

Conducting DPIAs for Generative AI in Schools, Trusts and Colleges

Practical guidance on assessing data protection risks, automated decision-making and UK GDPR compliance for generative AI and other AI-driven tools

This guidance helps data protection officers (DPOs) and data protection leads (DP Leads) in schools, multi-academy trusts and colleges assess the data protection risks of generative AI alongside their existing data protection impact assessment (DPIA) process. Although it focuses on generative AI, it applies to AI-driven tools more broadly, including predictive analytics, risk scoring and automated marking. It covers screening, describing data use, consultation, lawful basis, automated decision-making, risk assessment, practical controls and data subject rights. It also supports approval, monitoring and review, with particular attention to personal data, meaningful human oversight, supplier practices and international transfers.

It should be read alongside our *Using AI safely in schools, trusts and colleges: Practical guidance for responsible, secure and effective use*, which sets out the wider principles for staff and leaders. This guidance is written mainly for England. Organisations in Wales, Scotland and Northern Ireland should check the legislation and guidance that apply to them.

Version 1.0 | Last reviewed: October 2026. This version reflects the automated decision-making provisions introduced by the Data (Use and Access) Act 2025, in force from 5 February 2026.

1. Screening: is a DPIA needed?

Why a DPIA may be needed

Generative AI tools may process personal data to generate outputs, provide recommendations or automate tasks. They can also infer characteristics or create new information about individuals. A DPIA is required where the processing is likely to result in a high risk to people's rights and freedoms.

Factors indicating that a DPIA may be required:

- Use of new, potentially intrusive technology
- Large-scale profiling or inference
- Risk to vulnerable groups (children)
- Possible significant decisions about individuals (Articles 22A–22D UK GDPR)
- International transfers to AI compute centres
- Risk of data leakage into model training
- Staff use through personal or consumer accounts
- AI assistants with access to existing organisational data
- Direct use by pupils, uploading of images, or any biometric element

Use the following questions alongside your standard DPIA screening criteria. A “yes” response indicates that further assessment is needed; it does not automatically determine the outcome of the DPIA.

Q: Does the project involve the use of generative AI or automated decision-making systems?

If **yes**, assess whether the proposed processing is likely to result in a high risk to individuals. A DPIA is required where that threshold is met and must be completed before the processing begins.

Q: Will the AI system make or support decisions that could have a significant impact on individuals?

Examples:

- Automated marking
- Behavioural risk scoring
- Special educational needs and disabilities (SEND) identification suggestions
- Safeguarding risk flagging
- Predictive analytics on pupil performance

If **yes**, apply the two-question test in Section 4 (is the decision significant, and is it solely automated?) to decide whether the UK GDPR's automated decision-making provisions apply. Document the role of meaningful human review, the effect on individuals and the safeguards in place.

Q: Will personal data be input into a generative AI system, including prompts containing identifiable information?

If **yes**, additional risks must be assessed (e.g. data leakage, unintended training). Consider outputs as well as inputs: outputs can contain or infer personal data even when inputs do not, for example where a model asked to summarise a class draws conclusions about individual pupils.

Q: Does the vendor use your data to train or fine-tune models?

If **yes**, treat this as a significant risk requiring detailed contractual, technical and governance scrutiny, particularly where personal or special category data is involved.

Q: Will staff use the tool through personal or consumer accounts rather than an organisation-managed account?

If **yes**, treat this as higher risk. Consumer tiers often differ from enterprise or education tiers on whether prompts are used for training and how long they are retained, and the organisation has little control over them. Most everyday exposure in schools comes from staff using general-purpose chatbots to write reports, summarise behaviour logs or draft education, health and care plan (EHCP) paperwork. See "Access route" in Section 2.

Q: Can the tool search or access existing organisational data, such as SharePoint, OneDrive, Teams or email?

If **yes**, the tool will surface anything a user can technically access. Where files have been overshared over many years, this can expose safeguarding, HR or other sensitive records. Review permissions before rollout (see risk 11 in Section 5).

Q: Will pupils or learners use the tool directly?

If **yes**, assess minimum age terms, filtering and monitoring, and safeguarding arrangements (see “Pupil-facing use” in Section 2).

