

Madeley Academy



AI Policy for Staff and Volunteers

Prepared by:	Mr Ian Marshall
Date:	September 2026
Review Date:	September 2027

This policy sets out, in practical terms, how staff at Madeley Academy should use Artificial Intelligence (AI) tools in their day-to-day work. It is written for anyone using AI - whether that is a chatbot for lesson planning, an AI feature inside Microsoft 365, or a specialist education platform and is intended to be read alongside, not instead of, our Data Protection Policy, Online Safety and Acceptable Use Policy, and Safeguarding and Child Protection Policy.

The Academy's detail behind this policy - legal basis, impact assessments, and the framework the trust/school follows to approve new AI systems - sits in our separate AI Governance Policy and Privacy Notice. This document focuses on what that means for you, day to day.

In short

- AI can genuinely reduce workload and support teaching - used well, it is worth using
- You are always accountable for what you send, publish or act on, whether or not AI helped produce it
- The one rule that matters most: identifiable information about a child, colleague or family may only go into a tool that is both on our approved list and set up as a secure Academy account — never into a public tool, and never into a personal AI account, even for a tool the trust otherwise uses (eg Copilot, Gemini)

This policy applies to all staff (teaching, support, administrative and leadership) and to governors and trustees where they use AI tools in connection with their role at Madeley Academy. It covers AI used in the classroom, in administration, in communications with parents and carers, and in any other Academy-related activity.

AI tools are becoming part of ordinary working life in schools. Used carefully, they can save time on planning, drafting and admin, and can support students who need things explained in a different way. Used carelessly, they can put children's data at risk, produce inaccurate or biased content, and create safeguarding and reputational problems. This policy exists to help you get the benefit without the risk. Whatever tool you are using, and whatever it is for, these five habits should guide you.

You stay in charge

AI can draft, summarise and suggest - it does not decide. Any judgement that affects a child, a colleague, or a family must be made by a person, using their professional knowledge, not accepted from an AI tool because it sounds fluent and confident.

Check everything before you rely on it

AI-generated content can be wrong, out of date, or subtly biased, even when it reads as if it is correct. Fact-check names, dates, figures, quotations and legal or policy references before you use, share or act on anything AI has produced, particularly for anything leaving the building.

Say when AI has helped

Be open about it. Where a document, email or resource has had significant input from an AI tool, note that it has, using the wording in Appendix C. This is not about flagging every spell-check - it is about being straightforward when AI has shaped the substance of something.

Only use tools the Academy has approved

Personal or free-tier AI accounts are not appropriate for Academy business. Use only the systems on our approved tools list (Appendix B) and, where provided, your Academy AI account rather than a personal login. If a tool you want to use is not on the list, ask before you use it - see Section 5.

Protect Data — Know which tools you can trust with it

Most AI tools should never see identifiable information about a child, colleague or family. A small number of purchased, enterprise-grade tools - for example Microsoft Copilot or Google Gemini — are different, but only once they have been specifically checked, configured and confirmed as secure within our own Academy environment. Section 3 sets out exactly what this means in practice, and it is the principal staff get wrong most often, so read it carefully.

Data privacy: what you can and cannot put into an AI tool

Many AI tools use whatever you type as further training data, and even where they do not, information you enter may no longer be under the Academy's control. Treat anything, you type into an AI tool as if it could end up outside the organisation - unless it is one of the specific, approved exceptions described below.

Purchased, enterprise tools: the one exception — and where the line is

- Some AI tools we buy as an organisation - for example Microsoft Copilot or Google Gemini - can be configured so that data stays within our own secure tenancy and is not used to train the underlying model. Once IT and the DPO have confirmed a specific tool meets that standard, and it is added to Appendix B as “approved for personal data,” staff may use it with personal data as part of their normal work
- This only applies when you are signed in through your official Academy account (your Academy Microsoft 365 or Google Workspace login, for example) - the exact same tool, used through a personal or consumer account, is not covered and must not be used with any personal data
- It only applies to the specific tools listed in Appendix B as approved for personal data. A tool being “purchased” or “well known” is not enough - if it is not listed, treat it as unapproved
- If you are ever unsure whether you are in the secure Academy version of a tool or a personal one, stop and check with Mr Ian Marshall before entering anything personal

Category	Examples
Approved tenancy tools only — never anywhere else	Student, staff, parent or carer names, dates of birth, addresses, photographs, exam or assessment scripts, safeguarding notes, SEND/EHCP details, health information, HR or disciplinary records, financial or contract details. Only enter this into a tool marked “approved for personal data” in Appendix B, and only through your official Academy-tenancy account (see the box below).
Think twice — check first	Anonymised case studies, information about a small or identifiable group, draft communications that started from a real student record, anything you would not want to see repeated outside the Academy.
Fine in any approved tool	Generic lesson planning, subject knowledge questions, drafting a policy or letter from a blank page, summarising your own already-anonymised notes, general admin templates.

