



# Use of Artificial Intelligence (AI) Policy

## Version 1

<b>Name and Title of Author</b>	Trust IT Manager
<b>Name of Responsible Board/Committee</b>	FAR Committee
<b>Target Audience</b>	All Stakeholders
<b>Date Policy Agreed</b>	March 2026
<b>Review Date</b>	March 2027

## Contents

<b>1 Aims and scope.....</b>	<b>3</b>
<b>2 Roles and responsibilities .....</b>	<b>4</b>
<b>3. Definitions.....</b>	<b>6</b>
<b>4. Use of AI by staff across the trust, trustees and local governors .....</b>	<b>9</b>
<b>5. Educating students/pupils about Artificial Intelligence.....</b>	<b>10</b>
<b>6. Use of AI by Students/Pupils .....</b>	<b>11</b>
<b>7. Formal assessments.....</b>	<b>12</b>
<b>8. Staff training .....</b>	<b>13</b>
<b>9. Referral to our child protection and safeguarding policy.....</b>	<b>13</b>
<b>10. Breach of this policy.....</b>	<b>14</b>
<b>11. Monitoring and transparency .....</b>	<b>15</b>
<b>12. Links with other policies .....</b>	<b>15</b>

## 1 Aims and scope

The Brighter Futures Learning Partnership Trust recognises the significant potential of artificial intelligence (AI), including generative AI, to support and enhance educational practice. Appropriately implemented, AI technologies can contribute to improving administrative and operational systems, enhancing teaching and learning, enabling more personalised educational experiences, and support innovation across the Trust.

The Trust also acknowledges that the use of AI presents a range of risks, including those relating to data protection, intellectual property, ethical considerations, safeguarding, and compliance with statutory and regulatory requirements.

The purpose of this policy is therefore to provide a clear framework to ensure the ethical, safe and responsible use of AI technologies across the Trust.

This policy applies to all Trust staff, trustees, local governors and students/pupils, and covers the use of AI tools, including (but not limited to) generative AI platforms such as Microsoft Copilot and Google Gemini.

The Trust is committed to ensuring that any use of AI:

- Supports staff across the trust to explore AI solutions to improve efficiency and reduce workload
- Supports high quality education and student/pupil outcomes
- Prepares staff trustees, local governors and students/pupils for a future in which AI technology will be an integral part
- Promotes equity in education by using AI to address learning gaps and provide personalised support
- Ensures that AI technologies are used ethically and responsibly by all staff across the trust, trustees, local governors and students/pupils
- Protect the privacy and personal data of all staff across the trust, trustees, local governors and students/pupils in compliance with the UK GDPR
- Complies with legal, regulatory and ethical standards
- Maintains clear human oversight and professional judgement

### 1.2 Legislation

This policy reflects good practice guidelines / recommendations in the following publications:

- AI regulation white paper, published by the Department for Science, Innovation and Technology, and the Office for Artificial Intelligence
- Generative artificial intelligence (AI) and data protection in schools, published by the Department for Education (DfE)

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)

## 2 Roles and responsibilities

### 2.1 Trust-level AI lead

Our generative AI trust Lead is the Trust ICT Manager with certain duties delegated to the Assistant Trust ICT Manager. They are responsible for the strategic oversight of AI use across the Trust ensuring risks are identified and monitored and mitigated. They will ensure schools provide adequate training and guidance to support leaders and staff. They will provide advice and guidance in relation to AI tools used across the Trust. They will ensure technical security, data protection and system compatibility. They will monitor compliance with this policy and keep the Trust informed of developments in AI, regulation and best practice.

### 2.2 Board of Trustees

The Board of Trustees is responsible for providing strategic oversight and direction of the Trust's use of artificial intelligence. The Board will ensure that appropriate governance is in place with effective oversight and assurance being in place.

The Board will also maintain oversight of the use AI and the introduction of new AI tools, receiving regular updates and taking into account advice from the Trust ICT Manager, the CEO and the outcomes of relevant data protection impact assessments.

