Using AI safely in schools, trusts and colleges

Practical guidance for responsible, secure and effective use

Version 1.0 | Last reviewed: October 2026

Purpose

Artificial intelligence can reduce workload, support teaching and learning, improve accessibility and help staff work more efficiently. It also creates risks involving personal data, safeguarding, security, accuracy, bias, intellectual property and academic integrity.

This guidance is written primarily for education settings in England. Settings elsewhere in the UK should check the requirements and guidance issued by their own government, regulator and awarding bodies.

This guidance gives schools, multi-academy trusts and colleges a practical framework for using AI with clear accountability and appropriate human oversight. It should sit alongside existing data protection, safeguarding, cyber security, acceptable-use, assessment and procurement arrangements.

Core principles

- **Start with a clear purpose.** Use AI only where it addresses a defined educational or operational need.
- **Keep people accountable.** AI may support professional judgement, but it should not replace it.
- **Protect personal and confidential information.** Do not enter identifiable pupil, student, parent, carer or staff data into an AI tool unless its use has been formally approved.
- **Check outputs.** Treat AI-generated content as a draft. Verify accuracy, suitability, bias, sources and tone before use.
- **Use proportionate controls.** Higher-risk uses require stronger assessment, approval, monitoring and oversight.
- **Be transparent.** Where AI uses personal data, privacy information must explain this clearly. Explain other significant uses of AI to the people affected where appropriate.
- **Promote inclusion.** Consider accessibility, equality and whether reliance on paid tools could disadvantage some learners.

Governance and accountability

Assign a senior leader to oversee AI and define how education, safeguarding, data protection, cyber security, IT, procurement and curriculum responsibilities connect. Trust-wide decisions should set minimum standards while allowing settings to respond to local context.

Maintain an inventory of approved AI tools and uses. Record the purpose, users, data involved, supplier, risk owner, approval status and review date. Where an AI use involves personal data, it should also be reflected in the record of processing activities; maintaining or linking the two together avoids separate registers drifting apart. Establish a route for staff to propose new tools or use cases and a process for withdrawing approval.

© 2026 GDPR in Schools Limited (GDPRiS). All rights reserved. Permission is granted to schools, colleges, and Multi-Academy Trusts (MATs) to reproduce and distribute this document in its original, unaltered form for non-commercial, educational use only.

Review existing policies rather than treating AI as a standalone issue. Make responsibilities clear in staff and learner acceptable-use rules, privacy information, assessment procedures, safeguarding processes, procurement controls and incident response plans.

Data protection and privacy

Before an AI use involving personal data is introduced, identify the organisation's role, purpose and lawful basis; confirm what information the supplier receives; and check whether prompts, files or outputs are used to train or improve the service. Review retention, deletion, access controls, security, international transfers, sub-processors and support for individual rights.

Complete a data protection impact assessment where processing is likely to result in a high risk to people's rights and freedoms. A DPIA is particularly likely to be required where AI involves large-scale use of special category data, systematic monitoring, profiling, biometric data or solely automated decisions that have legal or similarly significant effects. Uses involving children's personal data require careful assessment because children may be particularly vulnerable, but the involvement of children's data does not by itself make every use high risk.

Apply data minimisation. Use anonymised, synthetic or non-identifiable information wherever possible. Staff should never paste safeguarding records, special educational needs information, health details, behaviour records, assessment data or identifiable casework into an unapproved tool.

Take particular care with AI meeting transcription and note-taking tools, whether built into video-conferencing platforms or provided by standalone bots. These are increasingly used in SEN reviews, parent meetings, safeguarding discussions and HR meetings, where sensitive information is often shared. Tell attendees before recording or transcription starts, check summaries for accuracy before they are saved or shared because they may become part of the record, set retention periods for recordings, transcripts and summaries, and consider whether some meetings should not be recorded at all. Do not allow unapproved note-taking bots to join meetings.

Privacy information should clearly explain material uses of AI. Do not assume consent is the correct lawful basis, and do not rely on a supplier's claims as evidence of compliance. Maintained schools, academy trusts and further education colleges cannot generally rely on legitimate interests for processing carried out in performing their public tasks, even where supplier materials suggest it; independent schools should take advice on their own position.

Decide whether AI prompts, chat histories, uploaded files and outputs are retained, where they are held, for how long and who can access them, rather than leaving this to supplier defaults. Where they contain personal data, they may fall within the scope of subject access requests. For maintained schools, academy trusts and colleges, recorded information held in AI tools may also be requested under the Freedom of Information Act 2000. Reflect these decisions in your retention schedule.

