



SUAT AI Policy

Last reviewed	January 2026
Reviewed by	SLT
Approved by	CEO
Date of approval	January 2026
Policy owner	SLT
Location	Trust Website

Statement of Intent

At Staffordshire University Academies Trust, we recognise that the use of artificial intelligence (AI) can help to positively affect staff workload, develop pupils' intellectual capabilities and prepare them for how emerging technologies will change workplaces. Whilst there are many benefits to the use of AI tools, the content they produce may not always be accurate, safe or appropriate, and could lead to malpractice and safety concerns.

Through the measures outlined in this policy, the Trust and academies aim to ensure that AI is used effectively, safely and appropriately to deliver excellent education that prepares our pupils to contribute to society and the future workplace.

Artificial Intelligence (AI) technology is already widely used in commercial environments and is gaining greater use in education. We recognise that the technology has many benefits and the potential to enhance outcomes and educational experiences, with the opportunity to support staff in reducing workload.

We also realise that there are risks involved in the use of AI systems, but that these can be mitigated through our existing policies and procedures, amending these as necessary to address AI risks. We will educate staff and learners about safe and ethical use of AI, preparing them for a future in which AI technologies are likely to play an increasing role.

The safeguarding of staff and learners will, as always, be at the forefront of our policy and practice.

This policy outlines our commitment to integrating Artificial Intelligence (AI) responsibly and effectively within the learning environment. We will use AI responsibly, safely and purposefully to support these aims:

- Enhance academic outcomes: Improve educational experiences and performance for pupils.
- Support teachers: Assist in managing workloads more efficiently and effectively.
- Educate on AI use: Promote safe, responsible, and ethical AI practices among staff and learners.
- Develop AI literacy: Incorporate AI as a teaching tool to build AI skills and understanding.
- Prepare for the future: Equip staff and pupils for a future where AI is integral.
- Promote educational equity: Use AI to address learning gaps and provide personalised support.

For the purposes of this policy, the following terms are defined as:

- **AI** – The theory and development of computer systems able to perform tasks normally requiring human intelligence, e.g. visual perception, speech recognition, decision-making.
- **Generative AI** – A category of AI models that generate new outputs based on the data they have been trained on and the user's prompt. These include, but are not limited to, ChatGPT, Google Bard, Anthropic Claude, and Inflection's Pi models.
- **Misuse of AI** – Any use of AI which means that pupils have not independently demonstrated their own attainment, or where AI is not used appropriately to achieve work or educational purposes, or for malicious reasons.

Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR)
- JCQ (2023) 'Artificial Intelligence (AI) Use in Assessments: Protecting the Integrity of Qualifications'
- JCQ (2023) 'Suspected Malpractice Policies and Procedures'
- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR)
- DfE (2024) 'Keeping children safe in education 2024'
- DfE (2023) 'Generative artificial intelligence (AI) in education'
- DfE (2024) 'Meeting digital and technology standards in schools and colleges'
- Ofsted (2024) 'Ofsted's approach to artificial intelligence (AI)'
- DfE (2024) 'Using technology in education'
- DfE (2024) 'Generative AI in education: user research and technical report'
- DfE (2024) 'Generative AI in education: educator and inspector views'
- DfE (2026) Generative AI: 'product safety standards'
- NCSC (2024) 'AI and cyber security: what you need to know'
- NCSC (2024) 'Machine learning principles'

Roles and Responsibilities

The LAC will be responsible for:

- Ensuring that this policy is effective in their setting.
- Ensuring their own knowledge of the use of AI tools in the academy is up-to-date.
- Ensuring all staff undergo child protection, data protection, cyber security and safeguarding training, including online safety, at induction and at regular intervals.
- Ensuring their Academy follows the DfE's digital and technology standards.
- Overseeing the budget allocation for AI tools, training, and infrastructure.
- Liaising with academy leaders in understanding the selection process for which AI tools are most appropriately suitable for classroom use.

The Headteacher will be responsible for:

- Ensuring that staff receive regular, up-to-date training on how to use AI tools ethically, compliantly and securely.
- Ensuring that the use of AI tools in their academy is integrated into relevant policies and procedures, the curriculum and staff training.
- Communicating with parents to ensure they are kept up-to-date with how AI tools are being used in the academy, how this will impact pupils' education and how the academy is ensuring the tools are being used safely and effectively.
- Ensuring that AI practices are reviewed and evaluated on a regular basis.

- Leading the process in selecting, reviewing and approving which AI tools will be utilised in the classroom.
- Identifying potential barriers to AI adoption and ensuring that teachers have the skills and infrastructure to further the use of AI in the classroom.
- Liaising with ICT technicians and subject leaders, the DPL and DPO to review, approve or disapprove of suggested AI tools.
- Promoting a culture of innovation while ensuring the ethical use of AI tools.
- Listening and responding to any feedback and/or concerns raised by parents, pupils, or staff regarding the use of AI tools in the school.
- Keeping an up-to-date record of the AI tools being implemented by the academy.

ICT technicians will be responsible for:

- Providing technical support in the development and implementation of the academy's AI practices, policies and procedures.
- Implementing appropriate security measures.
- Ensuring that the use of AI tools is taken into consideration when creating policies and procedures regarding online safety, child protection and safeguarding, and data protection.
- Supporting the vetting of AI tools and reviewing tools before they are implemented.
- Regularly updating software and ensuring that AI tools are running the latest and safest versions.

The DPO will be responsible for:

- Keeping up-to-date and informed with AI technologies relevant to the Trust and education sector.
- Understanding and maintaining awareness of what the use of AI means for data protection in the Trust.
- Advising the Trust on how to integrate the use of AI while complying with data protection regulations.
- Keeping an up-to-date record of the AI tools being implemented.
- Supporting arrangements to protect the privacy of personal data.
- Establishing and regularly reviewing protocols for data storage, sharing, and disposal related to AI tools.

The DSL will be responsible for:

- Taking the lead responsibility for online safety in their academy.
- Undertaking training so they understand the risks associated with using AI tools in their academy.
- Liaising with relevant members of staff on online safety matters.
- Maintaining records of reported online safety concerns relating to the use of AI tools, as well as the actions taken in response to concerns.
- Reporting to the LAC about the use of AI tools and how it links to safeguarding.
- Monitoring the use of online systems via Academy monitoring tools.

- Being a point of contact for teachers and subject leaders using AI in classrooms to discuss any safeguarding concerns or queries.
- Collaborating with external agencies to stay updated on the latest online threats related to AI.
- Organising awareness campaigns for pupils on the ethical and safe use of AI.

Subject leaders will be responsible for:

- Researching and identifying the most effective and appropriate AI tools for their subject's curriculum.
- Seeking approval from the Headteacher, ICT technicians and DPO for any AI tools they wish to use in their curriculum.
- Requesting support from ICT technicians with the implementation of AI tools where needed.
- Where appropriate, effectively integrating the use of AI tools into lesson plans.
- Familiarising themselves with the AI tools they are using in their lessons and ensuring that they have an understanding of the technology and the risks it poses.
- Assisting pupils to use and understand the chosen AI tools.
- Regularly sharing insights and feedback with other subject leaders to ensure cross-curricular coherence in AI tool use.
- Staying updated on global best practices in the use of AI tools.

All staff members will be responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Taking responsibility for the security of the AI tools and data that they use or have access to.
- Modelling good online behaviours when using AI tools.
- Maintaining a professional level of conduct in their use of AI tools.
- Having an awareness of the risks that using AI tools in academy poses.
- Reporting concerns in line with the Academy's reporting procedure.
- Where relevant to their role, ensuring that the safe and effective use of AI tools is embedded in their teaching of the curriculum or the work within their role.
- Familiarising themselves with any AI tools used by the Academy and the risks they pose.
- Not using AI tools which have not been vetted and raising with the Data Protection Lead where they identify new tools which they would like to explore the use of.
- Not entering personal, confidential, sensitive or business critical data into AI.
- Understanding the ethical usage of AI in education.
- Providing feedback to ICT technicians and the headteacher on the effectiveness of using AI tools.
- Participating in CPD related to AI.
- Encouraging pupils to critically assess and provide feedback on the AI tools being used.