When using generative artificial intelligence tools themselves, trustees are required to act in accordance with this policy and wider Trust information governance arrangements. Trustees will ensure that any artificial intelligence tools used are appropriate for the intended purpose and are used in accordance with this policy and the Trust's AI Tool Risk & Compliance Checklist. Trustees must consider data protection, safeguarding, security and ethical implications prior to use and liaise with the Trust ICT Manager for guidance and support where required. No personal, sensitive or identifiable information must be entered into AI tools. Trustees will clearly acknowledge the use of generative AI within their work and will critically evaluate and verify all AI-generated outputs to ensure accuracy, reliability and appropriateness.

### 2.3 Chief Executive Officer

The CEO is responsible for ensuring the effective implementation of this policy across the Trust and appoint a Trust AI Lead with sufficient expertise. They will ensure that AI use aligns with the Trust's vision and values. They will report to the Trust Board on significant developments, risks or incidents related to the use of AI.

### 2.4 Headteachers and Trust/School Leaders and LGBs

Local governing Boards and School leaders are responsible for the day-to-day leadership and management of the use of artificial intelligence within their school. They will ensure that AI is used in a manner that is consistent with this policy and the Trust's wider strategic approach to AI. They will ensure that staff understand acceptable use and receive

appropriate training. Governors will seek assurance that safeguarding and data protection requirements are met.

School leaders will work closely with the Trust AI Lead to ensure that the use of artificial intelligence complies with data protection legislation and relevant Trust information governance requirements. They will also liaise with the Designated Safeguarding Lead to ensure that the use of AI is aligned with the requirements of *Keeping Children Safe in Education* and the school's child protection and safeguarding policies.

Trust and School leaders will ensure that the guidance set out within this policy is understood and followed by all staff. They will ensure that staff receive appropriate training and support to enable the effective, safe and ethical use of artificial intelligence, and that students/pupils are taught about the effective use of AI, including an understanding of potential risks and limitations.

### **2.5 Trust Data Protection Officer (DPO)/Operation Director**

The Trust-level data protection officer (DPO) is an independent, external appointment. Day to day liaison is managed through the Trust Operations Director and the Trust IT Manager who act as the Trust's designated points of contact, The responsibilities of the DPO include advising the Trust Board, the CEO and senior leaders on data protection obligations arising from the use of AI. They provide, advice and scrutiny in relation to data protection legislation in relation to the use of AI across the Trust and advise on the lawful basis for processing personal data, including special data relating to children. They support the investigation and management of data breaches or incidents involving AI.

### **2.6 Designated Safeguarding Leads (DSLs)**

Designated Safeguarding Leads are responsible for monitoring and advising on the Trust's compliance with safeguarding requirements in relation to the use of artificial intelligence. This includes maintaining awareness of new and emerging safeguarding risks associated with AI technologies and their potential impact on children and young people.

Designated Safeguarding Leads will ensure that staff receive appropriate guidance and training on safeguarding risks linked to the use of artificial intelligence, including through updates to safeguarding training and briefings where necessary. They will respond to any safeguarding concerns or incidents arising from the use of AI in accordance with *Keeping Children Safe in Education* and the school's child protection and safeguarding policy.

Designated Safeguarding Leads will also maintain an understanding of the filtering and monitoring systems and processes in place on school devices and networks, ensuring that these systems are appropriately aligned to safeguard students/pupils when accessing digital and AI-enabled technologies.

### **2.7 All Staff**

In line with the Trust's commitment to reducing staff workload while improving outcomes for students/pupils, staff are encouraged to explore appropriate opportunities to support these aims through the use of appropriate artificial intelligence tools. Any use of AI must be in accordance with the requirements and guidance set out within this policy.