© 2026 GDPR in Schools Limited (GDPRiS). All rights reserved. Permission is granted to schools, colleges, and Multi-Academy Trusts (MATs) to reproduce and distribute this document in its original, unaltered form for non-commercial, educational use only.

Safeguarding, wellbeing and learner use

Apply the same safeguarding expectations to AI-enabled services as to other online activity. Consider age suitability, filtering, harmful or misleading content, manipulation, contact features, image generation, impersonation and the possibility that a learner may disclose sensitive information to a chatbot.

Set clear, age-appropriate rules for when learners may use AI, which tools are permitted, how use must be acknowledged and when adult supervision is required.

Rules alone are not enough. Learners will meet AI tools outside school, so settings should help them develop the knowledge and judgement to use AI safely and responsibly. Age-appropriate teaching might cover how AI tools generate content, why outputs can be wrong or biased, how to check information against reliable sources, what personal information should never be shared, how AI can be used to create fake images, voices or messages, and why AI should not replace trusted adults or friends when they need help. Where possible, build this into existing computing, online safety, PSHE and RSHE teaching rather than treating it as a separate topic, and help parents and carers reinforce the same messages at home.

AI must not be treated as a counsellor, safeguarding professional or substitute for trusted human support. Any concern identified through an AI interaction should follow the setting's normal safeguarding procedures.

Be prepared for AI-generated sexual imagery. Learners may use nudification, face-swap or other image tools to create sexual images of classmates or staff. Sexual imagery of anyone under 18 is illegal, however it was made, and must be treated as a safeguarding incident. Staff should not view the imagery unless it is unavoidable, and must not copy, print, forward, save or ask anyone to send it. Report concerns immediately to the designated safeguarding lead, who should follow the UK Council for Internet Safety guidance on sharing nudes and semi-nudes, involve the police where required and support everyone affected, including staff who are targeted.

Teaching, learning and assessment

Use AI where it has a clear educational benefit, such as helping staff generate ideas, adapt materials, improve accessibility or reduce routine administration. Staff remain responsible for the quality, accuracy, curriculum alignment and suitability of anything they use.

Define acceptable and unacceptable learner use for different tasks and assessments. Expectations should distinguish legitimate support, such as brainstorming or feedback, from work that misrepresents authorship. For formal assessments, follow the current rules of the relevant awarding body. Where AI use is permitted, require learners to identify the tool and generated material used, retain any evidence required by the awarding body and ensure that submitted work remains demonstrably their own.

For some learners with SEND or other access needs, AI-enabled assistive technology may be part of their normal way of working, a reasonable adjustment or an approved access arrangement. Manage these uses through the setting's SEND and access arrangements processes and, for formal assessments, the awarding body's rules, rather than applying general restrictions on AI use.

© 2026 GDPR in Schools Limited (GDPRiS). All rights reserved. Permission is granted to schools, colleges, and Multi-Academy Trusts (MATs) to reproduce and distribute this document in its original, unaltered form for non-commercial, educational use only.

Do not use AI output without meaningful human review as the basis for grading, disciplinary action, admissions, exclusions, SEND decisions, safeguarding judgements, recruitment shortlisting, staff capability or performance management, or other decisions that could significantly affect a person. AI-assisted CV screening should also be checked for discriminatory outcomes under the Equality Act 2010. Where personal data is used in solely automated decision-making that has legal or similarly significant effects, obtain specialist data protection advice and ensure that the use is lawful, transparent and subject to the safeguards required by data protection law, including an appropriate route to obtain human intervention and challenge the decision. Solely automated significant decisions involving special category data, such as health or SEND information and some safeguarding information, are permitted only in very limited circumstances; see the accompanying DPIA guidance for more detail.

Accuracy, bias and intellectual property

Generative AI can produce plausible but false, incomplete or inconsistent information. Check important claims against reliable sources, confirm quotations and references, and never present invented citations as genuine.

As part of due diligence, ask suppliers to provide evidence of how they have tested their tools for biased or unequal outcomes. After deployment, monitor real-world outcomes, particularly where outputs affect access, support, attainment, behaviour or opportunity; for example, check whether flags or recommendations fall disproportionately on particular groups. Raise concerns with the supplier and document how they are addressed.

Respect copyright, licensing and confidentiality. Check whether material may lawfully be uploaded, adapted or reused, and whether generated content can be published under the intended terms. Avoid prompting a tool to reproduce protected material or imitate a living creator’s work. Take particular care before uploading learners’ own work to AI marking or feedback tools: it is likely to include their personal data, and learners usually own the copyright in what they create. Use only approved tools, explain the use to learners and, where appropriate, parents and carers, and check whether the supplier retains the work or uses it to train its models.