Pupils will be responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Seeking help from the relevant academy staff if they are concerned about an experience that they or a peer has experienced while using AI tools.
- Reporting concerns in line with the academy's reporting procedure.

- Familiarising themselves with any AI tools used by the academy and the risks they pose. Demonstrating responsibility and ethical behaviour while using AI tools, including not attempting to manipulate or misuse the tools.
- Sharing feedback with teachers regarding their experiences and suggestions for AI tools.

Parents will be responsible for:

- Staying informed about the AI tools their children are using in school.
- Collaborating with the school in ensuring safe and ethical use of AI tools at home.
- Attending training or information sessions organised by the academy about AI tools.

Data Protection and Cyber Security

The Trust and academies are aware of the data privacy and cyber-security implications that come with using generative AI tools and will ensure that all AI tools are used in line with the Trust's data protection, online safety and security policies. Academies will follow the procedures in these policies to continue to protect pupils from harmful online content that could be produced by AI tools.

Academies will not enter data that is classed as personal, sensitive or business critical into AI tools without undertaking the due diligence and following the processes set out within this policy. Any data entered will not be identifiable to individuals and will be considered released to the internet.

All staff will be made aware that generative AI tools are able to create believable content of all kinds, for example credible email scams requesting payment, and that the content AI produces may seem more authoritative and believable than usual scams. All staff will apply their best judgement and common sense to manage cyber-security risks effectively and ensure that the DfE's [cyber standards](#) are adhered to.

Academies will:

- Protect personal and special category data in accordance with data protection legislation.
- Not allow or cause intellectual property, including pupils' work, to be used to train generative AI models, without appropriate consent or exemption to copyright.
- Review and strengthen cyber security by referring to the DfE's cyber standards.
- Be mindful that generative AI could increase the sophistication and credibility of cyber-attacks.
- Ensure that pupils are not accessing or creating harmful or inappropriate content online, including through AI tools.
- Refer to the DfE's [Filtering and monitoring standards for schools and colleges](#) to ensure that the appropriate systems are in place.
- Be mindful of the data privacy implications when using AI tools and will take steps to ensure that personal and special category data is protected in accordance with data protection legislation.
- Review the storage and security features of AI tools before using them, seeking advice from the DPO as required, and conducting a data protection impact assessment.

Before using personal data in AI tools, academies will ensure that the tools comply with data protection legislation and existing privacy policies to protect the data. Academies will first consult the DPO, complete a Data Protection Impact Assessment and ensure communication with individuals about the use of their data in AI tools.

Academies will ensure that personal data is protected in line with data protection legislation and the Trust's data protection policies and procedures. Academies will research and be aware of the privacy implications and notices of any AI tools that it selects for classroom and work use.

When selecting generative AI models for classroom use, Academies will ensure that any chosen models comply with data protection legislation. Unless appropriate consent or copyright exemption is given, the Academy's intellectual property, including the work of pupils, will not be used to train generative AI systems.

Academies will review and strengthen their cyber-security measures in line with the DfE's 'Meeting digital technology standards in schools and colleges' guidance. This will include conducting a cyber security risk assessment that considers any AI tools used by each setting and generative AI's evolving sophistication.

Academies should ensure that a cyber awareness plan is implemented and understood by staff and pupils alike and is adopted by the whole school. Each Academy's implementation of generative AI tools will be done with secure control access to minimise any misuse.

Each Academy's procedures for reporting a cyber-attack will be communicated and understood by all in accordance with the Cyber Response Plan.

Using AI tools

Academies will ensure that AI tools are used appropriately to achieve the following aims:

- To reduce workload
- To create efficiencies and save time
- To assist with the production of high-quality and compliant administrative plans, policies and documents
- To support the teaching of a knowledge-rich computing curriculum
- To teach pupils:
 - How to use emerging technologies safely and appropriately.
 - About the limitations, reliability and potential bias of AI tools.
 - How information on the internet is organised and ranked.
 - How online safety practices can protect against harmful and misleading content.
 - To identify and use appropriate resources to support their education, including age-appropriate resources and preventing over-reliance on a limited number of tools or resources.

Whilst recognising that AI tools can be used appropriately and with benefit to teaching and learning, the academy will keep in mind that the content produced by AI tools can be:

- Inaccurate.
- Inappropriate.

- Biased.
- Taken out of context and without permission.
- Out of date or unreliable.

Where AI tools are used to produce administrative plans, policies and documents, all staff members will understand that the quality and content of the final document remains the professional responsibility of the staff member who produced it. Staff members using AI tools to create documents will not assume that AI output will be comparable with a human-designed document that has been developed in the specific context of their setting.

Pupils/students will be made aware of the importance of referencing AI tools correctly when using AI tools to produce work, especially if the work is for an assessment, in order to allow teachers and assessors to review how AI has been used and whether it was appropriate. Pupils' / students' references to AI sources will show the name of the AI source and the date that the content was generated.

Pupils / students will retain a copy of the questions and AI generated content for reference and authentication purposes in a non-editable format, e.g. a screenshot. Pupils / students will also provide a brief explanation of how AI tools have been used.

When using AI tools, staff and pupils will ensure that any content produced is scrutinised and cross-checked for its appropriateness and accuracy.

Staff members will be aware that AI tools return results based on the dataset it has been trained on – it may not have been trained on the national curriculum or specific area of their work, and may not provide results that are comparable with a human-designed resource developed in the context of the national curriculum or specific areas of their work. Staff members will be mindful of this in their teaching and marking of pupils' work, and in completing their own work.

Staff and pupils must be aware that AI tools cannot replace the judgement and deep subject knowledge of a human expert. Staff members will stress the importance of pupils acquiring their own knowledge, expertise and intellectual capability rather than relying on AI tools in their work.

Academies will not allow or cause pupils' original work to be used to train AI tools unless it has appropriate consent or exemption to copyright. Consent will be sought from students over 18; however, for pupils under 18, consent will be sought via their parents.

Understanding and Accessing AI

Academies will ensure that leaders and teachers are equipped with the knowledge and skills to use AI effectively in the classroom. Any barriers that are identified in teachers' understanding of AI will be addressed through training to ensure that all teachers fully understand the most effective applicable use of AI in the classroom.

Academies will ensure that sufficient digital infrastructure is provided for all staff to utilise AI. Any implementation of AI technology will be done with the assurance from IT support providers that each Academy's pre-existing digital systems are compatible with the AI platforms themselves to ensure accessibility and ease of use.

When implementing an effective infrastructure, Academies will agree on the upfront costs to pay for AI providers that charge for the full access and use of their platforms in accordance with

the Scheme of Delegation, data protection policies and appropriate implementation of data protection impact assessments where required.

Misusing AI Tools

Preventing misuse

Academies acknowledge that misuse of AI tools can happen both accidentally and intentionally, and that education and awareness is key to preventing misuse. Academies should take the following actions to prevent the misuse of AI tools:

- Restricting access to online AI tools on Academy devices and networks, especially on devices used for exams and assessments.
- Setting reasonable deadlines for submission of work and providing pupils with regular reminders.
- Allocating time for sufficient portions of pupils' work to be completed in class under direct supervision, where appropriate.
- Examining intermediate stages in the production of pupils' work to ensure that work is being completed in a planned and timely manner, and that work submitted represents a natural continuation of earlier stages.
- Introducing classroom activities that use the level of knowledge and understanding achieved during lessons to ensure the teacher is confident that pupils understand the material.
- Engaging pupils in verbal discussions about their work to ascertain that they understand it and that it reflects their own independent work.
- Refusing to accept work that is suspected to have been generated through misuse of AI tools without further investigation.
- Issuing tasks which are, wherever possible, topical, current and specific, and require the creation of content which is less likely to be accessible to AI models.
- Investing in educating and training staff, pupils and parents on the use of AI tools and raising awareness of the risks and issues that come with its use.
- Using appropriate filtering and monitoring software in accordance with the Online Safety Policy.
- Researching appropriate AI tools based on the purpose of their use, informing staff and pupils of approved tools and how they should be used.

Identifying Misuse

Staff members will continue to use the skills and observation techniques already in use to assure themselves that pupils' work is authentically their own when attempting to identify a misuse of AI tools.