When using generative AI tools, staff must take appropriate steps to protect data and ensure compliance with Trust policies and statutory requirements. Staff must ensure that any

artificial intelligence tools used are appropriate for the intended purpose and are used in accordance with this policy and the Trust's AI Tool Risk & Compliance Checklist. Prior to using a new AI platform, staff must consider data protection, safeguarding, security and ethical implications and seek advice from their line manager, the Trust ICT Manager, Assistant Trust ICT Manager or the Designated Safeguarding Lead, as appropriate.

Staff must ensure that no personal, sensitive, proprietary or identifiable information relating to the Trust, schools, staff, students/pupils or families is entered into AI tools. This includes, but is not limited to, financial information, images, intellectual property, commercial materials or details relating to events, visits or locations that could identify an individual, school or the Trust. Generative AI tools must not be used to address emotionally or socially complex matters, including medical, wellbeing or safeguarding-related concerns.

All AI-generated outputs must be critically evaluated and fact-checked to ensure accuracy, reliability and appropriateness. Where AI has been used to support work, this must be clearly acknowledged, and staff must remain accountable for the final content. AI must not be used to generate official Trust, school, pupil or parent-facing communications without appropriate review and approval by a member of the senior leadership team or relevant line manager, including at central Trust level.

Staff must exercise due diligence to ensure that AI-generated content does not infringe third-party rights, including branding, copyrighted materials or academic outputs. The Trust will not accept responsibility for any inappropriate or infringing use. Artificial intelligence must not be used to make decisions with legal, safeguarding, disciplinary, employment or significant educational implications. All such decisions must be made by appropriately authorised staff, exercising professional judgement, and will not be determined solely by AI systems.

### 3. Definitions

For the purposes of this policy, **Artificial Intelligence (AI)** refers to technologies or systems that use algorithms or models to perform tasks that typically require human intelligence. This includes, but is not limited to:

- **Generative AI:** Tools that create new content (text, images, audio, or video) based on prompts, such as ChatGPT, Microsoft Copilot, or Google Gemini.
- **Machine Learning (ML):** Systems that learn from data to improve performance over time, such as predictive analytics or adaptive learning platforms.
- **Natural Language Processing (NLP):** Tools that interpret or generate human language, including chatbots and automated translation.
- **Computer Vision:** Systems that analyse or generate images or video.

#### **Excluded from this definition:**

- Simple automation or rule-based systems (e.g., mail merge, macros) that do not involve learning or autonomous decision-making.
- Standard software features that do not adapt or generate content independently.

- **Recommendation Engines:** Tools that suggest actions, resources, or content based on patterns in data.

### 3.1 Regulatory Principles

As a trust, we follow the 5 principles set out in the [AI regulation white paper](#).

REGULATORY PRINCIPLE	WE WILL ...
Safety, security and robustness	<ul style="list-style-type: none"> <li>• Ensure that AI solutions are secure and safe for users and protect users' data</li> <li>• Ensure we can identify and rectify bias or error</li> <li>• Anticipate threats such as hacking</li> </ul>
Appropriate transparency and explainability	<ul style="list-style-type: none"> <li>• Be transparent about our use of AI, and make sure we understand the suggestions it makes</li> </ul>
Fairness	<ul style="list-style-type: none"> <li>• Only use AI solutions that are ethically appropriate, equitable and free from prejudice – in particular, we will fully consider any bias relating to small groups and protected characteristics before using AI, monitor bias closely and correct problems where appropriate</li> </ul>
Accountability and governance	<ul style="list-style-type: none"> <li>• Ensure that the Board of Trustees, CEO and local governing bodies, ICT Manager and Headteachers and staff have clear roles and responsibilities in relation to the monitoring, evaluation, maintenance and use of AI</li> </ul>
Contestability and redress	<ul style="list-style-type: none"> <li>• Make sure that staff are empowered to correct and overrule AI suggestions – decisions should be made by the user of AI, not the technology</li> <li>• Allow and respond appropriately to concerns and complaints where AI may have caused error resulting in adverse consequences or unfair treatment</li> </ul>

Any plans, policies or documents produced with the support of artificial intelligence must be clearly identified as such. Where AI-generated content is used, the member of staff, trustee or local governor remains fully responsible for the accuracy, appropriateness and compliance of the final document. AI-generated plans, policies or documents must only be shared with others where the individual is satisfied that the content has been suitably reviewed, verified and is fit for purpose.

