming, sexual extortion, bullying, harassment, impersonation, deepfakes, misinformation, self-harm content, eating disorder content, violent content, extremist content and harmful advice.

Schools must consider whether filtering and monitoring systems are capable of handling real-time, dynamic, personalised and AI-generated content. Where learner-facing AI is introduced, the school must assess whether existing monitoring, alerting and reporting arrangements are sufficient and whether supervisors and DSLs can be alerted to harmful or inappropriate use.

Any AI-related safeguarding concern must be reported immediately to the DSL and handled in accordance with the Trust's Child Protection and Safeguarding Policy. Staff must not attempt to investigate safeguarding concerns outside agreed safeguarding procedures.

- Pupil-facing AI must be supervised and used within clear educational boundaries.
- AI tools must not be used to provide mental health counselling, therapeutic support, safeguarding advice or crisis response in place of human support.
- AI tools must not encourage secrecy, emotional dependence, manipulation or prolonged engagement with pupils.
- Staff must consider the needs of pupils with SEND, pupils with vulnerabilities, pupils with EAL and pupils at different ages and stages when planning AI use.

9. Fairness, bias, transparency and human oversight

AI systems can produce inaccurate, outdated, biased or discriminatory outputs. They may also present uncertain information with confidence. Staff must apply critical judgement to all AI output and must not rely on AI without checking accuracy, context, fairness and suitability.

The Trust will consider equality and bias risks before approving AI tools and will take steps to identify, monitor and address unfair outcomes. Particular care must be taken where AI outputs could affect pupils or staff with protected characteristics, SEND, disadvantage, EAL or other vulnerabilities.

Where AI materially supports a decision, communication or assessment affecting an individual, there must be meaningful human oversight. The responsible person must be able to explain the basis for the final decision and must not simply accept AI output because it appears authoritative.

Where appropriate, staff should be transparent with pupils, parents/carers, colleagues and leaders when AI has been used in a meaningful way to produce or support content, analysis or decision-making.

10. Intellectual property and copyright

The Trust will respect intellectual property rights when using AI. Staff and pupils must not enter copyright material into AI tools unless they have permission, a licence or a clear legal basis for doing so. This includes pupil work, teacher-created resources, commercially published materials, images, music, video and thirdparty policies or resources.

Pupil and staff work may be protected by copyright. The Trust will not allow pupil work or staff-created content to be used to train AI models unless there is an appropriate legal basis, permission or exception and any data protection requirements are also met.

AI-generated output may itself create intellectual property risks if it reproduces or closely imitates protected material. Staff must check outputs before use, especially where material will be published, shared externally or used in commercial, public-facing or assessed contexts.

Copyright and data protection are separate legal regimes. Permission to process personal data does not automatically give permission to use copyright material, and copyright permission does not remove data protection obligations.

11. Use of AI by staff, Trustees and local governors

Staff, Trustees and local governors may use approved AI tools to support appropriate tasks such as drafting, summarising, planning, idea generation, resource adaptation, accessibility support, translation support, administrative efficiency and professional learning, subject to the restrictions in this policy.

The person using AI remains responsible for the final output. AI must not be used as a substitute for professional judgement, subject expertise, safeguarding judgement, line management responsibilities or formal decision-making.

- Check whether the tool is approved for the intended purpose and whether it is open or closed.
- Do not enter personal, sensitive, confidential or safeguarding information into unapproved AI tools.
- Fact-check and sense-check outputs, including dates, citations, statistics, legal statements, safeguarding content, curriculum content and medical or wellbeing information.
- Adapt outputs to the Trust context, school context, pupil needs and professional standards.
- Acknowledge or record meaningful AI use where required by this policy, assessment rules, professional standards or local procedures.
- Do not use AI to impersonate another person, generate offensive content, bully or harass, create deepfakes, generate sexualised images, or manipulate pupils, colleagues or parents/carers.
- Do not use AI to make recruitment, disciplinary, capability, pay, safeguarding, admissions, exclusion, SEND or other significant decisions without an approved process and meaningful human oversight.

12. Use of AI by pupils

The Trust recognises that AI can support pupils to research, explore ideas, practise skills, receive feedback, improve accessibility and develop digital literacy. Pupils will be taught to use AI safely, ethically and critically.

Pupils may only use AI in school or for schoolwork where the use is permitted by staff, appropriate to their age and educational needs, and consistent with this policy, school rules, acceptable use arrangements and assessment requirements.

When AI is permitted, pupils must use it as a support for learning, not as a replacement for their own thinking, understanding, creativity, working out or independent work. Pupils must follow staff instructions on whether and how to acknowledge AI use.