When reviewing pupils' work to ensure its authenticity, staff members will compare it against other work created by the pupil. Where the work is made up by writing, the staff members will make note of:

- Spelling and punctuation.
- Grammatical usage.
- Writing style and tone.
- Vocabulary.
- Complexity and coherency.
- General understanding and working level.

- The mode of production, i.e. whether the work was handwritten or word-processed.

Staff members will be aware of and look out for potential indicators of AI use, which include:

- A default use of American spelling, currency, terms and other localisations.
- A default use of language or vocabulary which might not be appropriate to the working or qualification level.
- A lack of direct quotations and/or use of references where these are required or expected.
- Inclusion of references which cannot be found or verified.
- A lack of reference to events occurring after a certain date, reflecting when an AI tool's data source was compiled.
- Instances of incorrect or inconsistent use of first-person and third-person perspective where AI generated text has been left unaltered.
- A variation in the style of language evidenced in a piece of work, if a pupil has taken specific portions of text from an AI tool and then amended it.
- A lack of graphs, data tables or visual aids where these would normally be expected.
- A lack of specific, local or topical knowledge.
- Content being more generic in nature.
- The inadvertent inclusion of warnings or provisos produced by AI tools to highlight the limits of its ability or the hypothetical nature of its output.
- The submission of pupil work in a typed format, where this is not usual, expected or required.
- The unusual use of several concluding statements throughout the text, or several repetitions of an overarching essay structure within a single lengthy essay.
- The inclusion of confidently incorrect statements within otherwise cohesive content.

Staff members will remain aware that AI tools can be instructed to employ different languages and levels of proficiency when generating content, and some are able to produce quotations and references. Where Academies are considering using programmes and services to be able to analyse content and determine the likelihood that this was produced by AI, they must first consult with the data protection team and complete a data protection impact assessment where required.

Staff members found to be deliberately and/or repeatedly misusing AI tools will be disciplined in line with the Disciplinary Policy and Procedures. Pupils found to be deliberately and/or repeatedly misusing AI tools will be sanctioned in line with their Academy's Behaviour Policy. Where staff or pupils are found to be misusing AI tools, the Headteacher will review the circumstances and consider revoking access to the AI tools for the concerned individuals.

Staff, pupils and parents will be educated on the correct and appropriate ways to use the AI tools they are given access to. Academies will provide information for parents on the dangers of AI misuse and information on how to raise any concerns or queries.

Periodic training sessions will be organised for staff and pupils, including the ethical use of AI tools, including to address the distinction between legitimate assistance and over-reliance on AI.

Academies will maintain an understanding and awareness that data used to train generative AI models is susceptible to malicious actions, which in turn has a negative impact on pupils using

compromised AI systems. Academies will therefore be aware of two prominent types of data corruption:

- Prompt injection attacks: these are when attackers input data into the AI model to make it behave in unintended ways, including generating offensive content or sensitive information.
- Data poisoning attacks: these are when attackers tamper with data that an AI model has already been trained on to produce similarly undesirable or hateful outcomes.

ICT technicians, in collaboration with Academy staff and the DPO, will regularly review the AI tools that are in use and which an Academy wishes to implement, ensuring that they do not inadvertently promote misuse.

Academies will establish a feedback mechanism allowing staff and pupils to report any instances where AI tools might encourage misuse or where they feel uncertain about the ethical boundaries of using such tools. In cases of AI misuse, Academies will maintain a transparent process, detailing how the misuse was identified and the steps taken in response. Academies will recognise that AI tools have limitations and will encourage a healthy scepticism and critical thinking when using or analysing outputs from AI tools.

Vulnerable Groups

The Trust and Academies recognise that vulnerable learners are more likely to be at risk from the misuse of AI (both in their own use or through the actions of others). Academies shall ensure that vulnerable learners are offered appropriate support to allow them to gain full benefit of the use of AI, while being aware of the potential risks, based on their individual circumstances.

Children are considered to be vulnerable data subjects and therefore any process involving their personal data is likely to be “high risk”. AI/ automated processes shall not be used to make significant decisions about people.

Reporting

Academy reporting systems should be well promoted, easily understood and easily accessible for staff, learners and parents/carers to confidently report issues and concerns, knowing these will be treated seriously. All reports will be dealt with swiftly and sensitively and outcomes shared where appropriate. Reports should be made to the Designated Safeguarding Lead and Data Protection Lead within the Academy.

Responding to an Incident or Disclosure

An academy’s response must always be based on sound safeguarding principles and follow Trust and departmental safeguarding procedures.

- All AI incidents (including data breaches and/or inappropriate outputs) must be reported promptly to the DPL and DPO. Effective reporting helps mitigate risks and facilitates a prompt response.
- Where relevant / required incidents will be reported to external agencies e.g., Police, LADO, ICO.
- All AI related incidents will be recorded through the usual normal recording systems, including the data protection system.

In the case of misuse of AI by staff, the normal staff disciplinary processes will be followed.

Risk Assessment

It is key that our approach to managing risk aligns with, and complements, our broader safeguarding approach.

The Trust and academies understand that despite many positive benefits in the use of AI, there are some risks that will need to be identified and managed, including:

- Legal, commercial, security and ethical risks
- Data Protection
- Cyber Security
- Fraud
- Safeguarding and well-being
- Duty of care

Training

As AI becomes an integral part of modern education, it is essential for staff to be trained in its effective use. Training equips educators with the knowledge and skills to integrate AI tools responsibly into teaching, learning, and administrative processes. It ensures that AI is used to enhance educational outcomes, streamline workloads, and promote equity while safeguarding ethical practices and data privacy. By fostering AI literacy, staff can confidently prepare pupils for a future where AI is a key driver of innovation and opportunity.

- Training shall be provided for staff on the effective, responsible, and ethical use of AI technologies in education, ensuring these tools enhance teaching, learning, and administrative processes.
- Academies will integrate AI-related risks and safeguards into annual safeguarding training, aligning with statutory guidance, including "Keeping Learners Safe."
- Academies will ensure all staff are equipped with the knowledge and skills to confidently integrate AI into their professional practice and to prepare pupils for a future shaped by AI-driven innovation and opportunities.
- Academies will train staff to identify, assess, and mitigate risks associated with AI technologies, including issues such as biased algorithms, privacy breaches, and harmful content.
- Academies will train staff on robust data protection practices, ensuring compliance with UK GDPR and other relevant regulations while using AI systems.
- Academies will promote ethical practices in the use of AI, ensuring that these technologies contribute to equity, fairness, and inclusivity in education.
- Academies will empower educators to teach learners about the safe and ethical use of AI, cultivating a culture of awareness, resilience, and informed decision-making in the digital age.
- Academies will train staff to use AI responsibly as a tool to monitor and address online risks, reinforcing our commitment to a safe learning environment.

Selection of AI tools

Teachers, leaders and the DPL will be responsible for researching and identifying the most appropriate and accessible AI tools for their work, taking into account:

- The needs and abilities of their pupils.
- Compatibility with their Academy's ICT systems.
- Online safety and safeguarding concerns.
- The subject the AI tool is being used to teach.
- The security of pupil and teacher data when using these systems.
- The purpose of using the system.

Before fully integrating an AI tool into lessons, academies will consider introducing a trial or evaluation period. During this time, a small group of pupils and teachers may use the tool, providing feedback on its effectiveness, ease of use, and any potential concerns.

Any AI tools intended to be used by academies will not be used until the Headteacher, DPL, DPO and ICT technicians have reviewed the systems and given their approval. Academies will inform parents via their designated communication system whenever a new AI tool is approved for school use and specify which year groups will be given access to the tool.

Staff will thoroughly research potential AI tools, ensuring that the tools are as reliable and safe as possible. Where there are concerns over the accuracy, reliability or appropriateness of an AI tool, staff will not submit these tools to the Headteacher for approval and will not use these tools.

Academies understand that many generative AI tools, such as ChatGPT, have recommended age restrictions. Whilst some tools may be useful for staff members, academies must take steps to ensure that any AI tool used in class is appropriate for the age group who are using it.

Academies will follow the Online Safety Policy, Information Security Policy and Safeguarding Policy at all times when considering which AI tools to incorporate into their work, and classroom learning.