### **Specific Use of AI by Teaching Staff:**

- Teaching staff may use artificial intelligence tools to support the development of educational resources, including lesson planning, differentiated and personalised learning activities, assessment materials and the identification of potential gaps in knowledge. AI-based platforms may be used to generate suggestions aligned to the agreed curriculum, such as topics, learning sequences or activities. Any outputs generated by AI tools must be used as a starting point only, with teaching staff applying their professional judgement to review, adapt and refine content to ensure it is accurate, appropriate and meets intended learning objectives.
- AI tools can be used by teachers to engage students/pupils in digital learning platforms that comply with this policy and the AI Tool Risk & Compliance Checklist.
- Artificial intelligence tools may be used to support aspects of the marking and feedback process, including the automated marking of objective assessments such as multiple-choice or short-response tasks, and the identification of potential areas for improvement within extended written work. Any marks or feedback generated through AI tools must be reviewed, verified and, where necessary, amended by teaching staff to ensure accuracy, fairness and consistency. Professional judgement must be applied in all cases, particularly when assessing subjective or open-ended responses that require interpretation and deeper analysis.

**Any AI-based marking platform must receive prior Trust approval before implementation.** The quality and impact of AI-generated marking and feedback will be subject to quality assurance processes at subject, departmental and senior leadership level.

- Teaching staff can support students/pupils to gain feedback on their work using AI, replicating peer assessment processes. This will allow students/pupils to receive instant personalised and valuable feedback and improvement strategies in their work, helping to identify misconceptions and gaps in knowledge, as well as helping them develop more structured or creative writing. It is important that teaching staff play an integral role in this process and continue to monitor the feedback provided, as with peer assessment.
- Teaching staff may use artificial intelligence tools to support the drafting of pupil reports to improve efficiency and accuracy. Where AI tools are used, the member of staff remains fully responsible for the content of the final report and must review, amend and personalise any AI-generated text to ensure it accurately reflects their professional judgement, assessment evidence, observations and appropriate tone. Personal or identifiable pupil data must not be entered into AI tools at any stage of the report writing process.

## **Students/Pupils**

Pupils must:

- Follow the guidelines set out in section 6 of this policy ('Acceptable Use of AI by Staff and Students')

## **4. Use of AI by staff across the trust, trustees and local governors**

### **4.1 The Use of AI Tools**

At Brighter Futures Learning Partnership Trust (BFLPT), we are committed to supporting staff, Trustees, and Local Governing Board members in reducing workload wherever possible. Generative AI tools may be used to make certain written tasks quicker and more efficient. However, they cannot replace the professional judgement, expertise, or decision-making of a human. Regardless of the tools or resources used in the creation of plans, policies, or other documents, the quality, accuracy, and content of the final product remain the responsibility of the individual who produced it.

The Trust does not maintain a fixed list of approved AI tools. Given the widespread integration of AI into digital platforms, a risk-based approach is adopted.

The responsibility for ensuring that any AI tool is appropriate, secure and compliant with Trust policies rests with the individual user. Before using any new AI tool for Trust-related purposes, staff must complete the Trust's AI Tool Risk & Compliance Checklist (**Appendix 1**) and actively consider data protection, safeguarding, security and ethical implications.

Staff must not assume that a tool is suitable simply because it is widely available or embedded within existing software. Where there is any uncertainty regarding risk or compliance, staff must consult the Trust ICT Manager before proceeding. Failure to do so may be treated as a breach of this policy.

### **4.2 Data Protection and Privacy**

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, BFLPT will treat this as a data breach, and it will be reported to the CEO. We will follow the personal data breach procedure outlined in our Data Protection and information Management Policy. Please also refer to section 10 of this policy.