Security and procurement

Use approved organisational accounts and enterprise controls where available. Apply strong authentication, least-privilege access, secure configuration, logging and prompt software updates. Consider risks from malicious prompts, unsafe integrations, data leakage, generated code and “shadow AI” used outside approved arrangements.

Before purchase or deployment, assess the supplier against a documented set of requirements. Confirm the product’s intended educational purpose, age range, evidence base, filtering and moderation, monitoring and reporting, data handling, security, accessibility, intellectual property terms, service continuity and exit arrangements.

Governance should also cover AI features added to systems already in use, not just new purchases. Suppliers increasingly introduce AI into management information systems, office software and learning platforms through routine updates, sometimes enabled by default. Ask

© 2026 GDPR in Schools Limited (GDPRiS). All rights reserved. Permission is granted to schools, colleges, and Multi-Academy Trusts (MATs) to reproduce and distribute this document in its original, unaltered form for non-commercial, educational use only.

suppliers to notify you of new AI features, review release notes and administrator settings, and assess significant changes before making them available to staff or learners. AI assistants built into office platforms, such as Microsoft 365 Copilot, can surface any content a user already has technical access to. Before enabling them, review sharing settings and permissions across SharePoint, OneDrive, Teams and shared drives so that sensitive information is not exposed to people who should not see it.

Pilot higher-risk tools with a limited group before wider use. A pilot still involves real use, so complete supplier due diligence and, where the threshold is met, a DPIA before it starts. Define success metrics, monitor unintended effects and retain the ability to suspend the tool quickly.

Responding to incidents

Make it easy for staff and learners to report inaccurate, harmful, biased or unsafe outputs, suspected data disclosure, misuse, impersonation or academic misconduct. Preserve relevant evidence without unnecessarily copying personal or harmful content. Where an incident involves sexual imagery of a child, do not copy or share it as evidence; follow the safeguarding approach set out above.

Follow existing safeguarding, personal data breach, cyber incident, complaints and disciplinary procedures. Involve the designated safeguarding lead, data protection officer, IT or security lead and senior leadership as appropriate. Assess promptly whether the incident meets the applicable threshold for notifying the supplier, affected individuals, the Information Commission, police, awarding body, insurer or another relevant organisation, and record the decision and rationale. A personal data breach that must be reported to the Information Commission should be notified without undue delay and, where feasible, within 72 hours of becoming aware of it.

Record lessons learned and update controls, training, procurement decisions and approved-use guidance.

Implementation checklist

- Appoint a senior AI lead and agree cross-functional responsibilities.
- Audit current AI use, including unapproved or embedded tools.
- Publish an approved-tools list and a simple approval route.
- Define prohibited data and high-risk uses.
- Complete supplier due diligence and, where required, a DPIA.
- Update relevant policies, privacy information and incident procedures.
- Train staff in safe prompting, output checking, safeguarding, data protection and copyright.
- Teach learners age-appropriate AI literacy and academic integrity.
- Pilot, monitor and review tools against educational benefit and risk.
- Report regularly to governors or trustees on adoption, incidents, assurance and next steps.

Further guidance

- *Department for Education: Generative artificial intelligence in education*
- *Department for Education: Using AI in education settings – support materials*
- *Department for Education: Generative AI: product safety standards*

© 2026 GDPR in Schools Limited (GDPRiS). All rights reserved. Permission is granted to schools, colleges, and Multi-Academy Trusts (MATs) to reproduce and distribute this document in its original, unaltered form for non-commercial, educational use only.

- *Information Commission: Guidance on AI and data protection*
- *National Cyber Security Centre: AI and cyber security – what you need to know*
- *Department for Education: Keeping children safe in education*
- *Department for Education: Meeting digital and technology standards – filtering and monitoring*
- *UK Council for Internet Safety: Sharing nudes and semi-nudes – advice for education settings*
- *GDPRiS: accompanying guidance on data protection impact assessments for AI*

For qualifications and formal assessments, also check the current AI guidance issued by the relevant awarding body or the Joint Council for Qualifications. Requirements can change between assessment series and may specify how permitted AI use must be acknowledged, evidenced and authenticated.

Guidance, law and technology change quickly. Review this document regularly and check current government, regulator and awarding-body advice before making significant decisions. Most data protection changes under the Data (Use and Access) Act 2025 came into force on 5 February 2026, and the Information Commission (which continues to operate as the ICO) is still publishing new and updated guidance, so confirm that data protection advice remains current when this document is used.

© 2026 GDPR in Schools Limited (GDPRiS). All rights reserved. Permission is granted to schools, colleges, and Multi-Academy Trusts (MATs) to reproduce and distribute this document in its original, unaltered form for non-commercial, educational use only.