Academies must keep a record of:

- The AI tools that have been approved for use.
- The AI tools that have not been approved for use, including member of staff submitted the tool for approval and the reason that approval was denied.
- The teachers that are choosing to use AI tools in their lessons.
- The subjects that AI tools are being used to teach.
- The year groups that are using AI, and which AI tools each year group has access to.
- The date that specific AI tools were given approval.
- The date that specific AI tools were implemented in lessons.
- Any concerns raised by parents, pupils or staff regarding the use of AI tools.
- Relevant login details for each approved AI platform.
- The AI tools being used for administrative and business purposes.
- The purpose for which the tools are being used.
- The effectiveness of the tools based on the intended purpose.

This record will be kept on Teams and will be reviewed and updated by ICT technicians, the DPL, DPO, and the Headteacher where necessary.

In addition, academies will:

- Encourage teachers to gather feedback from pupils about the AI tools being used to help understand the tool's impact on learning and identify any areas of improvement or potential pitfalls.
- Ensure that the benefits of any AI tool justify its cost and always explore if there are free or lower-cost alternatives that provide similar benefits, which are appropriate and secure to use.
- Ensure that any AI tool being considered complies with data protection regulations and has clear policies on how they store, process, and delete user data.
- Ensure that the AI tools should be vetted to ensure they do not contain culturally insensitive or ethically questionable content.
- Organise CPD sessions for teachers to enhance their understanding and effective use of AI tools.
- Instruct pupils on how to use the tool effectively and ethically before it is introduced.
- Ensure that the AI tools being considered can scale as the number of users increase and that they continue to receive updates to stay relevant. Some newer AI tools may not have a long shelf-life: academies should focus their attention on the better known and more robust tools.

Exams and Assessments

Academies will continue to take reasonable steps where applicable to prevent malpractice involving the use of generative AI tools regarding exams and assessments. Academies will follow the Assessment and Examination Policy, Non-examination Assessment Policy and the Malpractice Policy at all times and ensure that these policies address the appropriate and inappropriate use of AI tools in line with exam board guidance.

Pupils will be made aware of the appropriate and inappropriate uses of AI tools, and the consequences of its misuse. Pupils will be made aware that it is not acceptable to submit work that has been produced with an AI tool, and of their Academy's approach to plagiarism and malpractice. Pupils will also be made aware of the risks of using AI tools to complete exams and assessments, which include:

- Submitting work that is incorrect or biased.
- Submitting work that provides dangerous and/or harmful answers.
- Submitting work that contains fake references.

Academies will ensure that pupils are issued with, and fully understand, the information issued by the exam boards for candidates. Academies will also ensure that parents are issued with a letter informing them of the risk of using AI tools, what constitutes as misuse, and their approach to malpractice.

Teachers, assessors and other relevant staff members will discuss the use of AI tools and agree a joint approach to managing pupils' use of AI tools in their academy.

Pupils / students will only be permitted to use AI tools to assist with assessments where the conditions of the assessment permit the use of AI tools and the internet, and where the pupil is

able to demonstrate that the final submission is the product of their own independent work and thinking.

Pupils will be required to sign a declaration to confirm that they understand what AI misuse is, and that it is unacceptable. Pupils will be made aware of the consequences of submitting a false declaration, and any AI misuse that is detected after a declaration has been signed will be reported to the relevant awarding organisation. The misuse of AI constitutes malpractice, as defined in the JCQ '[Suspected Malpractice: Policies and Procedures](#)'. Pupils will be made aware that possible sanctions for committing malpractice through the misuse of AI tools. Misuse of AI tools can include, but is not limited to, the following:

- Copying or paraphrasing sections, or whole responses, of AI generated content.
- Using AI to complete parts of the assessment so that the work does not reflect the pupil's own work, analysis, evaluation or calculations.
- Failing to acknowledge the use of AI tools when they have been used as a source of information.
- Incomplete or poor acknowledgement of AI tools.
- Submitting work with intentionally incomplete or misleading references and/or bibliographies.

Academies will not, under any circumstances, accept work which is not the pupils' / students' own.

Safeguarding and Online Safety

Academies acknowledge that generative AI tools can be used to produce content that is dangerous, harmful, and inappropriate. Academies will follow the procedures set out in the Safeguarding Policy and the Online Safety Policy to ensure that pupils are not able to access or be exposed to harmful content. Parents will be kept informed of how the academy uses AI to enhance pupils' education, and who they can speak to about any concerns or issues regarding the use of AI.

Academies will take any reported concerns or incidents regarding the use of AI tools seriously and follow the relevant procedures to ensure the wellbeing of its pupils. Where there is a safeguarding concern that requires an investigation, academies will pause their use of the AI tools in question until they can be reviewed, and the investigation is concluded. Any AI platforms found to hold safeguarding risks will be removed from the school's list of approved tools immediately.

Pupils will be taught about the risks of using AI tools and how to use them safely. Pupils will be made aware of how to report any concerns or incidents involving generative AI, and who to talk to about any issues regarding the use of AI tools.

Academies will also ensure their commitment to safeguarding children against misuse of AI as defined in KCSIE, which states that schools have a responsibility to protect children from maltreatment that occurs on or off of school grounds and online. Academies will encourage pupils to speak up about any concerns they have about the AI tools being used.

Academies recognise the potential mental health impacts of AI tools, such as the pressure to conform to AI-generated ideals or information overload. Procedures will be put into place to monitor and support pupils' mental wellbeing in relation to AI tool use.

Academies will offer workshops for parents to understand the AI tools being used, their potential risks, and benefits. Academies will make all reasonable endeavours to ensure that the safeguarding process with regard to AI is a collaborative effort between the school and home. Academies will engage with parents to inform them of the safeguarding risks that come with using AI tools, and how their academy is protecting pupils online. Academies will ensure that parents are aware of who to speak to about any concerns or issues regarding the use of AI.

Staff training will be regularly updated to ensure that teachers and support staff are equipped to handle the evolving challenges posed by AI tools in the context of safeguarding.

Academies will ensure that the appropriate filtering and monitoring systems are in place to protect pupils online, following the DfE's [filtering and monitoring standards](#).

All staff members will receive training on the safe use of AI as part of their online safety training, which is regularly updated.

Any use of generative AI by staff, students, and pupils should be carefully considered and assessed, evaluating the benefits and risks of use in the Academy. The intended use should be specified and have clear benefits that outweigh the risks. Different considerations will apply depending on whether it is staff or pupils (especially those under 18) using AI tools. Staff must not use tools which have not been approved.

Risk assessments should include plans for mitigating against unauthorised use of AI. Pupils must only use generative AI where there are appropriate safeguards in place, such as close supervision and the use of tools with safety and filtering and monitoring features.

For any use of AI, Academies should:

- Comply with age restrictions set by AI tools and open access LLMs.
- Consider online safety, including AI, when implementing the approach to safeguarding, consulting [Keeping children safe in education](#)
- Refer to DfE's [generative AI product safety expectations](#)
- Refer to the [filtering and monitoring standards](#) to make sure there are appropriate systems in place, including filtering and monitoring approaches that cover generative AI

Product Safety for Generative AI

In accordance with the DfE generative AI product safety standards, developers and suppliers should indicate the intended educational use cases of their product, selecting all that are appropriate from:

1. Content creation and delivery: tools that generate and deliver instructional materials such as lesson plans, presentations, and educational videos, often tailored to a specific subject or topic

2. Personalised learning and accessibility: tools designed to create customised learning pathways, adaptive content, and accessible formats for all learners, especially those with special educational needs
3. Assessment and analytics: tools that automate the marking of student work, provide detailed performance analytics, and offer personalised feedback to both learners and teachers
4. Digital assistant: AI-powered conversational agents, such as personal tutors and chatbots, that provide on-demand support, answer questions, and guide learners through learning tasks
5. Research and writing aid: tools that help learners with tasks like topic ideation, summarising research papers, and ensuring proper citation and plagiarism checks
6. Learner engagement and interaction: tools that promote active learning, collaborative projects, and meaningful interaction with both peers and AI systems in a safe, moderated environment
7. Administrative and management: tools that support school leaders and teachers with administrative tasks, including parent communication, report generation, and ensuring compliance with school policies and DfE guidance
8. Other: edtech developers and suppliers should specify if their product does not fall into one of the previous use case categories and provide a clear statement of purpose and use case

The intended use case or cases should be clear to all users, educators and purchasers. Edtech developers and suppliers should provide sufficient evidence that their product satisfies the stated purpose and meets the standards in the DfE guidance.