“Fine in any approved tool” still assumes a tool from Appendix B and requires judgement — if you are not sure, treat it as “think twice.”

Special Category and Safeguarding Information

Health, ethnicity, religion, safeguarding concerns and similar special category data need particular care. This includes information that could indirectly reveal these things - for example, a postcode or a combination of details that would let someone work out who a student is. Children are treated as vulnerable data subjects, so processing their data through AI is likely to be higher risk and needs extra safeguards, not fewer.

Sensitive Academy Information

The same caution applies to non-personal but sensitive material - strategic plans, contracts, HR matters, or anything commercially or reputationally sensitive. Do not put this into a third-party AI tool unless it has been specifically checked and approved for that purpose.

Why This Matters Beyond Data Protection

- **Cyber-crime:** information entered into AI tools can be pieced together and misused, including for impersonation or fraud
- **Copyright and IP:** do not feed a student's or colleague's original work, or copyrighted material, into a generative AI tool to train or generate content without the right to do so
- **Deskilling:** leaning on AI too heavily, for too long, can erode your own expertise. It is a tool to support your judgement, not a substitute for it

Using AI in your Day-to-Day Role

The principles above apply to everyone. In practice, they look slightly different depending on your role.

Role	In Practice This Means
Teaching staff	Only use tools from the approved list for lesson planning, resources and feedback; only enter student names or identifiable information into a tool marked "approved for personal data" in Appendix B, via your Academy account — never a personal one; tell students clearly when a resource has been AI-assisted; keep checking AI output against your own subject knowledge.
Support and admin staff	Use approved tools for templates, minutes and general drafting; only put personal or sensitive data into a tool marked "approved for personal data" in Appendix B, signed in through your official Academy account; flag new tools to the GDPR lead before trying them.
Middle and senior leaders	Model good practice; keep the approved and prohibited tools list current; make sure new uses go through the DPIA screening step; build AI awareness into induction and CPD; own the reporting route for concerns.
Governors/trustees	Ask for assurance that this policy is being followed; understand the risks in plain terms; treat AI as a standing item for review alongside data protection and safeguarding.

Approved Tools, and what to do if you want to try a new one

Madeley Academy maintains a list of approved AI tools (Appendix B) and a list of tools that must not be used for school business. Both are reviewed regularly and published to staff. Appendix B also shows which of those tools have been specifically confirmed as safe to use with personal data - being on the general approved list is not the same thing as being approved for personal data, so check both columns before you rely on a tool for anything involving a named student, colleague or family.

If you come across a tool you think would help in the classroom or in admin do not simply start using it.

Instead:

1. Speak to Mr Ian Marshall before you use it for anything involving Academy data.
2. They will carry out an initial check, including a short screening exercise to see whether a full Data Protection Impact Assessment (DPIA) is needed.
3. Where personal data will be involved, the DPIA will be carried out with input from the Data Protection Officer before the tool is approved.

4. Once approved, the tool is added to Appendix B and communicated to relevant staff.

This is not intended to slow good ideas down — it exists so that a tool with a data protection or safeguarding problem is caught before it is in wide use, not after.

Being Transparent about AI Use

Openness about AI use builds trust with students, parents, carers and colleagues, and protects you if a decision or document is later questioned. Where AI has meaningfully shaped a piece of work — not just tidied up spelling — use the disclaimer at Appendix C, or a version of it appropriate to the context (for example, in a footer, a covering note, or spoken to a class).

For anything shared with parents, carers, or external agencies, transparency also means being ready to explain, in plain terms, what role AI played and why the final content can be relied upon.

Safeguarding Considerations

AI brings some safeguarding risks that are new, and some that are familiar risks in a new form. Staff should be alert to:

- Deepfakes and impersonation — AI-generated images, audio or video used to deceive, embarrass or harm someone
- Bullying and harassment carried out or amplified using AI-generated content
- Grooming, coercion or exploitation, where AI tools may be used by those seeking to harm children
- Age-inappropriate or biased content, including image generation tools that are not designed with children in mind

Any concern involving AI and a child's safety should be raised through our normal safeguarding route — via Mr Duncan Marshall — not treated as a separate “IT issue.” AI can be an aggravating factor in a safeguarding matter, and should be considered as part of any investigation, not overlooked because the harm happened “on a computer.”

