Maiden Erlegh Trust

ACCEPTABLE USE OF ARTIFICIAL INTELLIGENCE (AI) POLICY

MAIDEN ERLEGH TRUST

Initial approval:	May 2026
Review frequency:	Annually
Date(s) reviewed:	

Contents

Purpose 3
Aims of the policy 3
Scope 3
Guiding Principles 4
Definitions 4
Legal Framework 5
Roles and responsibilities 6
Approved AI platforms for staff use 7
Prohibited AI platforms and devices 8
Rules about the use of AI tools 8
Staff Use of AI 9
Student use of AI and AI literacy 10
Preventing misuse of AI tools by pupils 11
Identifying misuse of AI tools by pupils 12
Use of AI in Assessment and Examinations 13
Misuse of AI in Assessments and Examinations 13
Safeguarding 13
Data Protection and cybersecurity 14
Incident reporting and data breach procedure 15
Review process 17

Purpose

This Acceptable Use of Artificial Intelligence (AI) Policy sets out how Maiden Erlegh Trust governs the appropriate use of artificial intelligence to support educational practice, operational processes and organisational decision-making. AI is used to inform and strengthen professional practice, while responsibility and accountability for decisions remain with staff.

Although AI technologies can offer meaningful benefits, their outputs may include inaccuracies, bias or inappropriate content and could lead to malpractice.

The Policy will provide a framework for the integration and management of AI as an educational tool, encompassing ethical compliance, educational enhancement, workload reduction, data security and innovation.

Aims of the policy

- **Educational enhancement**: to improve Teaching and Learning outcomes, and supporting our Trust-wide PedTech (pedagogical technology) principles
- **Legal and ethical compliance**: to ensure ethical and legal use of AI by all stakeholders
- **Protecting information**: to safeguard the privacy and data of all stakeholders
- **Workload reduction and efficiency**: to utilise AI where appropriate to reduce the administrative workload of all staff
- **Innovation**: to remain at the forefront of education practice, by integrating AI to enhance and supplement Maiden Erlegh Trust's mission to provide a high-quality education for all learners
- **Supporting accessibility and inclusion**: supporting the development of equitable learning and training opportunities for staff and students across the Trust
- **Future preparedness**: preparing staff and students for how emerging technologies are changing workplaces and society
- **Develop intellectual capabilities**: supporting staff and students to use AI to develop thinking, reasoning, and reflective abilities
- **Enhanced personalisation**: aiding the development of increasingly bespoke resources and learning and training experiences for staff and students

Scope

All academies and educational settings within the Trust are included in the Policy, covering all aspects of educational practice. All staff are included and must adhere to the AI Policy when using or commissioning AI tools. All forms of AI technology are covered, including generative AI, machine learning systems, analytics platforms, accessibility tools, communication tools, and operational software used across schools and support teams. All third-party AI tools used for any purpose must be risk-assessed, with DPIAs (Data Protection Impact Assessments) completed where personal data is processed.

Guiding Principles

The Trust's use of AI will be guided by the following core ethical principles:

- **Accountability, responsibility and human-centricity**: Artificial intelligence must be deployed in ways that assist professional decision-making. Final judgement, accountability and oversight remain the responsibility of people, not automated systems.
- **Transparency and openness**: All stakeholders should understand when and how AI is being used, including clarity around why the system is being used, the nature of the information it draws upon, and the constraints or risks associated with its outputs.
- **Inclusivity and accessibility:** The Trust will ensure AI tools are accessible and beneficial to all learners, with particular attention to SEND students and promoting digital dignity.
- **Privacy first approach**: The Trust prioritises the protection of personal and sensitive data. Personal, student or operational information must only be processed using approved platforms supported by appropriate contractual, technical and organisational safeguards.
- **Fairness and equity**: AI systems must be designed, implemented and reviewed to reduce the likelihood of unfair outcomes, discriminatory effects or disproportionate impacts on individuals or groups.
- **Safety and reliability:** AI tools must be robust, evidence based, and safe to use in real-world settings. The Trust should monitor performance, mitigate risks, and discontinue use of tools that fail to meet agreed operational, safeguarding or ethical standards.
- **Alignment**: AI adoption must align with the Trust's strategic vision to ensure consistency of approach across all schools and functional areas, whilst reinforcing our educational and organisational priorities.
- **Monitoring**: The Trust will maintain robust data, safeguarding, and ethical standards, including regular bias monitoring, cybersecurity protections, and validation of AI outputs across all professional areas.

Teaching staff are expected to oversee and shape students' interactions with AI tools in line with curriculum expectations and the Protocol for Acceptable Use of Digital Technology for Staff.

Definitions

- **AI**: Technology that enables computer systems to carry out tasks that would typically require human intelligence, such as recognising images, understanding speech, or making decisions.
- **Consumer grade:** Tools designed for personal, public use, often available for free or through individual accounts. These tools typically do **not** provide organisational data protections and may use user inputs to train their models, creating privacy and compliance risks in schools. They offer no administrative controls for safeguarding or data-governance needs.