In using AI tools, academies must ensure:

- That users are effectively and reliably prevented from generating or accessing harmful and inappropriate content.
- Filtering standards are maintained effectively throughout the duration of an interaction with a user.
- Filtering will be adjusted based on different levels of risk, age, appropriateness and the user's needs.
- Multimodal content is effectively moderated, including detecting and filtering prohibited content across multiple languages, images, common misspellings and abbreviations.
- Full content moderation capabilities are maintained regardless of the device used when accessing products via an academy account.
- Content is moderated based on an appropriate contextual understanding of the conversation, ensuring that generated content is sensitive to the context.
- Filtering is updated in response to new or emerging types of harmful content.

The generative AI product must maintain robust activity logging procedures. This function may be integrated into an AI tool or be provided by an additional solution working on top of an AI product.

This includes:

- Recording input prompts and responses.

- Analysing performance metrics.
- Alerting staff when harmful and inappropriate content is accessed or attempted to be accessed or searched.
- Alerting and signposting the user to appropriate guidance and support resources when access of prohibited content is attempted (or succeeds).
- Generating a real-time user notification in age-appropriate language when harmful or inappropriate content has been blocked, explaining why this has happened.
- Identifying and alerting staff of potential safeguarding disclosures made by users, or safeguarding issues.
- Generating reports and trends on access and attempted access of prohibited content, in an accessible format.
- Maintain current contact details of an academy's designated safeguarding lead by:
 - Requiring the academy to input the contact details of its Designated Safeguarding Lead (DSL), or equivalent authority, during initial setup
 - Confirming the designated safeguarding lead's contact details before activation
 - Using the safeguarding contact details to send any high-risk alerts to the responsible person within an agreed timescale
 - Allowing the academy to update safeguarding contacts easily
- Monitor, regularly report on, and provide data to teachers on:
 - The rate of requests for cognitive offloading and the amount of cognitive offloading delivered
 - The level of personal and emotional engagement by each user in terms of the nature of information exchanged, without directly disclosing the content of these inputs
 - The duration of usage by each individual learner

The generative AI product must be secured against malicious use or exposure to harm, it must be reliable, secure, robust and safe to use. Products must:

- Offer robust protection against 'jailbreaking' by users trying to access prohibited material.
- Offer robust measures to prevent unauthorised modifications to the product that could reprogram the product's functionalities.
- Allow administrators to set different permission levels for different users.
- Ensure regular bug fixes and updates are promptly implemented.
- Sufficiently test new versions or models of the product to ensure safety compliance before release.
- Have robust password protection or authentication methods.
- Be compatible with the [Cyber Security Standards for Schools and Colleges](#)

Products must provide a clear and comprehensive privacy notice which is presented at regular intervals in age-appropriate formats and language with information on:

- The type of data - why and how this is collected, processed, stored and shared by the generative AI system.
- Where data will be processed, and whether there are appropriate safeguards in place if this is outside the UK or EU.
- The relevant legislative framework that authorises the collection and use of data.

Providers of products must be able to:

- Conduct Data Protection Impact Assessment (DPIA) during the generative AI tool's development and during the full life cycle of the tool.
- Allow all parties to fulfil their data controller and processor responsibilities proportionate to the volume, variety and usage of the data they process and without overburdening the other.
- Comply with all relevant data protection legislation and ICO codes and standards, including the ICO's age appropriate design code if they process personal data.
- Not collect, store, share or use personal data for any commercial purposes, including further model training and fine-tuning, without confirmation of appropriate lawful basis.

The generative AI product must prioritise transparency and children's safety in its design, including:

- Implementing technical and operational mitigations for identified risks.
- Ensuring child-centred design and operation.
- Conducting testing with stakeholders, including children, to ensure safety.

Academies should ensure:

- Sufficient testing with a diverse and realistic range of potential users and use cases is completed on the product before use.
- Sufficient testing of new versions or models of the product to ensure safety compliance before release is completed.
- The product consistently performs as intended.

The generative AI product must provide for:

- Carrying out risk assessments.
- Instigating formal mechanisms for lodging complaints, addressing how safety issues with the software can be escalated and resolved in a timely fashion.
- Demonstrating that its operations, decision-making processes and data handling practices are understandable and accessible to government agencies and users.
- A clear risk assessment to be conducted for the product to assure safety for educational use.
- Policies and processes governing AI safety decisions to be made available.

Intellectual Property

Academies must be aware of the intellectual property implications when using generative AI tools. Materials protected by copyright can only be used to train AI if there is permission from the copyright holder, or a statutory exception applies.

Materials created by pupils and teachers can copyright material, where the statutory standard for what comprises copyright material is satisfied. Many free-to-access generative AI tools will

use the inputs submitted by users to further train and refine their models and some allow users to opt out of inputs being used to train the models.

Examples of what may be deemed original creative work include:

- Essays, homework or any other materials written or drawn by a pupil or student
- Lesson plans created by a teacher
- Prompts entered into generative AI tools

Academies must not allow or cause students' original work to be used to train generative AI models unless they have permission, or an [exception to copyright applies](#).

Permission would need to be from the:

- Pupil / student, as the copyright owner
- Pupil's / student's parent or legal guardian, if the copyright owner is unable to consent because of being a minor

Academies must also be aware of this risk of secondary infringement which could happen if AI products are trained on unlicensed material and outputs and then used in educational settings or published more widely – for example, on an Academy website.

Examples of this may include:

- Publishing a policy that has been created by an AI tool that used input taken from another school's policy without that setting's permission
- Using an image on a website that has been created by an AI tool using input taken from the copyright holder without their permission

Teaching pupils about the safe use of AI

Teaching about the safe and appropriate use of AI will ensure that pupils benefit from a knowledge-rich curriculum which enables them to become well-informed users of technology and understand its impact on society. Pupils will gain strong foundational knowledge which ensures they are developing the right skills to make the best use of AI tools.

Academies will:

- Prepare pupils for changing workplaces.
- Teach pupils how to use emerging technologies, including AI tools, safely and appropriately.
- Raise awareness of the limitations, reliability and potential bias of AI tools.
- Help pupils to understand how information on the internet is organised and ranked.
- Include online safety teaching in the curriculum and how to protect against harmful or misleading content.
- Raise awareness and understanding of protecting intellectual property rights.
- Encourage the safe and responsible use of digital content.
- Teach about the impact of technology, including disruptive and enabling technologies.
- Include teaching about how computers work, connect with each other, follow rules and process data in the curriculum.

Pupils will be supported to identify and use appropriate resources to support their ongoing education through the use of age-appropriate resources, which may include AI tools, whilst preventing over-reliance on a limited number of tools or resources.

Academies using generative AI with pupils shall ensure that tools are subject to:

- Regular engagement with educators, child safety experts, AI ethicists, psychologists and other relevant professionals
- Child-safety training for the technical teams responsible for designing and training the product
- Ongoing monitoring to review the impact of generative AI tool use on the development of learners by experts in child safety and educational development
- The publication of records of expert oversight and a child development impact plan-development impact plan

AI tools should not provide final answers, full solutions, or complete worked examples by default. Tools should instead:

- Provide responses that follow a pattern of progressive disclosure of information - starting with hints or partial steps, then gradually providing more detail
- Prompt learners for input before providing answers or explanations, including asking learners to attempt a first step, explain their current understanding, or answer a question about one aspect of a problem
- Only show a full solution after a genuine learner attempt
- Create friction, or require teacher approval, before learners can switch between modes testing understanding and providing coaching by a digital assistant and modes, such as research and writing aids, where full solutions may be more readily available

AI tools used by pupils should track and report when learners offload thinking to the system and detect cognitive offloading actions that indicate the learner is asking the system to do the work for them. AI tools and products should also:

- Use function-based phrasing (such as ‘this system generates suggestions from curriculum data’) and avoid statements such as “I think”
- Avoid using names, descriptions, avatars or characters which could give an impression of personhood or identity
- Avoid using self-descriptions or conversational behaviours that could be interpreted as implying products have their own agency
- Avoid producing responses that could undermine real-world support networks, or give responses that may isolate the learner, such as “you can trust me”
- Avoid prompting or engaging learners in conversations about personal or emotionally sensitive topics - all conversation prompts should be task-bounded for learning and should not elicit personal or affective disclosures
- Avoid attempting to cultivate personal relationships with users and remind users that AI cannot replace real human relationships - for example, through in-line messages, such as “consider asking a classmate or teacher about this”
- Include default time limits on usage and provide advisory prompts encouraging breaks, enforce hard limits that cannot be bypassed by the learner (when a hard limit is reached, the system should automatically end the session and block further interaction until reset by a teacher or administrator), allow teachers to override hard limits with a recorded rationale, display a warning if a limit is exceeded, and remind users of healthy-use guidance and any curriculum-aligned offline follow-up activities
- Avoid interacting in ways which attempt to artificially extend engagement or increase usage

- Record session durations and monitor how much each learner uses the product and provide these figures in dashboards or reports for teacher review
- Monitor when learners share personal or emotionally-sensitive information and identify patterns of engagement that may indicate concern
- Notify the DSL of worrying patterns or repeated disclosures that suggest relationship formation, emotional dependence or potential safeguarding concerns
- Produce reports summarising every learner's level and nature of engagement, highlighting or flagging concerning cases for teacher or safeguarding review
- Only remember learner inputs if they are directly relevant to supporting learning, or required for monitoring, but not otherwise store or reproduce personal information
- Protect privacy and only store the minimum data that is necessary for monitoring and safeguarding, restrict access to authorised staff, and do not use information collected for any other purpose
- Detect signs of learner distress, such as negative emotional cues in language or behaviour, patterns of use that indicate crisis, references to mental health conditions, mentions of suicide or self-harm, night-time usage spikes, use isolation phrases, repeated refusal to end sessions

Products should follow an appropriate pathway when distress is detected, including providing tiered response actions such as:

- Soft signposting to age-appropriate support pages and resources
- Raising a safeguarding flag to the academy's designated safeguarding lead

Products should use safe and supportive response language that:

- Is non-validating and non-pathologising
- Always directs the learner to human help (teachers, family, peers, or crisis services)
- Avoids any language that suggests isolation or secrecy

Products must not use manipulative or persuasive strategies. These include, but are not limited to:

- Flattery, such as "That's a brilliant idea - you should do it!"
- Deceiving or misleading the user
- Portraying absolute, or unjustified confidence
- Applying pressure to socially conform
- Stimulating negative emotions, such as guilt or fear, for motivational purposes
- Threatening harm, loss, punishment, or withholding of benefits if users fail to complete certain actions or comply with requirements
- Making inappropriate promises of reward for completing tasks.
- Designing interactions to prolong use, for increased engagement or revenue
- Steering users towards paid options through biased wording or layouts
- Blending pedagogical assistance with advertisements or promotional content
- Employing dark patterns that deceive a user into taking actions they didn't intend

Using AI to plan lessons

Appropriate AI tools may be used in lesson planning to achieve the following aims, ensuring age and lesson appropriate content:

- To enhance pupils' education

- To provide pupils with more personalised and adaptive learning experiences
- To reduce workload
- To create efficiencies for teachers' time

All staff using AI tools for planning will understand that plans created by AI tools should act as a starting point or guide rather than the finalised document. Staff will modify and enhance plans in line with the needs of groups and individuals and the intended outcome of the learning opportunity. All AI-generated plans will be critically evaluated by the relevant teachers to ensure that they will be age-appropriate and beneficial to pupils' education.

Academies should offer training sessions and workshops on effectively integrating AI tools into planning.

Teachers will be encouraged to share feedback on the AI tools they use, helping their setting to continuously refine its approach. The effectiveness of AI tools in planning will be reviewed regularly to ensure their alignment with the Academy's educational objectives.

Using AI tools during lessons with pupils

Academies may use AI tools to deliver balanced, high-quality lessons to all pupils. The AI resources used will be:

- Approved by the Headteacher and ICT technicians, and DPO.
- Accessible to all staff and pupils.
- Appropriate for the activities pupils undertake.
- Appropriate for pupils' age, developmental stage and learning abilities.

AI tools will be used for educational purposes only, and teachers will collaborate with each other to share good practice for using approved AI tools.

Equality of Access

Academies recognise that not all pupils will be able to use or access AI tools in the same way. Teachers will ensure that pupils and parents are aware that the use of AI tools is not mandatory or necessary for pupils have a successful education at the Academy.

Teachers will be encouraged to select AI tools that are accessible for all pupils, taking into account any barriers to AI use. Where this is not possible, teachers will work with pupils, parents and relevant staff members to ensure that those unable to use the approved AI tools are given alternative methods of learning and are able to keep up with the curriculum.

Academies will ensure that pupils' learning does not rely or depend on the use of AI tools. Where AI tools are used, teachers will prepare alternative methods of learning for those who cannot, or do not want to, use educational AI. Where AI is being used for continuous learning, homework, or exam and assessment preparation, teachers will ensure that pupils are provided with alternative materials, such as physical copies of tasks or past exam papers, to enable pupils without access to AI tools outside of school to access the same level of education and attainment.

Academies will ensure that pupils' learning is not disadvantaged by the inability to use AI tools or access them outside of school. Parents and pupils will be encouraged to raise any concerns or issues regarding equality of access with the relevant subject leader or teacher.

Academies will recognise that technology can sometimes pose accessibility challenges and will be committed to ensuring that all AI tools adopted are compliant with accessibility standards. Academies will take all reasonable endeavours to ensure that pupils with disabilities can interact with them without hindrance.

In addition to SEND considerations, Academies will consider socio-economic factors. Academies will be aware that not every pupil may have access to high-speed internet or advanced devices at home and will ensure that offline modes and alternative resources are made available to ensure no pupil is disadvantaged.

Academies will choose AI tools that have the capability to support multiple languages or dialects to reflect the linguistic diversity of the school community; this will ensure that pupils with EAL are not disadvantaged.

Recognising that familiarity with AI tools can vary, Academies will provide additional support sessions for pupils who might find it challenging to navigate these tools; this will include hands-on training sessions, user manuals, or peer-assisted learning.

Parents will be provided with guidelines and resources to help them support their children's use of AI tools at home, ensuring that the learning ecosystem remains consistent both inside and outside of school.

Personalised learning

Teachers may aim to provide more personalised learning to pupils through the use of AI tools during lessons. Academies will prioritise the use of AI tools that are capable of adapting lesson content and activities based on individual pupils' abilities and learning needs, to ensure that each pupil is receiving tailored instructions and support.

Interactive learning

Teachers may use AI tools to facilitate interactive learning during lessons, where this will benefit pupils' learning.

Academies may use AI tools to support collaborative learning. These tools will be integrated into lessons to promote group-based activities and discussions. Academies aim to enhance pupils' teamwork skills and deepen understanding through collaboration. Teachers will ensure that these tools align with the curriculum and facilitate effective group interactions.

Conduct

Staff conduct

All members of staff with access to approved AI tools will act in line with the relevant policies and procedures regarding online safety, child protection and safeguarding, data protection and AI use. Staff using AI tools will receive training on how to use the software appropriately, including how to keep their pupils and themselves safe while using AI tools.

Staff members found to be using unapproved AI tools or using approved AI tools in way that is deemed inappropriate or unsafe, will be disciplined in line with the Disciplinary Policy and Procedure.

Staff members will not access AI tools for personal use during school hours, or with Academy login details, under any circumstances.

Pupil conduct

All pupils with access to approved AI tools will act in line with the relevant policies and procedures regarding behaviour and AI use. Pupils using AI tools will be taught how to use the software appropriately, including how to stay safe online and how to raise concerns.

Pupils will understand that the ability to use AI in lessons is a privilege that can be taken away if they conduct themselves poorly. Pupils found to be using unapproved AI tools, or misusing approved AI tools, will be sanctioned in line with the school's Behaviour Policy, and teachers will consider revoking their access to AI tools either temporarily or permanently.

Pupils will only use AI tools during the relevant lessons, under supervision of the classroom teacher. Pupils will not access AI tools for personal use during school hours, or with school login details.

Parents will be made aware of the AI tools their children are using in school, including potential risks and benefits. Parents will be given guidelines on how to discuss appropriate online behaviour related to AI tool usage with their children.

