



Date: September 2025
Review Date: September 2026
Responsible person: Jess Temple

Introduction and Purpose

This policy provides clear guidance for all staff at More Than Ed on the appropriate use of artificial intelligence tools in their professional work. As an SEMH school working with vulnerable young people, we recognise that AI can support our planning and administrative tasks while maintaining the highest standards of data protection and confidentiality.

This policy applies to all staff members, including teachers, support staff, administrators, and leadership, when using AI tools such as ChatGPT, Claude, Twinkl AI, or any similar platforms for work purposes. This policy operates within the framework of our E-Safety Policy 2025 and should be read in conjunction with that document.

Fundamental Rule: No Personal Data

The most important principle of this policy is absolute:

No student names, personal information, or any identifiable data must ever be entered into any AI system.

This prohibition includes, but is not limited to:

- Student names, dates of birth, addresses, or parent/carer details
- Specific medical or SEMH diagnoses
- Detailed behavioural incidents
- Assessment scores or data linked to individuals
- EHCP details or safeguarding information
- Any combination of information that could identify a student

Even with names removed, contextual details can be identifying, so staff must exercise extreme caution. This aligns with our E-Safety Policy requirement that children's names should not be entered into any internet-based software.

Acceptable Use of AI

Staff are trained and able to use AI tools to enhance their professional efficiency in appropriate ways. AI can be particularly helpful for:

- Generating lesson plan templates and curriculum frameworks
- Creating generic educational resources and worksheets
- Developing differentiated activities for various learning needs
- Drafting assessment criteria and marking rubrics
- Producing example texts for teaching purposes
- Creating newsletter content without personal information
- Brainstorming teaching strategies for common SEMH needs

When using AI for these purposes, frame all requests in general terms. For example, ask for "strategies to teach mathematics to students with anxiety" rather than referencing any specific student or situation.

The key to safe AI use is maintaining complete separation between AI assistance and personal data. You might use AI to generate a bank of report comments or create lesson templates, but the moment you add specific student information, this must be done without AI assistance. Think of AI as a tool for creating the framework and structure of your work, while all personalisation happens offline.

Professional Responsibility and Quality Assurance

While AI can be a valuable tool, all staff remain fully responsible for any content they use professionally, regardless of whether AI assisted in its creation. Every piece of AI-generated content must be thoroughly reviewed before use for:

- Factual accuracy and reliability
- Age-appropriateness for our students
- Suitability for students with SEMH needs
- Potential triggers or sensitive content affecting students with trauma histories
- Alignment with school values, policies, and curriculum requirements

Staff should be particularly mindful that AI can generate plausible sounding but incorrect information. Mathematical problems should be checked for accuracy, historical facts should be verified, and any scientific content should be confirmed against reliable sources. Resources should always be adapted to meet the specific needs of our student population, as AI cannot understand the unique context of our school community.

Data Protection and Safeguarding

This policy ensures our compliance with UK GDPR and the Data Protection Act 2018, as outlined in our E-Safety Policy. Most AI platforms store and may train on the data users' input, and we cannot control where this data goes, who accesses it, or how long it is retained. By absolutely prohibiting personal data entry, we eliminate these risks entirely.

Even platforms that claim not to train on user data cannot guarantee complete security, making our blanket prohibition essential for protecting our vulnerable students. This approach aligns with our school's broader commitment to E-Safety and responsible digital practice.

Safeguarding Considerations

Safeguarding matters must never involve AI. Never use AI to:

- Analyse safeguarding concerns
- Respond to disclosures
- Make decisions about student welfare
- Draft safeguarding reports or documentation

All safeguarding matters must be handled through established procedures with appropriate human professional judgement, as outlined in our safeguarding policies.

Data Breach Procedures

If you accidentally enter any personal or safeguarding information into an AI system, stop immediately and report the incident to the Compliance Manager within two hours. This aligns with our E-Safety Policy requirement that all E-Safety issues must be reported immediately to the Headteacher.

Practical Implementation

When planning lessons or creating resources, think strategically about how to use AI effectively while maintaining data protection. Develop a collection of useful prompts that generate helpful content without requiring personal information. For instance, you might build a library of prompts for different subject areas and SEMH needs that can be reused and refined over time.

Consider using placeholder names when creating example work or scenarios, making it clear these are fictional. If you need to create differentiated resources, describe the needs in terms of general categories rather than individual students. Share successful approaches with colleagues to build collective expertise.

Remember that the time saved through AI use should enhance, not replace, the personalised attention we give to our students' individual needs. All AI-generated resources must be thoroughly reviewed and adapted before use with students.

Training and Compliance

All staff will receive training on this policy, including:

- Practical examples of acceptable and unacceptable use
- Techniques for using AI safely and effectively
- Understanding of data protection implications
- Integration with E-Safety procedures and protocols

The school will maintain a list of approved AI tools and provide ongoing support through sharing best practices and effective strategies. This training forms part of our broader E-Safety training programme.

Consequences of Policy Breaches

If a staff member accidentally breaches this policy by entering personal data into an AI system, they must:

- Immediately stop using the tool
- Report to the Compliance Manager and Headteacher within 2 hours
- Document what information was shared
- Cooperate fully with breach investigation procedures

Deliberate or negligent breaches may result in:

- Removal of AI access privileges
- Mandatory additional training
- Formal disciplinary procedures
- Potential personal liability for data protection violations

These consequences align with our E-Safety Policy protocols for breaches of digital safety standards.

Monitoring and Review

The Senior Leadership Team will regularly review AI use within the school, ensuring compliance with this policy and identifying opportunities for improved practice. This monitoring forms part of our overall E-Safety and data protection oversight.

This policy will be reviewed annually or sooner if significant changes in technology or legislation occur. Staff will be notified of any updates and required to confirm their understanding of changes. The policy will be reviewed in parallel with the E-Safety Policy to ensure continued alignment.

Summary for Quick Reference

The Golden Rule:

Never enter any student names or personal information into AI systems.

Safe to use AI for:

Generic lesson planning, resource templates, teaching strategies, curriculum planning, and general administrative tasks.

Not safe for AI:

Anything containing names, personal details, specific incidents, medical information, safeguarding matters, or any potentially identifying information.

If you make a mistake:

Stop immediately and contact the Compliance Manager and Headteacher within 2 hours.

Remember:

You remain responsible for all content you use, even if AI-generated. Always review and adapt AI content before use. This policy operates within our E-Safety Policy framework.

Related Policies:

- E-Safety Policy 2025
- Data Protection and GDPR Policy
- Safeguarding Policy
- Acceptable Use Policy