- **Enterprise grade:** Tools built specifically for organisational use, with strong security, governance, and administrative controls. These systems guarantee that data is **not** used to train public AI models and that all processing stays within the organisation's secure environment. They are contractually compliant with data-protection requirements and suitable for professional and educational settings.
- **Generative AI**: A type of artificial intelligence that creates new content or outputs based on patterns learned from the data it was trained on.
- **Misuse of AI**: Any inappropriate, unethical, or unauthorised use of artificial intelligence tools by pupils or staff that undermines integrity, safety, data protection, professional standards, or the authenticity of work or decision-making.
- **AI literacy**: The skillset needed to understand what AI can and cannot do, recognise its ethical considerations, and critically judge the accuracy and reliability of AI-generated material.
- **AI-assisted output**: Work or content that has been supported or partially generated by AI but still involves human oversight, editing, or decision-making. This is different from fully automated output.
- **AI bias**: A systematic error in an AI system that results in unfair or unequal outcomes for individuals or groups (e.g., SEND pupils, behaviour profiling, recruitment).
- **Hallucination**: When an AI system produces information that appears credible but is false, inaccurate, or entirely invented.
- **AI Enhanced wearable**: A device worn on the body that uses artificial intelligence for real-time support, data recording, or communication—for example, smart glasses with features such as video capture, translation, or live streaming.
- **Autonomous AI agent**: An AI tool capable of acting on its own, solving complex problems, and completing multi-step activities without ongoing human control. This includes systems able to browse the web or run tasks in the background independently.
- **AI meeting notetaker**: Software that uses AI to automatically record, transcribe, summarise, or interpret spoken content during face-to-face or online meetings. Examples include Otter, Fireflies, and VoiceNotes.

Legal Framework

This policy takes account of all relevant statutory guidance and regulatory frameworks, including, but not limited to, the documents listed below, and any future updates or replacements issued by the relevant authorities. This policy will be reviewed accordingly as and when any relevant statutory guidance and/or regulatory frameworks are renewed:

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR)
- DfE (2025) 'Keeping children safe in education 2025'
- DfE (2023) 'Generative artificial intelligence in education'
- DfE (2023) 'Meeting digital and technology standards in schools and colleges'

- DfE (2024) 'Generative AI: product safety expectations'
- DfE (2025) Using AI in education settings: support materials
- JCQ (2023) ‘Artificial Intelligence (AI) Use in Assessments: Your role in protecting the Integrity of Qualifications’
- JCQ (2023) ‘Suspected Malpractice Policies and Procedures’
- Online Safety Act 2023
- Equality Act 2010

Roles and responsibilities

The AI and Systems Governance Panel will be responsible for:

- Ensuring that this Policy is effective and complies with relevant laws and statutory guidance
- Keeping up to date and informed with AI technologies relevant to the Trust
- Understanding and maintaining an awareness of what the use of AI means for data protection in the Trust
- Approving Data Protection Impact Assessments (DPIAs)

Headteacher:

- Ensuring that staff receive regular training on how to use AI tools
- To report any suspected breaches of the policy to the AI and Systems Governance Panel

IT Service Provider:

- Providing technical support in the development and implementation of the Trust’s AI practices, policies, and procedures
- Implementing appropriate security measures
- Supporting the technical aspects of AI tool, vetting, and deployment
- Managing network security and access controls relating to AI use

School Improvement Director – Safeguarding and Culture:

- Taking the lead responsibility for online safety including AI-specific safeguarding risks across the Trust
- Undertaking training to understand the risks associated with using AI tools in school, including deepfakes, AI-facilitated harassment, and misinformation
- Maintaining records of reported online safety concerns, relating to the use of AI tools and actions taken in response to concerns
- Reporting to the AI and Systems Governance Panel about the use of AI tools on a regular basis and how it links to safeguarding
- Ensuring enhanced safeguarding measures for vulnerable learners, including SEND students

Staff:

- Adhering to the Protocol for Acceptable Use of Digital Technology for Staff and Data Protection Policy and other relevant policies
- Take responsibility for the security of the AI tools and data they have access to
- Demonstrating appropriate professional conduct and digital practice when engaging with AI systems

- Maintaining a professional level of conduct in their use of AI tools
- Maintaining an informed understanding of the potential risks associated with the use of AI tools in educational settings.
- Reporting concerns in line with the Trust reporting procedure

Students:

- Adhering to the Student E-Safety Agreement and Data Protection Policy and other relevant policies
- Taking appropriate steps to avoid sharing personal or sensitive information when using AI-enabled systems
- Maintaining academic integrity by properly acknowledging AI assistance
- Take responsibility for the security of the AI tools and data they have access to
- Having an awareness of the risks that using AI tools in school poses
- Reporting concerns in line with the Trust reporting procedure

Approved AI platforms for staff use

To ensure the security of Trust and school data and to comply with our data protection obligations, the use of consumer-grade AI platforms, such as OpenAI ChatGPT, for any Trust-related work is now **strictly prohibited**.