- Pupils must not present AI-generated work as their own independent work.
- Pupils must not use AI to cheat, plagiarise, complete assessed work unless expressly permitted, or mislead staff about how work was produced.
- Pupils must not enter personal information about themselves or others into AI tools unless specifically instructed by staff using an approved tool.
- Pupils must not use AI to generate or share harmful, offensive, discriminatory, bullying, sexualised, violent, extremist, impersonation or deepfake content.
- Pupils must report concerning AI content or use to a member of staff.

13. Assessments, examinations and academic integrity

The Trust will continue to take reasonable steps to prevent malpractice involving AI in assessments, including internal assessments, coursework, non-examination assessments and public examinations where applicable.

The Trust will follow current JCQ guidance on AI use in assessments. Pupils must understand that assessed work must be their own. Where AI is used as a source of information and the assessment rules permit that use, pupils must acknowledge it appropriately, including the name of the AI tool and the date the content was generated, and retain evidence of the AI-generated content where required including prompts, AI-generated responses and an explanation of how the AI tool was used where required by the relevant assessment arrangements.

Schools will ensure that parents and carers of pupils undertaking relevant qualifications are provided with appropriate information about the permitted and prohibited use of AI in assessed work, the Trust's and awarding organisations' expectations regarding academic integrity, and the potential consequences of AI misuse or malpractice.

AI misuse in assessment may include copying or paraphrasing AI-generated content without acknowledgement, using AI to complete work so that it does not reflect the pupil's own work, failing to acknowledge AI use, using misleading references, submitting AI-generated images or other media as original work, or using AI during an assessment where it is not permitted.

Staff will use a range of professional approaches to help prevent and identify misuse, such as knowing pupils' usual work, checking drafts and intermediate stages, asking pupils to explain their work, designing tasks that require personal, local, current or in-class work, and following exam-board procedures where malpractice is suspected.

AI detection tools must be used with caution. They can be unreliable and should not be the sole basis for an allegation of misuse. Any concern must be considered fairly and in line with the relevant assessment, behaviour, examinations or malpractice procedure.

14. AI-enabled wearable and recording-capable devices

The Trust recognises that wearable and AI-enabled technologies, including smart glasses, AI glasses, smart watches, body-worn cameras, audio-recording devices and similar technologies, may collect, record, analyse or transmit personal data. This may include images, video, audio, location information, health information and biometric data.

Such devices must not be used to record, monitor or process personal data on behalf of the Trust unless their use has been authorised and an appropriate lawful basis, safeguarding review and data protection safeguards have been established. Where the proposed use is likely to result in a high risk to individuals, including where innovative technology, systematic monitoring, biometric data or children's personal data is involved, a DPIA must be completed before the technology is introduced.

Staff, pupils, visitors and contractors must not use personally owned smart glasses, AI-enabled wearable devices or other recording-capable wearable technology to capture or process pupil, staff or Trust personal data unless expressly authorised by the Trust. Schools may restrict or prohibit recording-capable wearable devices on Trust premises or during Trust activities where their use presents a safeguarding, privacy, confidentiality, security, behaviour or data protection risk.

This section should be read alongside the Trust's Data Protection Policy, Online Safety Policy, Behaviour Policy, Safeguarding Policy, CCTV/video surveillance arrangements and, where applicable, mobile phone and device procedures.

15. Training and curriculum education

The Trust will support staff to develop appropriate AI literacy, including the benefits, limitations and risks of AI; safe prompting; data protection; cyber security; safeguarding; bias; intellectual property; assessment integrity; and how to check outputs.

Training will be proportionate to role and risk. Staff who approve, procure, administer or supervise AI tools, and those who use AI with pupils, may require additional training.

Pupils will be taught, through the curriculum and wider digital education, about safe and responsible AI use. This will include how AI works at an age-appropriate level, how to question AI outputs, how information is organised and ranked online, how bias and misinformation can arise, how to protect personal data and intellectual property, and how to report harmful or concerning content.

The Trust will use current DfE support materials and other appropriate resources to keep staff and pupils informed as AI practice and guidance develops.

16. Concerns, complaints, incidents and breach of policy

Concerns about AI use should be raised promptly. Staff should speak to their line manager, Head Teacher, Trust AI Lead, DPO, DSL or IT support as appropriate to the nature of the concern. Pupils should report concerns to a member of staff.

Safeguarding concerns must be reported immediately to the DSL. Personal data breaches or suspected data breaches must be reported immediately in accordance with the Data Protection Policy and Personal Data Breach Procedure. Cyber security incidents must be reported through Trust IT/cyber incident procedures.

Parents/carers, pupils, staff or others who believe AI use has caused unfair treatment, harm, error or inappropriate processing of personal data may use the relevant Trust complaints, data protection, safeguarding or HR procedure.

