David Ross Education Trust

Broadening Horizons

Acceptable Use Policy – Staff Artificial Intelligence

Document Management Information

Applicable to:	All staff in all Academies and Central Support Services including individuals employed by the Trust, contractors and agency staff. All Members and Trustees.
Dissemination:	The policy will be available to staff via the Trust's Policy Centre
Implementation:	Applicable to all DRET academies
Training:	On request and mandatory awareness training
Review Frequency:	The policy will be reviewed every three years. The policy will also be reviewed earlier if needed in the light of new evidence/legislation/guidance
Policy Author:	George Selby, Head of Data Protection and Compliance
Executive Policy Owner:	Maria Maltby, Director of Governance
Approval by:	Executive Team
Approval Date:	19 October 2026
Next Review Due:	October 2029

Revision History

Document version	Description of Revision	Date Approved
v.1	Original draft approved by Executive Team	9 December 2025
v.1.1	Tightening of wording. Inclusion of human oversight	19 October 2026

Contents

Contents 3
1. Introduction 4
2. Purpose 4
3. Policy Scope 4
4. Policy Statement 5
5. Data Protection Implications using AI 6
6. Technical Robustness and Safety 6
7. Information Availability 7
8. Prohibited uses of AI 7
9. Implementation of New AI Tools 8
10. Reporting and Consequences of Non-Compliance 8
11. Policy Status 8
12. Related Policies 8

1. Introduction

1.1 The David Ross Education Trust recognises that Artificial Intelligence (AI) technology is already widely used in both commercial and everyday applications, and its influence is anticipated to grow exponentially, impacting almost all industries and job sectors including education.

1.2 Whilst AI was typically used by specialists to complete a specific task, it has become a widely used tool in a short period of time that is more accessible in a range of disciplines. In particular, the growth in Generative AI has led to new opportunities to use AI tools. Generative AI is a rapidly evolving and increasingly freely available technology, which can generate new writing, audio, codes, images and video simulations. Whilst this offers opportunities for staff in enhancing efficiency, decision-making and service delivery, it also increases risk.

1.3 This policy establishes the expectations for the responsible and effective use of all AI in our Trust by users.

1.4 By embracing AI technology, we aim to:

- Support staff to manage their workload more efficiently and effectively.
- Prepare students for a future in which AI technology will be an integral part.
- Use AI to promote fairness in education by supporting the work to bridge learning and accessibility disparities; and
- Ensure value for money in our services by using appropriate AI tools to improve efficiency, reduce duplication and support better use of staff time.

1.5 The Trust needs to ensure that the use of AI is organised and controlled in a manner which will be beneficial to the safety of individuals and groups of people and is in alignment with applicable laws and regulations.

1.6 The Trust recognises that this is a rapidly developing area and like many other organisations, will need to continually review and adapt practice to changes in technology. Our Digital Strategy includes an acknowledgement and commitment to exploring the opportunities offered by AI technology. This policy will be regularly reviewed to ensure that it remains relevant and applicable in practice. The Trust recognises that it is important to provide early appropriate guidance and advice to employees, to encourage users to be transparent about the use of AI, and to support a culture of responsible AI use as these rapid changes take place.

2. Purpose

2.1 The purpose of this policy is to ensure users are aware of the controls and methods in place to manage the use of AI. Users are expected to comply with the policy to ensure that AI tools are used appropriately. There are a number of other relevant policies which this policy links with, including but not limited to the Data Protection Policy and Acceptable Use Policy. This is supplementary to existing policies and should be read in conjunction with them.

2.2 The policy also aims to ensure the ethical, safe, and effective use of AI and data tools in our educational environment. It aims to provide clear guidelines for all users on the appropriate use of AI and data technologies in our Trust.

3. Policy Scope

3.1 This policy applies to the use and configuration of all AI tools that have either been provided by the Trust as part of general IT tools available to staff and other AI tools, which may be available for free

or on a subscription basis and directly accessed by users via the internet, or procured by the Trust for a specific use.

3.2 These rules apply when using both Trust-owned devices and any personal devices which may be used for Trust business.

3.3 This policy applies to all employees, agency staff, contractors, volunteers, apprentices, and student/work experience placements who have access to these tools, described as "users" within this document. All users are responsible for reading and understanding this policy before using any AI technology.

4. Policy Statement

4.1 This policy applies to all AI and data technologies used in the Trust, whether for teaching, learning, administration, or other Trust-related activities. This includes but is not limited to, AI systems used for assessing work, personalised learning platforms, data analysis tools, and any other AI or data technologies implemented in the Trust. It also applies to detecting and preventing misuse of AI-generated content, particularly regarding identity fraud, misinformation, and impersonation risks.