### **4.4 Intellectual Property**

Most generative AI tools use inputs provided by users to train and improve their underlying models. Students/Pupils retain the intellectual property (IP) rights to any original content they produce, including work that demonstrates reasoning, calculations, or extended responses beyond simple multiple-choice questions. Brighter Futures Learning Partnership Trust (BFLPT) will not permit, and will not facilitate, the use of intellectual property, including students/pupils' work, to train generative AI models without appropriate consent or a clear legal exemption under copyright law. Exemptions to copyright are limited, and where there is any uncertainty regarding compliance with the law, the Trust will seek formal legal advice before proceeding.

#### **4.5 Bias**

We are aware that AI tools can perpetuate existing biases, particularly towards protected characteristics including sex, race and disability. For this reason, critical thought must be applied to all outputs of AI applications. This means fact and sense-checking the output.

BFLPT will ensure we can identify and rectify bias or errors by training staff in this area. We will also regularly review our use of AI to identify and correct any biases that may arise. If parents/carers or students/pupils have any concerns or complaints about potential unfair treatment or other negative outcomes because of AI use, these will be dealt with through our usual BFLPT Complaints Procedure.

#### **4.6 Raising Concerns**

Staff are encouraged to raise any concerns regarding the use of AI, or any incidents where AI may have been used in a way that results in errors, adverse consequences, or unfair treatment, with their Line Manager or Headteacher in the first instance. Any suspected misuse of AI by staff must also be reported to the Headteacher, who will inform the CEO. Safeguarding concerns arising from the use of generative AI by students/pupils must be reported immediately to the Designated Safeguarding Lead (DSL) in accordance with the Trust's Safeguarding Policy.

#### **4.7 Ethical and Responsible Use**

BFLPT will always:

- Use generative AI tools ethically and responsibly
- Remember the principles set out in our trust's equality policy when using generative AI tools: BFLPT Equality & Diversity Policy
- Consider whether the tool has real-time internet access, or access to information up to a certain point in time, as this may impact the accuracy of the output
- Fact and sense-check the output before relying on it

Staff members, trustees and local governors must not:

- Generate content to impersonate, bully or harass another person
- Generate explicit or offensive content
- Input offensive, discriminatory or inappropriate content as a prompt

### **5. Educating students/pupils about Artificial Intelligence**

The Brighter Futures Learning Partnership Trust (BFLPT) recognises that students/pupils benefit from a knowledge-rich curriculum that enables them to become well-informed users of technology and to understand its impact on society. A strong foundation of knowledge will support students/pupils in developing the skills necessary to use generative AI effectively and responsibly.

- A culture of responsible AI use will be fostered by engaging students/pupils in discussions about data privacy, bias, safeguarding, and the wider social impact of AI applications, delivered through a curriculum approach agreed by each school or UTC.
- Students/Pupils will be explicitly taught not to input personal, sensitive, or confidential information into generative AI tools, including email addresses.
- AI education will be embedded within the curriculum to provide students/pupils with a clear understanding of AI's capabilities, limitations, and ethical considerations. Guidance will be provided on recognising reliable AI sources and evaluating the credibility and accuracy of AI-generated information.
- AI tools and technologies will be incorporated into teaching and learning across subjects and year groups, offering students/pupils hands-on experience and opportunities to develop AI literacy and practical skills.
- Safe use of AI will be an integral part of online safety education, ensuring students/pupils are protected from harmful or misleading content.

## 6. Acceptable Use of AI by Staff and Students

### 6.1 – Staff

#### Staff MUST:

- Apply professional judgement to all outputs and maintain accountability for final work
- Fact-check and verify all AI content
- Acknowledge AI-supported work where appropriate
- Consider bias and equality implications
- Consult the Trust ICT Manager when introducing new AI tools
- Follow the AI Tool Risk and Compliance Checklist (Appendix 1) prior to introducing new AI tools
- Report safeguarding or data concerns immediately
- Promote and uphold academic integrity, emphasising the importance of critical thinking, creativity, originality, and honesty in pupil work, and discouraging the misuse of AI as a form of plagiarism or academic dishonesty
- Clearly communicate expectations and guidance regarding acceptable and unacceptable uses of AI, particularly in relation to assessments
- Use a range of assessment approaches to verify pupil understanding and ensure work reflects genuine learning. These may include class discussions, oral presentations, practical tasks, written reflections, and in-class assessments
- Schools/UTCs within BFLPT will consider any unattributed use of AI-generated text or imagery to be plagiarism and will follow our plagiarism procedures as set out in the relevant school/UTC exam policy

