AI& DATA PROTECTION APPROVED PLATFORMS

ISSUE 26

Contents

Legislation & Guidance

This policy meets the requirements of the UK Government AI Policy & Guidance

AI Regulation White Paper (2023) | A pro-innovation approach to AI regulation
https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach

Guidance for Regulators on Implementing AI Principles (2024) | Implementing the UK's AI regulatory principles: Initial guidance for regulators
https://www.gov.uk/government/publications/implementing-the-uks-ai-regulatory-principles-initial-guidance-for-regulators

UK Government AI Playbook (for public sector use) | Artificial Intelligence Playbook for the UK Government
https://www.gov.uk/government/publications/ai-playbook-for-the-uk-government

Data Protection & AI Guidance | ICO – Guidance on AI and Data Protection (Explains fairness, transparency, automated decision-making rules, etc.)
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/

Online Safety

Online Safety Act 2023 | (Important for AI-generated content and platform responsibilities)
https://www.gov.uk/government/collections/online-safety-act-2023

Data Protection

AI tools may process or store data, often on external servers. Any processing of personal data must comply with UK GDPR.

- Personal data should not be input into any AI systems that will learn from the input, consult the 'Approved AI tools register' for tools that are approved for this purpose. Using tools that are unapproved for this purpose risks data breaches, which should be reported instantly in line with the Data protection policy.

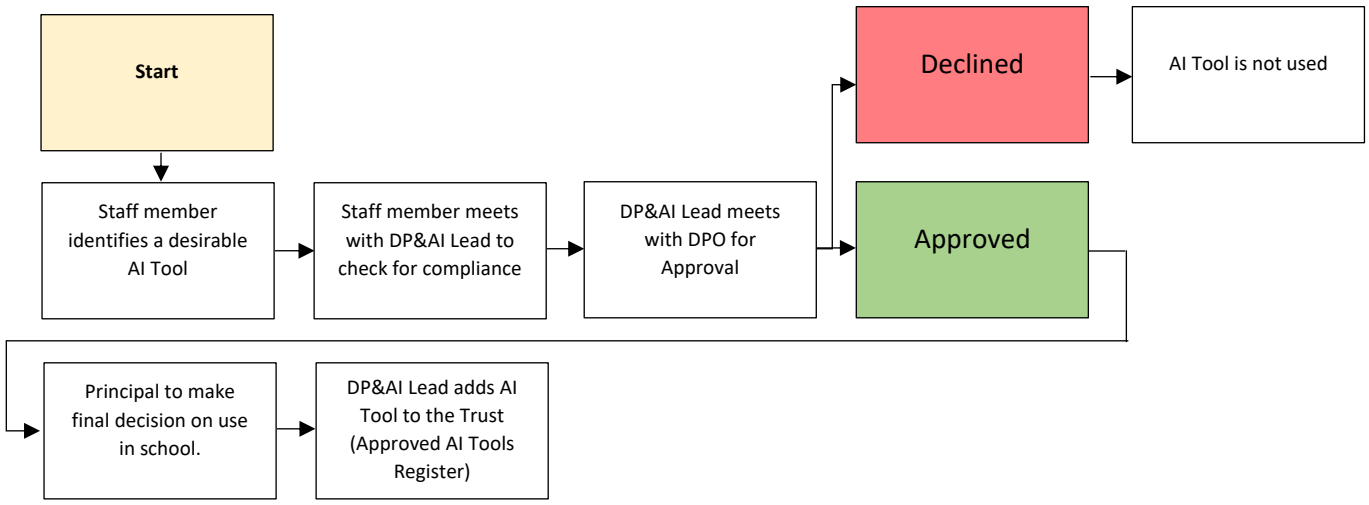
AI systems often learn and evolve based on the data provided, raising significant data protection concerns. Staff must not input any school data into AI systems that aren't secure, for example the freely available version of ChatGPT.

In compliance with the General Data Protection Regulation (GDPR), our policy states that:

- Any AI tool used within the school environment must be approved by the Trust DPO as well as going through the DPIA process.
- No sensitive student data should be input into any AI system. For example, student ethnicity, health records or special educational needs.
- All staff members are required to participate in routine data protection training, which includes best practices in handling and interacting with AI platforms.

Key Principles:

- Personal data includes names, assessment records, and anything identifiable.
- Lawful processing must have a clear basis; the most common of these are: public task, legitimate interest, or consent.
- Schools must not input personal or sensitive data into generative AI systems without approval from the AI & Data Protection Lead, and Data Protection Officer (DPO).
- AI systems must not store or learn from personal data, to avoid this only trust approved AI tools should be used, as listed on the 'Approved AI tools register'.
- Schools must ensure data retention, deletion and storage policies are adhered to.



Ethical Position on AI

Partnership Learning's Stance

Partnership Learning recognises that AI can have both positive and negative impacts on education. Our approach is measured and cautious, focusing on understanding how AI operates and affects learners and staff, managing its use ethically and transparently, and protecting against misuse, over-reliance, or inequity.

Ethical Principles

All AI and data use within Partnership Learning will adhere to:

- Human Oversight – AI must never replace human judgment or accountability.
- Fairness and Non-Discrimination – AI tools must not introduce or reinforce bias.
- Transparency – Users must know when and how AI is involved in a process.
- Privacy – AI use must comply with data protection laws and avoid unnecessary data processing.
- Educational Integrity – AI should support learning awareness, not replace authentic student effort.