Q: Will images of pupils or staff be uploaded, or does the tool involve facial recognition or other biometrics?

If **yes**, assess image-misuse risks and, for any biometric element, the requirements of the Protection of Freedoms Act 2012 (see “Images and biometrics” in Section 2).

2. Describe the processing

For each DPIA, document:

Inputs: personal data entered in the AI system

- Pupil names, behaviour notes, attendance patterns
- Staff performance data
- Free-text prompts containing personal data
- Documents, spreadsheets, or images uploaded for analysis

Processing activities

- AI model analyses data
- Generates synthetic content
- Produces recommendations, classifications, predictions, or scores
- May create inferred or derived data

Outputs

- Suggested actions
- Risk scores
- Summaries of behavioural patterns
- Reports, emails, or generated learning materials

Data flows, retention and storage

- Where does the model run? (UK/EEA/US/other)
- Does the model retain input data?
- Does the vendor use prompts for model improvement?
- Are outputs stored, and if so, where and for how long?

Indicators of higher risk

- Black-box system with limited explainability
- Automated recommendations influencing pupil outcomes
- Vendor opacity about training data
- Cloud services involving sub-processors in multiple jurisdictions

Access route: consumer or enterprise accounts

Much day-to-day exposure comes from individual staff using general-purpose tools such as ChatGPT, Gemini or Copilot, not just from procured systems. Record:

- Whether staff will use an organisation-managed enterprise or education account, or personal or consumer accounts
- Whether the tier used trains on prompts and how long it retains prompts, uploads and outputs; consumer tiers usually differ from enterprise and education tiers on both
- Which approved tools staff should use instead of consumer services, and how this is communicated
- Whether the tool can search existing organisational data (for example SharePoint, OneDrive, Teams or email) and whether permissions have been reviewed

Pupil-facing use

Where pupils or learners use a tool directly, the DPIA should also cover:

- The provider's minimum age terms, and whether all intended users meet them
- Filtering and monitoring arrangements, in line with the DfE filtering and monitoring standards
- How the tool meets the DfE's generative AI product safety standards
- Where relevant, JCQ rules on the use of AI in assessed work

Images and biometrics

Uploading pupil photos or video for analysis increases the risk of image misuse, including deepfakes. Biometric data used to identify individuals, such as facial recognition, is special category data and brings in the Protection of Freedoms Act 2012 requirements for schools and colleges: notify parents, obtain written consent from at least one parent before processing a child's biometric information, do not process it if the child or any parent objects, and provide a reasonable alternative.

3. Consult the right people

AI projects affecting pupils, learners or staff should include proportionate consultation with the people and professional roles affected by the proposed use.

- Consultation with staff
- Consultation with pupils, learners, parents or carers where proportionate to the proposed use and its potential effects
- Seek the advice of the DPO, as Article 35(2) UK GDPR requires, and record that advice at sign-off (see Section 8)
- Consult the Information Commission (ICO) before processing begins if the DPIA identifies a high residual risk that cannot be reduced through additional measures

Provide clear, accessible information about how AI is used, what personal data is processed, the purpose of the processing and any significant consequences for individuals. Where relevant, explain the factors and information used in AI-supported decisions in language appropriate to the audience.

4. Assess necessity and proportionality

Lawful basis and special category data

Identify and document the appropriate Article 6 lawful basis for each purpose. Where special category data is processed, identify a separate Article 9 condition and any relevant condition in UK law. Do not assume that consent is appropriate simply because a tool is optional or experimental.

- **Public task** will usually be the appropriate basis for maintained schools, academy trusts and FE colleges where the processing is necessary for their education functions.
- **Legitimate interests**, including the new recognised legitimate interests under Article 6(1)(ea), cannot be relied on by public authorities for processing carried out in performing their tasks. Maintained schools, academy trusts and FE colleges should therefore not use legitimate interests for their core functions, even where vendor materials suggest it; it will rarely be available.
- **Independent schools** are generally not public authorities, so legitimate interests may be available to them. A legitimate interests assessment is still needed, unless a recognised legitimate interest applies.
- **Consent** must be freely given, specific, informed and capable of being withdrawn; consider carefully whether the power imbalance in an education setting makes it suitable. Where consent is relied on for an online service offered directly to a pupil under 13, parental authorisation is required, which makes consent even less practical.