#### Staff MUST NOT:

- Enter personal, safeguarding, financial or identifiable data into AI tools
- Use AI to make legal, disciplinary, HR or safeguarding decisions

- Generate official communications without appropriate review
- Upload pupil work or intellectual property into public AI tools
- Use AI to harass, impersonate or mislead
- Rely solely on AI without human oversight

**Students MAY:**

- Complete age-appropriate AI-based activities that help them develop skills in knowledge building, problem-solving, data analysis, and creative expression when directed by staff
- Use AI to support self-assessment, peer assessment, or teacher-guided assessment processes, enabling students/pupils to receive timely, personalised feedback and suggestions for improvement
- Study AI within curriculum contexts, for example in IT lessons or in creative subjects such as art, including work involving AI-generated images

**Students MUST:**

- Acknowledge the use of AI tools when used as a source of information. References should include the name of the AI tool used and the date on which the content was generated
- Use AI tools ethically, responsibly, and respectfully, and must consider the impact of their actions on others

**Students MUST NOT:**

- Use AI during any form of assessment, including internal and external examinations, tests, and coursework
- Use AI to complete homework or classwork where AI-generated content (text, images, or solutions) is presented as the pupil's own work
- Enter personal information into AI systems
- Use AI to bully, harass or generate harmful content
- Create, request, or share explicit, offensive, or inappropriate content, including (but not limited to) the generation of sexualised or inappropriate images of students or staff
- Enter prompts or instructions that are offensive, discriminatory, abusive, or otherwise inappropriate
- Attempt to bypass filtering systems

## 7. Formal assessments

Brighter Futures Learning Partnership Trust (BFLPT) will continue to take all reasonable steps to prevent malpractice arising from the use of generative AI in assessments. Headteachers are responsible for ensuring that all students/pupils understand that failing to attribute AI support or content in work submitted for external qualifications, including coursework,

constitutes malpractice. Such incidents may need to be reported to the relevant exam board and could result in disqualification from the affected unit, qualification, or all qualifications awarded by that board, in accordance with the Joint Council for Qualifications (JCQ) regulations (see Section 5). The Trust will adhere to the most up-to-date guidance issued by the JCQ regarding the use of AI in assessments.

## **8. Staff training**

- All staff will engage in an introductory training session to provide them with a foundational knowledge and understanding of AI and its permitted use within the Trust, alongside safe internet use and online safeguarding training. This will also be a part of the new staff induction process at trust, school and central team level when new colleagues join the trust.
- Subsequently, staff will receive ongoing training and support to effectively integrate AI into their work, including professional development opportunities focused on AI tools and their effective integration into trust and school administrative and teaching practices.
- Training and support will be planned as part of an ongoing professional development programme and on an as-needed basis. Staff have a responsibility to identify any training, and development needs to ensure they adhere to this policy and should discuss these with their line manager.
- Headteachers, senior leaders and central trust members will receive relevant and regular updates on the use of AI as appropriate to keep abreast of best practice through CEO Headteacher Board meetings or specifically calendared focus meetings.

## **9. Referral to our child protection and safeguarding policy**

The Trust is aware that the use of generative AI may in some circumstances lead to safeguarding concerns including, but not limited to:

- Sexual grooming
- Sexual harassment
- Sexual extortion
- Child sexual abuse/exploitation material
- Harmful content including Deepfakes
- Harmful advertisements and promotions
- Bullying

Where there are safeguarding concerns arising from the use of generative AI a report must be made to the DSL immediately.