Responsible AI Management in Education

Approach

AI may appear in educational or administrative tools used across Partnership Learning schools, even when not actively introduced. The Trust's responsibility is to identify, evaluate, and manage such technologies to ensure correct use.

Example Areas of Use (Monitored)

- Automated marking or feedback systems.
- Language learning or accessibility applications.
- Administrative chatbots or data management tools.

Each of these areas will be reviewed for privacy, equity, and pedagogical impact before use.

Risk Management

For every identified platform that AI is utilized, a GDPR (DPIA) **Data Protection Impact Assessment** must be completed to address the potential risks to subjects data.

User Responsibilities

Staff and Leaders

Staff are responsible for using AI-related tools only when authorised and understood, ensuring that human professional judgment guides all final decisions, and reporting any AI system or digital tool that operates without clear transparency or data protection assurance.

Students

Students should avoid using AI tools to complete or generate assessed work unless explicitly permitted, acknowledge any use of AI in learning or research, and understand both the potential and the limitations of AI.

Data and Safeguarding

All AI use must align with GDPR, safeguarding, and online safety standards. Data must not be entered into AI platforms unless explicitly approved and securely managed.

Privacy, Data & Security

Partnership Learning prioritises data minimisation, protection, and informed consent in all digital systems.

AI tools that process data will be subject to Trust-level DPIA (data protection impact assessment) and must comply with existing Data Protection and ICT Acceptable Use Policies.

Human Agency Oversight

AI should always operate under human supervision.

Teachers, leaders, and IT staff must be able to explain, question, and override AI-driven recommendations. Training will be provided to ensure staff can identify and manage AI-related risks.

Approved AI Platforms

Refer to your DP&AI Lead to grant you access for using these platforms.

AI Platform	Website	Authorised DPIA
Canva	www.canva.com	
Turnitin	www.turnitin.co.uk	
Microsoft Copilot	www.office.com/copilot	

Attention | Under any circumstances should you be using a free AI Platform where personal information are uploaded for correction, regeneration, manipulation or alteration of any personal and intellectual property.

In a nutshell

Here is what teachers are allowed and not allowed to use AI for.

Permitted	Not Permitted
Drafting Lesson Plans, Resources, Admin Content	Uploading Student Names, Photos, or Personal Data
Summarising Documents	Using AI to make decisions about Students
Improving Staff's Subject Knowledge	Using unapproved AI tools with Students
Creating Example Feedback (Anonymised)	Trusting AI output without checking
Using AI Approved by the school	Uploading Copyrighted Materials (i.e. Student Coursework)
Using Anonymised Data	Allowing AI to interact with pupils unsupervised

In detail

GOOD USE

What Staff Can Do When Using AI

1. Use AI to support planning and workload reduction | Staff can use AI to:

- Draft lesson plans or schemes of work
- Generate differentiated questions, worksheets, or resources
- Summarise long documents or research
- Create administrative content (letters, policies drafts, templates)

Acceptable as long as staff review and edit outputs themselves.

2. Use AI for professional development | Staff may use AI to:

- Ask AI to explain topics, pedagogy, or classroom strategies
- Use it to help generate ideas for subject knowledge improvement

3. Use AI tools approved by the school/Trust | Staff should follow the school's:

- Acceptable Use Policy (AUP)
- Data protection and safeguarding policies
- Cloud/third-party software approval processes

4. Use AI for marking guidance (but not replace their judgment) | AI can:

- Suggest feedback wording
- Identify common misconceptions in anonymised work

Staff must still make their own professional judgement.

5. Use AI with anonymised student data | You can use AI if:

- No names, photos, or identifiable details are included
- Student information is generalised or fictionalised
- The platform is GDPR-compliant and approved

NOT GOOD USE

What Staff Must Not Do When Using AI

1. Do NOT input personal, sensitive, or identifiable student data | This includes:

- Student names
- Photos or videos
- SEN information
- Safeguarding concerns
- Behaviour or wellbeing notes
- Assessment data linked to identifiable pupils

This breaches UK GDPR and is the most important rule.

2. Do NOT use AI to make high-stakes decisions about students | AI must not be used to:

- Decide predicted grades
- Make safeguarding judgements
- Assess eligibility for support or interventions
- Diagnose SEND needs
- Evaluate staff performance

Decisions about individuals must always be made by humans.

3. Do NOT use unapproved AI tools with student accounts | Students shouldn't be asked to use AI apps unless:

- The school has checked data-protection compliance
- Parents have been informed where required
- There is clear educational purpose

4. Do NOT trust AI-generated content without checking it | Staff must not:

- Copy resources or facts without verifying accuracy
- Present AI output as factual without quality checks
- Allow AI-produced feedback or reports to be used verbatim

AI tools can make errors or invent information!

5. Do NOT upload copyrighted materials without permission | E.g. sharing:

- Entire textbooks
- Purchased exam papers
- Paid resources

This can breach licensing agreements.

6. Do NOT allow AI to interact with students unsupervised | No:

- AI chatbots acting as teaching assistants
- One-to-one AI tutoring without monitoring
- Safeguarding-sensitive conversations