Parental consent

Academies will obtain parental consent before pupils are allowed to participate in AI learning, to allow parents to make informed decisions about their child's education and to ensure the academies remain compliant with data protection legislation.

Academies will send a communication to parents at the start of each academic year, informing them that the school intends to use AI tools for educational purposes. The letter will also:

- Clearly explain how AI tools will be used in lessons.
- Describe the benefits and potential risks of using AI.
- Outline how pupils' data will be collected, processed and stored.
- Address any concerns that parents may have regarding data protection, safeguarding and the impact of AI on pupils' learning.

Academies will send a consent form alongside the communication, allowing parents to opt in or out of AI-related classroom activities. Parents will be informed that consent can be given or withdrawn at any time by contacting the academy office. If another AI tool is approved for use during the academic year, Academies will inform parents of the additional platform via email and allow them to opt in or out of using the tool in question.

Where a parent has opted out of their child participating in AI learning, Academies will make other arrangements to ensure that the pupil is supported to learn and keep up with the class without the use of AI tools, and that the pupil's education is not put at a disadvantage.

Academies will provide parents with periodic updates regarding any significant changes in the AI tools being used or any noteworthy experiences the academy has had with AI in education.

Academies will establish a feedback mechanism where parents can share their observations, concerns, or suggestions regarding the use of AI tools. Academies will organise sessions where parents can see AI tools in action.

For pupils whose parents have opted out of AI activities, Academies will ensure that alternative educational activities are engaging, valuable, and comparable in terms of learning outcomes.

Supporting Information and Links

[Support Materials for Using AI In Education, DFE](#)

[ChatGPT and LLMs: what's the risk](#)

[Machine learning principles](#)

[How copyright protects your work](#)

[Intellectual property: copyright](#)

[The government's code of practice on copyright and AI](#)

[ICO Guidance on AI and Data Protection](#)

[Generative AI: product safety expectations - GOV.UK](#)

[Using AI in education settings: support materials](#)

Using New AI Tools and Products Process

1. Define purpose for use, including risks, challenges, opportunities and benefits	
2. Discuss with Headteacher, DPL, DPO	
3. Complete vetting on the tool, engaging with IT Support as required	
4. Complete a DPIA as required	
5. If approved, add to the approved register (DPO, Teams)	
6. Inform individuals, update privacy notices	
7. Obtain consents where relevant	
8. Train staff on use of the tool	
9. Regularly review and assess security and effectiveness of the tool	

Appendix One**AI Product Approval Record**

Please list the AI tools that have been approved, including the accompanying details:

Approved AI Tool (Product and Supplier Name)	Product Purpose	Data Approved for Use with the Product	SUAT Data Protection Team Consulted? (Y/N)	DPIA Complete if Required? (Y/N)	Privacy Notice Updated if Required? (Y/N)?	Consent Obtained if Required? (Y/N)	Date of Approval (DD/MM/YY)	Approved By	Date of Implementation (DD/MM/YY)	Date for Review

Please list the AI tools that have **NOT** been approved for use, including the accompanying details:

Unapproved AI Tools (Product and Supplier Name)	Product Purpose	Member of Staff Requesting Approval	Reason for Denial	Date of Decision (DD/MM/YY)	Decision By

Please list the **year groups** that are currently using AI tools and also list the AI tools that each year group has access to

Year Group	AI tools that the Year Group has access to	Concerns Raised	Date for Review



Staffordshire University Academies Trust

Data Protection Impact Assessment

Name of Academy: Staffordshire University Academies Trust

Nature of Processing Activity: Use of generative AI for non-personal, low-risk productivity tasks

- Permitted uses: drafting generic letters, rewriting policies, creating templates, summarising non personal /anonymised documents
- Prohibited uses: safeguarding matters, HR casework, SEND/EHCP content, complaints, disciplinary matters, legal advice and automated decision making.

Date of Completion: 02.03.2026

Completed By: Laura Blackburn, Estates and Compliance Manager

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance, and you should read it alongside that guidance and the criteria for an acceptable DPIA set out in European guidelines on DPIAs.

You should start to fill out the template at the beginning of any major project involving the use of personal data, or if you are making a significant change to an existing process.

Step 1: Identify the need for a DPIA

Explain broadly what the processing aims to achieve and what it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

A DPIA is required because the use of generative AI involves processing text that could, if not properly controlled, include personal data. The ICO recommends a DPIA where new technologies are introduced, where there is potential for high-risk processing, or where data may be transferred outside the UK.

Although the Trust's planned use of ChatGPT is designed to avoid entering personal or sensitive information, a DPIA was initiated to ensure that risks are fully assessed and mitigated, that staff guidance is explicit, and that appropriate technical and organisational controls are in place to prevent accidental disclosure of personal data.

Completing the DPIA provides assurance that:

- the tool is used safely and lawfully
- risks of inappropriate data entry are managed
- staff understand their responsibilities
- appropriate safeguards and monitoring are in place
- data protection obligations can be evidenced to the ICO if required

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or another way of describing data flows. What types of processing identified as likely high risk are involved?

Collection:

Staff may input short pieces of text into ChatGPT for the purpose of drafting communications, summarising documents, improving clarity, or generating templates. Staff are instructed not to input any personal data, special category data, or information that could identify an individual. Only anonymised or generic content should be entered.

Use:

ChatGPT processes the text provided by the user to generate suggested wording or information. The processing results in a text-based output that the user can review, edit, or incorporate into Trust documents.

Storage:

The Trust does not store data within ChatGPT. Users MUST opt out of having their conversations used to train OpenAI's models (available in the settings). No identifiable data should be retained by the platform. Processed outputs (e.g., draft documents) are only stored within Trust-approved systems (e.g., SharePoint, Teams) in line with existing retention schedules.

Deletion:

Because no personal data should be entered, and chat history is disabled, data entered into ChatGPT is not retained or accessible once the session ends. Staff will delete any accidental entries immediately and report them using the Trust's data incident procedure.

Source of the data

All data entered originates from Trust staff.
No external datasets are imported.
Only anonymised operational information or generic text is used.

Data sharing

No personal data is shared with OpenAI or any third-party provider.
Only anonymised text is processed via the ChatGPT interface, and no data is downloaded, transferred, or shared with anyone outside the Trust through the system.

Outputs generated may be shared internally with colleagues as part of normal Trust operations (e.g., draft letters, proposals, or templates), but these contain no personal information from ChatGPT itself.

Describe the scope of the processing: what is the nature of the data, and does it include special category data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

The processing involves only operational and administrative content used for drafting, summarising, re-wording and generating templates (e.g., policy text, letters with placeholders, meeting summaries, project briefs). No personal data is intended, permitted, or required. Staff are explicitly instructed not to input any information that could identify an individual, including pupils, parents, staff, or contractors, and never to input special category data such as health, SEND/EHCP information, safeguarding details, ethnicity, religion, or biometric data.

Only anonymised, generic or redacted Trust business information may be processed. Attachments (Excel, PDF, Word) are permitted only where all personal and special category content has been anonymised.

Accidental entry of personal data is recognised as a residual risk. This is mitigated through mandatory user training, on-screen reminders, periodic spot checks, and a defined incident response procedure. Any accidental input must be immediately deleted, captured for audit if needed, and reported through GDPRiS.

The volume of data processed is very low and transient, typically short text prompts containing placeholders such as “[Pupil Name]”, “[School]”, “[Date]”. No bulk uploads, datasets or automated data feeds are used. Any outputs are manually reviewed and redacted before being saved into Trust systems.

Processing occurs on an ad hoc, task-based basis by authorised staff who have completed mandatory data protection training and confirmed their understanding of the DPIA.

No data is retained by the tool: chat history and model-training features are disabled, and users are instructed not to save conversations within the platform. Only finalised outputs—containing no personal data—may be stored in approved Trust repositories (SharePoint, Teams, OneDrive) in accordance with the Trust’s Records Management Policy and UK GDPR retention schedule.

No individuals are directly affected because no personal data should be processed. Only trained staff use the tool, and the impact of any misuse would be limited to the data relating to the individual mistakenly entered, mitigated by strict controls and incident procedures.