Automated decision-making and profiling

From 5 February 2026, section 80 and Schedule 6 of the Data (Use and Access) Act 2025 replaced Article 22 UK GDPR with Articles 22A–22D. These provisions apply to significant decisions based solely on automated processing, including profiling. To decide whether they apply, ask two separate questions:

1. **Is the decision significant?** It produces a legal effect or a similarly significant effect on the individual.
2. **Is it solely automated?** Under Article 22A, a decision is based solely on automated processing only where there is no meaningful human involvement in it. The extent to which the decision is reached by means of profiling should be considered.

The provisions apply only where the answer to both questions is yes. Not every AI suggestion is caught, but a quick glance at a suggestion does not take a decision out of scope either. Markers of meaningful human involvement include:

- The reviewer has the authority and competence to change the outcome
- The reviewer sees the underlying information, not just the score or recommendation, and considers other relevant information
- Records show that reviewers depart from the AI output in practice, at a rate that is monitored; a rate of zero over time suggests the review is a formality

Ordinary personal data versus special category data

- **Ordinary personal data:** significant decisions based solely on automated processing are permitted, provided the Article 22C safeguards are in place.

- **Special category data:** under Article 22B, a significant decision based entirely or partly on special category data must not be taken based solely on automated processing unless one of the following conditions is met.
 - (a) The individual has given explicit consent.
 - (b) The decision is necessary for entering into or performing a contract with the individual, and the substantial public interest condition in Article 9(2)(g) applies.
 - (c) The decision is required or authorised by law, and the substantial public interest condition in Article 9(2)(g) applies.

The Article 22C safeguards still apply in every case.

In schools, trusts and colleges this split is decisive. SEND identification often involves health data, and safeguarding flags often draw on health or other special category data, so both fall under the stricter Article 22B regime. Automated marking generally does not. In practice, build meaningful human involvement into SEND and safeguarding decisions so that they are not solely automated; explicit consent is rarely appropriate in an education setting.

Although the law permits solely automated significant decisions on ordinary personal data where safeguards are in place, GDPRiS recommends, in line with our guidance on *Using AI safely in schools, trusts and colleges*, that AI output is not used as the sole basis for grading, disciplinary action, admissions, exclusions, SEND decisions, safeguarding judgements or other decisions with a significant effect.

Examples of decisions that may be significant in schools, trusts and colleges:

- Automated marking affecting grades
- SEND identification or classification decisions
- Safeguarding referrals or interventions based on risk scores
- Disciplinary action, admissions or exclusions
- Predictive behaviour or attainment modelling
- Staff performance scoring

Whether any of these is in scope depends on the second question: how the human review works in practice.

Worked example: the same tool, inside or outside scope

A tool analyses attendance, behaviour and health notes and flags pupils who may have unidentified SEND.

- **Outside scope (not solely automated):** the special educational needs coordinator (SENCO) receives each flag with the underlying evidence, considers teacher observations and parent input, and decides whether to begin assessment. The SENCO regularly disagrees with the tool and records why.
- **Inside scope (solely automated):** flagged pupils are automatically added to the SEND register or an intervention list, or the SENCO approves the list in bulk without looking at the evidence. Because the tool draws on health data, the Article 22B restrictions apply.

Where the automated decision-making provisions apply, document the lawful basis for the processing and ensure that the Article 22C safeguards are in place. These must include measures that:

- Provide the individual with information about significant decisions taken about them
- Enable the individual to make representations about those decisions
- Enable the individual to obtain human intervention, and to contest those decisions

As good practice, also keep clear records showing that any human review is genuine, informed and able to change the outcome.

Data minimisation

Ensure:

- No unnecessary personal data in prompts
- Use anonymised or synthetic data where possible
- Confirm that the provider does not reuse the organisation's personal data to train or improve its models unless that use has been specifically assessed, formally approved and documented

Transparency

- Update privacy information with AI-specific sections
- Explain the use of AI in clear, accessible and age-appropriate language for pupils and learners, and in suitable language for staff, parents and carers
- Provide information about automated decision-making

Preventing function creep

- Restrict new use cases
- Require internal approval for changes
- Update the DPIA for any expanded processing

5. Identify and assess the risks

Record the following risks in your organisation's DPIA risk assessment, considering the likelihood and severity of harm and the residual risk after controls are applied.