Any such incident will be dealt with according to the procedures set out in the Trust's Safeguarding Policy. This includes risks arising from AI-generated or manipulated images, video, or audio ("deepfakes") which may be used to harass, groom, extort, or falsely implicate individuals.

Any AI-related incident involving safeguarding, personal data, reputational risk, or media interest must be escalated to the CEO immediately.

## 10. Breach of this policy

### 10.1 By staff

Breach of this policy by staff will be dealt with in line with the Trust's Staff Code of Conduct:

Where disciplinary action is appropriate, it may be taken whether the breach occurs:

- During or outside of working hours
- On an individual's own device or a Trust/school device
- At home, at school or from a remote working location

Staff members will be required to co-operate with any investigation into a suspected breach of this policy. This may involve providing the trust with access to:

- The generative AI application in question (whether or not it is one authorised by the trust)
- Any relevant passwords or login details

You must report any breach of this policy, either by you or by another member of staff, to your senior leader/line manager immediately.

### 10.2 By Trustees or Local Governing Board Members

Trustees or local governors found in breach of this policy will require a response that is proportionate, procedurally fair, and fully aligned with governance obligations under:

- The *Academies Trust Handbook*
- Charity Commission expectations for trustee conduct
- Trust-level policies (e.g., ICT Acceptable Use, Data Protection, AI Use Policy, Code of Conduct)

The process for managing a breach of the AI policy is as follows:

An AI breach or incident includes any actual or suspected misuse, failure or unintended outcomes arising from the use of an AI system that may impact on safeguarding, data protection, security, accuracy or professional standards.

Immediate action will be to:

- Stop using the AI tool immediately
- Preserve any evidence e.g. screenshots, outputs or system logs
- Report to the Trust IT Manager and CEO immediately.

**Concerns should not be investigated by staff.**

The breach will be reported to the Operations Director. Any safeguarding concerns will be reported immediately to the DSL and Headteacher. The external DPO will be advised, and the Trust will assess whether notification to the Information Commissioner's Office (ICO) is required within appropriate statutory timescales. The Trust will investigate the incident, maintain clear records of the breach and take appropriate actions. The Trust Board and Local Governing Board will be informed of serious AI incidents.

Following the investigation, the Trust may implement appropriate actions, which could include:

- Mandatory training or refresher guidance;
- Restriction of access to systems or AI tools;
- Referral to external regulatory or oversight bodies (e.g., Charity Commission, Information Commissioner's Office) where required;

All decisions, supporting evidence, and actions taken must be formally recorded and retained in accordance with Trust policy.

### **10.3 By Students/Pupils**

Any breach of this policy by a pupil will be dealt with in line with the Behaviour Policy of the school/UTC where the pupil attends.

## **11. Monitoring and transparency**

AI technology, including its benefits, risks, and potential harms, evolves rapidly. As such, this policy is a live document and must be updated by the Trust AI Lead whenever there are significant changes to the use of AI within the Trust or to the associated risks of AI use. This policy will also be reviewed regularly to ensure alignment with emerging best practice, technological developments, and changes to legislation or regulations.

The policy will be reviewed annually and shared with the Board of Trustees. All teaching staff are required to read and adhere to this policy, with Headteachers responsible for ensuring compliance within their schools/UTC. The Trust AI Lead will monitor the effectiveness of AI use across the Trust and ensure that all members of the Trust community are kept informed about AI technologies and their educational applications.

As part of this ongoing evaluation, feedback from students/pupils, parents/carers, and staff, collected through regular surveys, will be considered to inform the development and implementation of AI across all schools in the Trust. The Trust AI Lead will maintain a comprehensive audit log of used AI tools, Data Protection Impact Assessments (DPIAs), staff training completion, and any reported incidents, and will report on these matters to the Board on an annual basis.