4.2 Examples of business tasks that users may use AI for include suggesting drafting improvements to documents, call transcription, summarising large or specialist documents, translation, drafting communications, content creation and reviewing materials for accessibility.

4.3 Examples of teaching tasks that users may use AI for include lesson planning, marking, adapting materials and plans to ensure they are accessible to all students, timetabling, monitoring IT and online activity for safeguarding purposes and attainment tracking.

4.4 Users may explore and use approved AI-based tools and technologies to support their work, provided they follow the Trust's IT, data protection, safeguarding and online safety policies. AI must support, not replace, professional judgement. Users remain responsible for checking the accuracy, appropriateness, fairness and tone of any AI-generated output before it is relied on, shared or published.

4.5 A list of approved and prohibited AI tools will be maintained by the IT Director, in consultation with the Data Protection Officer and relevant Executive Leads, and will be made available to staff through the Trust's usual policy and IT guidance channels. It will be reviewed at least annually, and sooner where there are significant changes in technology, legislation, guidance or risk.

4.6 Decisions to permit, restrict or remove AI tools, whether Trust-wide or for a specific purpose, must follow the IT Change Management process and must be supported by an appropriate Data Protection Impact Assessment where personal data may be processed. No AI tool should be procured, implemented or promoted for Trust use until the relevant approval process has been completed.

4.7 The Trust is committed to leveraging the benefits of AI and data technologies to enhance teaching and learning while upholding our ethical responsibilities. We believe in the potential of these technologies to support personalised learning, improve educational outcomes, and streamline administrative processes. However, we also recognise the importance of using these technologies in a manner that respects privacy, promotes fairness, and prevents discrimination. All users of generative AI will comply with relevant laws, regulations, policies, and guidelines, including but not limited to Keeping Children Safe in Education (KCSIE), UK GDPR, Equality Act 2010, intellectual property and copyright laws, exam board guidelines, and data protection standards. We will prioritise safeguarding our students (as outlined in our Trust Safeguarding and Child Protection Policy) and their online safety, and we will not knowingly use any AI technology that puts them at greater risk. Staff will not provide intellectual property, including pupils' work, to train generative AI

models without appropriate written consent or lawful exemptions in place.

4.8 Users will receive appropriate training and support to integrate AI into their work safely and effectively, including professional development focused on approved AI tools, data protection, safeguarding, reliability and appropriate use. Training and support will be considered through personal development reviews and appraisals, or on an as-needed basis. Users are responsible for identifying any training needs and raising these with their line manager, with support from the Trust's IT team where appropriate.

4.9 The current list of approved and prohibited AI tools will be maintained by the IT Department and published through the Trust's usual staff communication and policy channels.

5. Data Protection Implications using AI

5.1 Users must treat data protection as a key consideration when using AI. Information entered into some AI tools may not remain private or secure and may be used by suppliers to improve, train or develop their systems. Users must not enter personal data, special category data, safeguarding information, staff records, pupil records, parent/carer information, confidential business information or intellectual property into any AI tool unless the tool has been approved for that specific use and the user is clear that it is lawful and appropriate to do so.

5.2 Users who wish to utilise new AI tools or new AI functionality within existing tools must follow the Data Protection Policy and Data Protection Impact Assessment Procedure. Users should be aware that it is not always easy to recognise when AI tools are processing personal data and they should not presume that no processing is taking place. The Trust's Data Protection Officer must be consulted in the first instance.

5.3 Where AI use is appropriate, users must minimise the information shared. Personal information should be anonymised wherever possible before being uploaded. Staff must not upload identifiable pupil, parent, carer or staff information, including SEND information, safeguarding records, behaviour records, health information, assessment data or HR information.

5.4 Unless a tool is listed as approved, or specific written approval has been given, staff must not use it for Trust business. Use of non-approved AI tools for Trust work may be treated as a breach of this policy and may also constitute a data protection, cyber security, safeguarding or confidentiality incident.

5.5 Where users are unsure whether information may be entered into an AI tool, they must seek advice from their line manager, the IT team or the Data Protection Officer before using the tool.

6. Technical Robustness and Safety

6.1 The Trust is committed to using technically robust and safe AI and data technologies. Reliability and safety of these technologies is crucial for their effective and ethical use in our educational environment.

6.2 The Trust's IT Department has implemented several measures to ensure the technical robustness and safety of the AI systems in use in the Trust:

- **Security Measures:** Sufficient security to protect against data breaches is in place which includes physical and digital security measures to protect data from unauthorised access, use, disclosure, alteration, or destruction.

- **Monitoring and Testing:** The IT Department has a process to monitor and test whether the AI system is meeting the goals, purposes, and intended applications. This includes regular reviews of

AI systems' performance and outcomes and audits of data collection, use, and protection practices.