Example AI-related risks

1. Model inferencing causes unintended profiling
2. Sensitive pupil data used to train third-party models
3. Data leakage via prompts
4. Opaque, unpredictable or inconsistent AI decisions lead to unfair outcomes, which may amount to unlawful discrimination under the Equality Act 2010
5. Bias in model produces discriminatory outputs, risking breaches of the Equality Act 2010 and the Public Sector Equality Duty (PSED)
6. Solely automated significant decisions are made without the required lawful basis or safeguards
7. Hallucinations generate false information about individuals
8. Unexplainable outputs undermine trust

9. Restricted transfers are made without applicable adequacy regulations, appropriate safeguards or the required data protection test
10. Vendor unable to delete model-embedded data
11. AI assistants with access to SharePoint, OneDrive, Teams or email surface overshared safeguarding, HR or other sensitive files
12. Staff use personal or consumer AI accounts outside organisational controls

Record the initial risk rating, the controls selected, the person responsible for each action and the residual risk after those controls are applied.

Linking risks to controls

Risk	Key controls (Section 6 unless stated)
1. Unintended profiling	Data minimisation and restricting new use cases (Section 4); human review of significant outputs
2. Training on pupil data	“No training” configuration; enterprise or education tier; contractual no-training clause; vendor role check
3. Data leakage via prompts	Data loss prevention (DLP) or blocking tools; staff training; “no personal data in prompts unless formally approved” policy
4. Unpredictable or unfair outcomes	Meaningful human review; challenge and appeal process; explainability commitments
5. Bias and discrimination	Fairness and bias reviews (Equality Act 2010 and PSED); vendor documentation on training sources
6. Unlawful solely automated decisions	Two-question test and Article 22B check (Section 4); Article 22C safeguards; markers of meaningful review
7. Hallucinations about individuals	Human review of outputs; rectification process (Section 7); staff training
8. Unexplainable outputs	Privacy information and transparency (Section 4); explainability commitments
9. Unlawful restricted transfers	Transfer mapping; adequacy regulations, IDTA or UK Addendum; transfer risk assessment
10. Vendor unable to delete data	Contractual retention and deletion terms; no-training configuration; erasure process (Section 7)
11. AI assistants surface overshared files	Permissions review before rollout; logging and access controls; phased pilot
12. Consumer account use	Approved enterprise or education tools; restrict consumer services; staff policy and training

Worked example: recording a risk

This illustrative example shows how one risk might be recorded. Adapt the ratings, controls and owners to your own setting.

Risk	Likelihood	Severity	Controls	Owner	Residual rating
11. An AI assistant surfaces overshared	Likely: years of broad sharing on	Severe: special category and	Permissions review of sensitive sites before rollout;	IT lead, with designated safeguarding	Medium: review after pilot

safeguarding and HR files to staff who should not see them	SharePoint and Teams	safeguarding data	remove organisation-wide links; restrict sensitive libraries from AI search; phased pilot; monitor access logs	lead (DSL) and HR lead	
---	----------------------	-------------------	--	------------------------	--

6. Record controls and actions

Include the following measures:

Technical controls

- Configure the service to prevent the provider retaining prompts, uploaded content and outputs for model training or other secondary purposes, unless this use has been specifically assessed and approved
- Use data loss prevention (DLP) or blocking tools to detect and stop personal or sensitive data being entered into unapproved AI services
- Use tenant-isolated or “no training” enterprise AI platforms
- Implement logging and access controls
- Review and tighten SharePoint, OneDrive, Teams and email permissions before enabling AI assistants that can search organisational data
- Implement content filtering on inputs and outputs
- Require vendor documentation on model training sources

Organisational controls

- Mandatory staff training on safe AI use
- Clear policy: “No personal data in prompts unless formally approved”
- Human review for all significant AI-generated outputs
- Documented challenge/appeal process for decisions
- Periodic AI fairness and bias reviews, with reference to the Equality Act 2010 and the Public Sector Equality Duty
- Provide approved enterprise or education AI tools for staff, and restrict the use of consumer services
- Run a phased pilot before wider rollout
- Require staff to report straight away if personal data is entered into an unapproved AI tool or otherwise exposed; treat this as a possible personal data breach under the organisation’s breach procedure, and report notifiable breaches to the ICO within 72 hours of becoming aware of them
- Strict procurement due diligence for vendors