## **12. Links with other policies**

This AI policy is linked to our trust and individual school policies, including:

- Data protection and Information Management policy

- Safeguarding policy
- Non-Examination Assessment policy
- Exams policy
- Homework policy
- Behaviour policy
- Staff code of conduct
- Marking and feedback policy
- ICT acceptable use policy
- Digital safety policy
- Equality and diversity policy
- Insert any other relevant policies

## Appendix 1: AI Tool Risk & Compliance Checklist

This checklist is provided to support staff in making informed, responsible decisions when considering the use of artificial intelligence (AI) tools for Trust-related purposes.

All staff are expected to apply professional judgement and use this checklist to assess suitability, risk and compliance before using any AI-enabled platform.

Where there is any uncertainty regarding risk, compliance, safeguarding or technical suitability, staff must seek advice from the Trust ICT Manager before proceeding.

Ultimate responsibility for the appropriate use of AI rests with the individual user.

AI Tool Risk & Compliance Checklist	
<b>Purpose &amp; Suitability</b>	<ul style="list-style-type: none"><li>• Before using an AI tool, consider:<ul style="list-style-type: none"><li>• Is there a clear educational or operational benefit?</li><li>• Is AI genuinely appropriate for this task?</li><li>• Will a human review and verify all outputs before use?</li><li>• Will AI be avoided for high-stakes decisions (e.g. safeguarding, disciplinary, legal, HR or employment matters)?</li></ul></li><li>• If the answer to any of the above is unclear, seek advice.</li></ul>
<b>Data Protection and Privacy</b>	<ul style="list-style-type: none"><li>• Ask yourself:<ul style="list-style-type: none"><li>• Will I enter any personal, sensitive or identifiable information into this tool?</li><li>• Does the tool explain how it stores and processes data?</li><li>• Is there any indication that data may be used to train public AI models?</li><li>• Would entering this information comply with UK GDPR and Trust data protection policies?</li></ul></li><li>• If personal data may be involved, consult the Trust ICT Manager before use.</li><li>• Personal, safeguarding, financial or confidential Trust data must not be entered into AI tools unless appropriate safeguards are confirmed.</li></ul>
<b>Security &amp; Technical Risk</b>	<ul style="list-style-type: none"><li>• Consider:<ul style="list-style-type: none"><li>• Is the platform accessed via a secure (HTTPS) connection?</li><li>• Does it request unnecessary permissions?</li><li>• Does it integrate with Trust systems or accounts?</li><li>• Could it bypass filtering or monitoring systems?</li></ul></li><li>• Where integration, logins or system access are involved, consult the Trust ICT Manager.</li></ul>

<b>Safeguarding and Student Protection (if applicable)</b>	<ul style="list-style-type: none"> <li>• If the tool will be used with or accessed by students/pupils: <ul style="list-style-type: none"> <li>• Does it include content moderation or safety controls?</li> <li>• Could it expose students to harmful, biased or inappropriate content?</li> <li>• Are age restrictions appropriate?</li> <li>• Is staff supervision in place?</li> </ul> </li> <li>• If there are safeguarding concerns, consult the DSL and/or Trust ICT Manager before use.</li> </ul>
<b>Ethical Use, Bias and Fairness</b>	<ul style="list-style-type: none"> <li>• Reflect on: <ul style="list-style-type: none"> <li>• Could this tool generate biased or discriminatory outputs?</li> <li>• Are outputs transparent and explainable?</li> <li>• Can AI suggestions be challenged or overridden?</li> <li>• Does use align with the Trust’s Equality &amp; Diversity Policy?</li> </ul> </li> <li>• All AI outputs must be critically evaluated and not relied upon without professional judgement.</li> </ul>
<b>When to Seek Support</b>	<ul style="list-style-type: none"> <li>• You must contact the Trust ICT Manager before proceeding if: <ul style="list-style-type: none"> <li>• Personal or sensitive data may be processed</li> <li>• The tool integrates with Trust systems</li> <li>• Students will use the platform independently</li> <li>• Payment or procurement is involved</li> <li>• You are unsure about security, safeguarding or compliance</li> </ul> </li> </ul>