Reporting concerns and getting help

Something has gone wrong, or you are not sure it has

Tell Mr Ian Marshall as soon as you become aware of it — for example, personal data entered into a tool by mistake, an AI tool producing something inappropriate or biased, or a suspected misuse of AI by a member of staff, student, or third party. Early reporting makes a real difference to how quickly a problem can be contained.

It involves possible illegal activity or risk of serious harm

Escalate immediately through our safeguarding procedures, in addition to reporting it as above. Where AI tools are used to help monitor or flag incidents, a person must always review the output — automated systems can miss context and nuance that matters.

You are just not sure what is allowed

Ask before you act. Contact Mr Ian Marshall, who will involve the Data Protection Officer where needed. It is always better to check first than to explain afterwards.

Training and Support

Madeley Academy will provide training to help staff use AI safely and effectively, including an introduction for all staff and more detailed sessions for those using AI regularly in their role. You also have a responsibility to recognise your own gaps — if you are unsure how to use a tool safely, say so, rather than guessing.

Quick-Reference Checklist

Before you use an AI tool for anything work-related, run through this:

Ask yourself, every time

- Is this tool on our approved list?
- If I'm about to type anything identifiable, is this tool specifically marked "approved for personal data" in Appendix B, and am I signed in through my official Academy account rather than a personal one?
- If either answer is no, have I kept every student's, colleague's or family's identifiable information out of what I've typed?
- Have I checked the output for accuracy, bias, and anything that doesn't sound right?
- Do I need to tell anyone AI was involved in producing this?
- If this affects a real decision about a person, has a human — me — actually made that decision?
- If I'm not sure about any of the above, have I asked before going ahead?

Appendix A: Where to Find More Detail

- Legal basis for our use of AI, and students'/staff's data protection rights — see the AI Privacy Notice.
- Governance, roles and the trust-level decision-making process for adopting new AI systems.
- Online conduct expectations more broadly — see the Online Safety and Acceptable Use Policy.
- Reporting a data protection concern — see the Data Breach Staff Guide.

Appendix B: Approved AI Tools

This list is maintained and published by Mr Ian Marshall and reviewed at least termly. Staff should check the current version rather than relying on this printed copy.

The “Approved for personal data?” column matters as much as the tool's name. A tool can be approved for general Academy use (drafting, planning, admin) without being cleared for personal data — that separate confirmation only follows a specific security check of our own tenancy configuration for that tool. The example rows below show the format; each entry must be confirmed for our own environment before it is marked “yes,” and access must always be through the official Academy account for that tool, never a personal one.

Tool	Access route	Approved for personal data?	Notes / restrictions
Microsoft Copilot	Academy Microsoft 365 tenancy account	Yes — confirmed secure within our tenancy	Must be accessed via your Academy Microsoft 365 login. Do not use a personal/consumer Copilot account for Academy business.
Google Gemini	Academy Google Workspace tenancy account	Yes — confirmed secure within our tenancy	Must be accessed via your Academy Google Workspace login. Do not use a personal Gmail-linked Gemini account for Academy business.

Tools not to be used for Academy Business

This includes personal/individual AI accounts set up using a Academy or personal email address, any tool the Academy has specifically prohibited, and any tool not yet checked and approved.

Appendix C: Suggested AI Use Disclaimer Wording

Standard wording:

“This policy was produced with the assistance of AI tools in line with Madeley Academy’s AI policy. All content has been reviewed and is subject to human oversight and professional judgement.”

Appendix D: Quick DPIA Screening Questions

Before adopting a new AI system, work through these with [named GDPR Lead]. A “yes” to any of them is a strong signal that a full DPIA is needed before proceeding.

- Will the tool collect new information about identifiable individuals?
- Will it require individuals to provide information about themselves?
- Will data be used for a purpose it was not originally collected for?
- Does it involve new or privacy-intrusive technology, such as profiling or facial recognition?
- Could it result in decisions or actions being taken about individuals that have a significant effect on them?
- Does it involve particularly sensitive information — children's data, health, or HR records?
- Could it result in contacting individuals in a way they might find intrusive?