Contractual controls

First, determine the vendor’s role for each purpose. Many AI vendors act as processors for service delivery but as controllers for model improvement, abuse monitoring or analytics. Article 28 processor terms only cover the processor activities. For any purpose where the vendor acts as a controller, assess whether that sharing is lawful, transparent and acceptable, or configure the service and contract to prevent it.

The data processing agreement or contract with the AI provider should address:

- No training or fine-tuning on your data
- Data processed only under your instruction
- Documented retention periods, deletion procedures and contractual commitments covering prompts, uploaded content, outputs, backups and account closure
- Sub-processor transparency
- Location of data centres
- Incident response times
- Explainability/algorithmic transparency commitments

International transfers

If personal data may be accessed, stored or otherwise processed outside the UK, first determine whether this constitutes a restricted transfer under the UK GDPR. If it does:

- Identify every country in which personal data may be accessed, stored or otherwise processed
- Check whether UK adequacy regulations apply
- Where no adequacy regulations apply, put an appropriate safeguard in place, such as the UK International Data Transfer Agreement (IDTA) or the EU Standard Contractual Clauses with the UK Addendum
- Complete and document the required data protection test, commonly recorded as a transfer risk assessment, when relying on appropriate safeguards

7. Data subject rights

AI use directly affects several individual rights. Record where AI-held personal data sits, including prompts, uploaded files, outputs and logs held by your organisation or the provider, who can retrieve it, and how requests will be handled.

- **Right of access:** subject access requests may need to cover prompts and outputs that relate to the individual. Know where these are stored, how long they are kept, and how to search and export them.
- **Rectification:** where an AI output contains inaccurate information about an individual (risk 7), correct or annotate the record and stop the inaccuracy spreading into other systems.
- **Erasure:** understand what the provider can and cannot delete, including backups and any data embedded in models (risk 10), and reflect this in contracts and privacy information.
- **Objection and automated decisions:** individuals may object to processing based on public task, and can make representations about, and contest, significant automated decisions (Section 4).

8. Approve, monitor and review

Add AI-specific items in sign-off:

- Confirm whether Articles 22A–22D apply (the decision is both significant and solely automated), whether special category data brings in Article 22B, and record the lawful basis and safeguards used
- Confirm that meaningful human review is built into decisions with legal or similarly significant effects

- Confirm that supplier due diligence and contractual checks are complete, including the vendor's role for each purpose
- Confirm that any international transfer assessment is complete
- Record the DPO's advice and, where it is not followed, the reasons why
- Record the named approver (for example the headteacher, CEO or senior information risk owner (SIRO)) and the senior AI lead
- Ensure governors or trustees have visibility of high-risk uses
- Update the record of processing activities (RoPA) and privacy information
- Add the tool to the organisation's inventory of approved AI tools
- Assign owners for monitoring accuracy, bias, security, misuse and complaints
- Set a proportionate review date and review sooner if the tool, purpose, data, supplier terms or risk profile changes

Annex: Further reading

- GDPRiS: [Using AI safely in schools, trusts and colleges: Practical guidance for responsible, secure and effective use](#)
- Information Commission (ICO): [Guidance on AI and data protection](#)
- Information Commission (ICO): [draft guidance on automated decision-making, including profiling](#), and [guidance on recognised legitimate interest](#)
- Department for Education: [Generative artificial intelligence \(AI\) in education](#)
- Department for Education: [Generative AI: product safety standards](#)
- Department for Education: [Using AI in education settings: support materials](#)
- Department for Education: [Meeting digital and technology standards – filtering and monitoring](#)
- Department for Education: [Keeping children safe in education](#)
- Department for Education: [Protection of children's biometric information in schools](#)
- JCQ: [AI Use in Assessments: Your role in protecting the integrity of qualifications](#)
- National Cyber Security Centre (NCSC): [AI and cyber security: what you need to know](#)