- **Oversight Mechanisms:** The IT Department has appropriate oversight mechanisms for data collection, storage, processing, minimisation, and use. This includes procedures for responding to any technical issues or incidents in a timely and effective manner.

7. Information Availability

7.1 The Trust will make appropriate information available to reassure pupils, parents, carers and other stakeholders about the technical robustness, safety and responsible use of AI systems. This includes being transparent about how approved AI technologies are used, how decisions are made, and how data is collected, processed and protected.

8. Ethical use of AI

8.1 The use of AI systems, in particular Generative AI, will be carried out with caution and an awareness of their limitations. Users should be mindful of the following considerations:

- **Bias** - data and information generated by AI will reflect any inherent biases in the data set accessed to produce it. This could include content which may be discriminatory based on factors such as race, gender, or socioeconomic background. Users must ensure they follow the requirements of the Equality Act 2010.
- **Accuracy** - information may be inaccurate when generated so any content should be fact-checked. Tools may provide highly plausible and coherent results but may still contain errors.
- **Human oversight** - AI outputs must be reviewed by a suitably knowledgeable human before they are relied on, shared or published. Users must not use AI to make final decisions about pupils, parents, carers, staff or other individuals without appropriate human review and lawful decision-making processes. The user remains accountable for any content, communication, recommendation or decision that incorporates AI-generated output.
- **Transparency** - Where AI has made a substantial contribution to published content, users should consider whether transparency regarding its use is appropriate.
- **Currency** – some AI models only collate data prior to a certain date so content generated may not reflect the most recent information.
- **Environmental issues** - use of AI requires energy to run. Therefore, it should only be used when relevant, appropriate and proportionate, where it is the most suitable and sustainable option.
- **Reputational** - trust in our Trust systems and relationships with stakeholders may be harmed if we do not demonstrate our commitment to ensuring they are not harmed by our use of AI.

9. Prohibited uses of AI

9.1 The following uses are prohibited at the Trust:

- AI systems designed to deceive, coerce or influence human behaviour in harmful ways.
- AI tools that prey on an individual's vulnerabilities, such as age, disability, or socio-economic status.
- Emotion recognition within the workplace or educational settings.

- AI systems that use AI for 'social scoring' where scores are assigned to individuals based on their behaviour, affecting access to services, employment or other opportunities.
- Biometric categorisation based on sensitive biometric attributes such as race.
- Real-time biometric identification in publicly accessible spaces for law enforcement purposes.
- AI used to predict criminal offences solely based on profiling or assessing personality traits.
- Uploading confidential or identifiable pupil, parent, carer, staff, governor, trustee or Trust information into any non-approved AI tool.
- Using AI to make final decisions about admissions, exclusions, suspensions, assessment outcomes, SEND provision, safeguarding, complaints, recruitment, performance management or disciplinary matters.
- Creating or distributing misleading, harmful or unauthorised AI-generated images, audio, video, deepfakes or impersonations of pupils, staff, parents, carers or other individuals.
- Using AI-generated content without checking accuracy, suitability, copyright position, source reliability and potential bias.

10. Implementation of New AI Tools

10.1 Staff who wish to use a new AI tool, or new AI functionality within an existing tool, must not begin using it for Trust business until approval has been obtained. Requests should be submitted through the Trust's IT Change Management process and should include the intended purpose, users, supplier, data involved, expected benefits, risks and any proposed use with pupils.

10.2 The IT Director, in consultation with the Data Protection Officer and relevant Executive Leads, will consider cyber security, data protection, safeguarding, equality, reliability, procurement, contractual and value-for-money implications. Executive approval must be obtained before any new AI tool is procured, implemented or made available for wider Trust use.

10.3 Approved tools will be added to the list maintained by the Director of IT and communicated to staff as appropriate. Where a tool is rejected, restricted or withdrawn, staff must comply with the decision and must not seek to bypass Trust controls.

11. Reporting and Consequences of Non-Compliance

11.1 Users must promptly report any suspected misuse of AI, inappropriate output, data protection concern, cyber security concern, safeguarding concern or accidental disclosure of information through the Trust's usual reporting routes. Non-compliance with this policy may lead to disciplinary action and may also require reporting under data protection, safeguarding or other relevant procedures.

12. Policy Status

12.1 This policy does not form part of any employee's contract of employment.

13. Related Policies

13.1 This policy is related to the following other Trust policies:

- Data Protection Policy

- Safeguarding and Child Protection Policy
- Online Safety Policy
- Acceptable Use Policy
- IT Change Management Procedure
- Data Protection Impact Assessment Procedure