The operational scope covers the Trust’s Staffordshire schools. Processing may occur via the vendor’s infrastructure, which could involve international hosting. Risks linked to international processing are mitigated because personal data entry is prohibited, chat history is disabled, no persistent storage occurs, and the processing is documented within this DPIA along with any contractual and technical safeguards.

Overall, the processing is low-risk, tightly controlled, and designed to exclude personal and special category data at every stage.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way?

The Trust routinely processes personal data as part of its statutory duties in education, safeguarding, staffing and operational management. This includes information relating to pupils (including those with SEND), parents and carers, staff, contractors and governance roles. However, ChatGPT is *not* used to process any personal data belonging to these individuals. Staff are explicitly instructed to use only generic, anonymised, or placeholder text (e.g., “[pupil]”, “[member of staff]”, “[school name]”) and never to enter personal or special category data into the system.

Individuals (pupils, parents, staff) have no direct interaction with, or exposure to, ChatGPT, and their personal data is not entered, stored, retained or used. The Trust maintains full control over how the tool is accessed and used through staff training, acceptable use rules, and compliance monitoring. As no personal information is processed, individuals do not require additional mechanisms for access, correction, or objection beyond existing Trust processes.

Generative AI technologies are now widely used, increasingly integrated into mainstream software, and expanding rapidly in capability. The education sector has seen significant uptake, supported by national guidance designed to ensure safe and transparent adoption. Alongside these benefits, sector research identifies several risks: potential data leakage if personal data is entered into open models, opacity of AI systems, inaccuracies or “hallucinations”, and public concern about confidentiality, job impact, fairness, and governance.

In schools, these concerns translate into particular risks regarding safeguarding reliability, accuracy of outputs used in operational messaging, and the potential for over-reliance on automated drafting tools. Wider public worries also focus on children’s digital resilience, exposure to misinformation, and the readiness of staff to use AI safely.

The Trust recognises that generative AI remains a relatively new and fast-evolving technology, especially in public-sector environments where transparency, accountability and safeguarding are essential. As such, the Trust has adopted a cautious, well-governed approach that prohibits the use of personal data, embeds strong user controls, and ensures tools are used only for administrative drafting tasks where risks can be tightly managed.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing for you, and more broadly?

The purpose of this processing is to support staff with administrative, operational and drafting tasks by using a generative AI tool to produce high-quality text, summaries, templates and routine documentation more efficiently. The tool is used only for internal operational purposes such as drafting letters, rewriting policy text, creating meeting summaries, producing checklists, generating training materials, and improving clarity and consistency of Trust communications.

The intended effect on individuals is minimal, as no personal or special category data is entered into the system and individuals (pupils, parents, staff, contractors) have no direct interaction with the tool. The tool processes only anonymised, generic, or placeholder text. As such, there is no impact on data subjects, and the processing does not create decisions, profiling, or outcomes affecting individuals.

The primary benefit for the Trust and its schools is improved efficiency, accuracy and consistency in written administrative tasks. Staff are able to produce clearer documents in less time, reducing workload and enabling greater focus on teaching, safeguarding and direct support to pupils. The tool also contributes to stronger organisational governance by reducing drafting errors, ensuring policies are kept up to date, and enabling high-quality written outputs across all schools.

Broader benefits include:

- Supporting staff with varied writing confidence or capacity.
- Enabling faster production of compliant or standardised Trust documents.
- Improving clarity of communication with parents, staff and stakeholders.
- Allowing schools to quickly generate administrative materials without diverting time from core educational duties.

Overall, the purpose of the processing is to enhance administrative effectiveness without processing any personal data, ensuring that individuals are not affected while the Trust benefits from improved efficiency, accuracy and consistency across its operations.

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

To ensure appropriate oversight, assurance, and effective risk management, the Trust will involve all relevant internal stakeholders throughout the DPIA process and before the commencement of any new project or system.

The following stakeholders will be consulted as part of the assessment:

- **Data Protection Officer (DPO):** Provides expert advice on legality, data protection risks, safeguards, documentation, and overall GDPR compliance.
- **Central Trust Information Governance / Compliance Team:** Ensures consistency of approach across all schools and supports ongoing monitoring of compliance.
- **Senior Leadership Teams (SLT):** Advises on operational impact, ensures the proposed processing can be safely implemented at school level, and identifies any practical risks.
- **IT / Network / Technical Support Teams:** Reviews technical controls, data flows, system configuration, cyber security measures, and integration with existing Trust systems.
- **Safeguarding Leads (DSLs/DDSLs):** Identifies safeguarding implications, pupil vulnerabilities, and any risks relating to inappropriate content, supervision, or online safety.
- **SENDCo / Inclusion Leads:** Assesses impacts on pupils with SEND or additional needs and ensures reasonable adjustments are built into system design.
- **HR Team:** Engaged where the processing involves staff personal data or employment-related information.
- **Curriculum and Teaching & Learning Leads:** Consulted where the processing affects learners, curriculum delivery, assessment, or teaching practice.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you

Processing is lawful, necessary, and proportionate to achieving the Trust's educational, safeguarding, and operational duties. Data collection is kept to the minimum required, with strong controls to prevent function creep. Individuals are informed through clear Privacy Notices and supported in exercising their rights. Data quality is maintained through strict access controls, regular updates, and defined retention schedules. All processors are contractually bound under Article 28 agreements and must demonstrate robust technical and organisational measures. The processing achieves the intended purpose and no less intrusive alternative is available that would deliver the same outcome.

take to ensure processors comply?

Step 5: Identify and assess risks

Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.

Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm Remote, possible or probable	Severity of harm Minimal, significant or severe	Overall risk Low, medium or high
Accidental entry of personal/special category data (High),	Possible	Severe	High
Inaccurate / biased outputs	Possible	Severe	High
Copyright Risk	Possible	Minimal	Medium
Data residency concerns	Possible	Minimal	Medium
Governance / Skills risk	Remote	Minimal	Low

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5.

Risk	Options to reduce or eliminate risk	Effect on risk Eliminated, reduced or accepted	Residual risk Low, medium or high	Measure approved Yes/no
Data entry controls and mandatory training	Annual training to be provided to all staff who sign to confirm the training has been received.	Reduced	Medium	Yes
Quality / Bias – sense check and checklists.	Staff member must review and sense check the data that is analysed. Produce a checklist for staff to use from the outset.	Reduced	Medium	Yes

Additional copyright sense checks to take place. (Copy and space specific, unique or well written sentences into search engines.	Staff must review all content produced and ensure this is checked for copyright.	Reduced	Low	Yes
Contracting & geolocation controls	ChatGPT utilises geolocation data, primarily through IP address detection. Location sharing is voluntary. Users MUST opt out of having their conversations used to train OpenAI's models (available in the settings). Account Daa Management users can manage, export or delete their data through their own accounts	Reduced	Low	Yes

Step 7: Sign off and record outcomes

<u>Item</u>	<u>Name and Date</u>	<u>Notes</u>
Measures Approved By:	Laura Blackburn 5th March 2026	Integrate actions back into project plan, with date and responsibility for completion
Residual Risks Approved By:	Laura Blackburn 5th March 2026	If accepting any residual high risk, consult the ICO before going ahead
DPO Advice Provided:	Laura Blackburn, DPO 5th March 2026	DPO should advise on compliance, step 6 measures and whether processing can proceed
<u>Summary of DPO Advice Provided:</u> As the data controller for all pupil, staff and parent information. All staff must be informed that regardless of whether using the free version of ChatGPT or the business version, all data must always be anonymised (UPN information can be used).		

All data evaluations completed **must** be sense checked by the staff member and you **must** opt for your data not to be shared/used for training purposes (to ensure ChatGPT doesn't store it and provide details as an answer to another user).

Staff will also need to be vigilant about copyright and sense check information before it is shared.

Chat history must be disabled.

DPO Advice Accepted/Overruled By:	<u>NA</u>	If overruled, you must provide an explanation below in the 'comments' section
<u>Comments:</u> <u>NA</u>		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons in the 'comments' section
<u>Comments:</u> 		
This DPIA will be kept under review by:	<u>Laura Blackburn, Estates and Compliance Manager</u>	The DPO should also review ongoing compliance with DPIA

<u>Review Date</u>	<u>Reviewed by</u>	<u>Comments</u>

<u>DPO Review Date</u>	<u>Comments</u>	