Breach of this policy by staff may be dealt with under the Staff Code of Conduct, Disciplinary Policy or other relevant procedure. Breach by pupils may be dealt with under the Behaviour Policy and related school procedures. Breach by Trustees or local governors will be considered under the relevant code of conduct and governance arrangements.

17. Monitoring and review

AI technology, guidance and risks are developing quickly. This policy will be reviewed annually and sooner where there is a significant change in law, statutory guidance, DfE expectations, JCQ guidance, Trust practice, AI tools or associated risks.

The Trust AI Lead, DPO, DSLs, IT/digital leads and senior leaders will contribute to monitoring the effectiveness of AI use and the controls in this policy. The Trust Board will receive appropriate assurance on AI governance as part of wider digital, safeguarding, data protection or risk reporting.

The approved AI tools register should be reviewed regularly and whenever a new tool, feature, use case, provider contract or risk is introduced.

18. Links with other policies and documents

- Data Protection Policy and privacy notices
- Personal Data Breach Procedure and Subject Access Request Procedure
- Child Protection and Safeguarding Policy
- Online Safety Policy and filtering and monitoring arrangements
- Cyber Security Policy / Cyber Response and Recovery Plan
- ICT Acceptable Use Policy and device agreements
- Behaviour Policy
- Assessment, Examination, Non-examination Assessment and Malpractice procedures
- Staff Code of Conduct and Disciplinary Policy
- Equality and Accessibility policies
- CCTV/video surveillance, mobile phone and device procedures where applicable
- Procurement and contract management procedures

Appendix 1: Approved AI tools and permitted uses

The Trust will maintain this table as a live register. A tool listed below is approved only for the users and purposes shown. Any wider use requires further approval.

Approved AI tool	Approved for	Permitted uses and restrictions
Microsoft Copilot / approved Microsoft 365 AI features	Staff and central team users where enabled by the Trust	Drafting, summarising, planning and administrative support within approved Trust accounts. Personal or sensitive data must only be used where the tool and configuration have been approved for that purpose. Outputs must be checked.
Google Gemini / approved Google Workspace AI features	Staff and pupils where enabled and approved by the Trust or school	Educational and administrative use within the Trust's Google tenancy where approved. Must comply with age restrictions, settings, safeguarding and data protection controls. No unapproved personal or sensitive data.
Oak National Academy AI lesson assistant / approved education resource tools	Teaching staff	Lesson planning, resource adaptation and curriculum support. Staff must check accuracy, curriculum fit, accessibility and suitability for pupils.
Approved accessibility or assistive AI tools	Named pupils or staff where approved by SEND, IT and/or senior leaders	Accessibility, translation, reading, transcription or communication support where proportionate and risk assessed. Must comply with data protection, safeguarding and age-appropriateness requirements.
Open public AI tools	Staff only, for low-risk use	Idea generation and drafting where no personal, confidential, sensitive, safeguarding, pupil work or Trust operational information is entered. Outputs must not be relied on without checking. Not approved for pupil personal data or high-risk decisions.

Appendix 2: AI tool approval checklist

Before approving a new AI tool, feature or use case, the following checklist should be completed proportionately and retained with the approval record.

Area	Minimum considerations before approval
Purpose and benefit	What problem is the tool intended to solve? What educational, workload or operational benefit is expected? Is AI necessary and proportionate?
Users and context	Who will use the tool? Are pupils using it directly? What age groups, phases, subjects or roles are involved? Are there SEND, EAL or vulnerability considerations?
Safeguarding	Could the tool expose pupils to harmful content, grooming, sexualised material, misinformation, bullying, manipulation, emotional dependence, mental health risks or unsafe advice? How will concerns be detected and escalated?

Area	Minimum considerations before approval
Filtering and monitoring	Can current filtering and monitoring handle dynamic, personalised and Algenerated content? Does the tool provide logging, alerts, moderation and supervisor reporting where needed?
Data protection	Will personal data or special category data be processed? What is the lawful basis? Is a privacy notice update or DPIA required? Where is data stored and who can access it?
Cyber security	Does the tool meet Trust security expectations, including authentication, access controls, patching, administrator controls and resilience against misuse or prompt injection?
Product safety	For pupil-facing or education-specific tools, has the Trust considered DfE product safety standards, including cognitive development, emotional and social development, mental health and manipulation?
Accuracy and bias	How reliable is the output? What are the risks of bias, hallucination, outdated information or discriminatory outcomes? How will outputs be checked?
Intellectual property	Will prompts or outputs include copyright materials, pupil work, staff resources or third-party content? Could inputs be used to train the provider's model?
Assessment integrity	Could the tool undermine authentic pupil work or assessment rules? What restrictions or declarations are needed?
Human oversight	Who remains accountable for outputs and decisions? Is meaningful human review built into the process?
Review and exit	When will the approval be reviewed? How can the tool be disabled or data exported/deleted if the Trust stops using it?