All staff are required to use one of the two officially sanctioned, **enterprise-level AI platforms** provided by the Trust:

- **Microsoft Copilot** - using only an organisation-provided Microsoft 365 account
- **Google Gemini** – using only an organisation-provided Google account

Access to both Microsoft Copilot and Google Gemini must be through the user's official Trust-provided username and password. This ensures that all activity is contained within our secure, data-protected enterprise environment. Using personal accounts to access these services for Trust-related work is not permitted.

Use of AI within the Trust is restricted to approved enterprise platforms because these environments provide enforceable safeguards around data use, security and governance, including assurances that Trust data is excluded from the development of public AI models.

Other approved AI applications:

- Notebook LM
- Olex AI
- Teach Mate AI
- Phrasly AI (AI detection tool)
- Adobe Firefly
- SLT AI
- Canva
- Brisk Teaching
- Curiopod

The following tools containing AI features are also approved:

- Socrative
- Quiziz
- Quizlet

Any other AI platforms or products that are being considered for local or departmental use must undergo a formal risk assessment. This requires the completion of a Data Protection Impact Assessment (DPIA) and a formal consultation with The AI and Systems Governance Panel before the platform can be approved.

If staff are using any programme or application with add-on AI features which is not on the approved list, then they must seek approval from The AI and Systems Governance Panel.

Prohibited AI platforms and devices

All other AI platforms and tools are prohibited (this currently includes, but is not limited to, OpenAI ChatGPT, Otter.ai (Otter Notetaker and OtterPilot), Fireflies.ai and Read.ai.

A significant number of AI platforms present unacceptable risks to data protection, safeguarding, privacy, and statutory compliance. These platforms may present unacceptable risks unless formally assessed and approved. In addition, some AI systems have been identified as fundamentally incompatible with the protection of individual rights and freedoms.

Rules about the use of AI tools

No personal or sensitive data can be entered into AI tools e.g. names, year group, ethnicity. AI is a drafting tool and should always be reviewed by humans afterwards. AI must not replace professional judgement.

Risks of Using AI Tools in Education

The Trust is aware that the use of Artificial Intelligence (AI) tools in education presents significant opportunities but also introduces important risks that schools and trusts must manage carefully.

Risks include:

- Risk of academic dishonesty, including AI-generated homework, coursework, essays, and assessments.
- Potential reduction in students' critical thinking, creativity, independent learning, and problem-solving skills through overreliance on AI tools.
- AI systems may generate inaccurate, misleading, biased, or inappropriate content that could negatively affect teaching and learning.

- Risk of non-compliance with UK GDPR, copyright, confidentiality, and safeguarding obligations.
- Unequal access to AI technologies may increase educational disadvantage and widen the digital divide.
- Challenges in verifying the authenticity of student work and assessing genuine understanding and progress.
- Ethical concerns relating to transparency, accountability, bias, and fairness in AI-generated outputs.
- Risk that AI-generated content may expose students to harmful, inappropriate, or unmoderated material.
- Potential overdependence on AI tools by both students and staff, reducing the role of professional judgment and human interaction.
- Concerns around intellectual property, ownership, and copyright of AI-generated materials.
- Rapidly changing AI technologies may create difficulties in maintaining effective oversight, governance, and staff awareness.
- Reputational risks to the Trust if AI tools are misused or implemented without appropriate controls.
- Cybersecurity risks associated with unapproved or unsecure AI applications and platforms.
- Need for clear policies, staff training, monitoring, and responsible use guidance to ensure safe and effective implementation of AI tools within the Trust.

Staff Use of AI

Staff may use approved AI tools in line with Trust policy for the following professional activities and purposes.

Please note this is not exhaustive. If in doubt about whether an intended use of AI meets our acceptable use guidelines, please refer to The AI and Systems Governance Panel.

Where AI tools are used for these purposes, all staff members will understand that the quality and content of the final document remain the professional responsibility of the staff member who produced it. Staff members using AI tools to create documents will not assume the AI output will be comparable with a human-designed document that has been developed in the specific context of the Trust.

Teaching staff:

- Drafting of lesson plans, worksheets, and resources
- Creating model answers, rubrics, and question banks
- Summarising long documents, e.g., policies, research
- Generating administrative templates, e.g., emails, letters
- Creating differentiated examples or explanations
- Informal or formative assessment activities, for example short retrieval tasks or in-class knowledge checks.
- Suggesting alternative teaching approaches or scaffolds
- Supporting curriculum planning through idea generation
- Developing analogies or visual explanations to clarify concepts

- Generating personalised tasks and reading – without the inputting of personal and/or sensitive data
- Summarising research articles or academic papers to support evidence-informed practice
- Generating reflective prompts, e.g., for professional development conversations Providing example feedback comments that can then be personalised
- Producing timelines, checklists, or procedural guides

Associate Staff*:*

- Drafting routine emails, letters, memos, or communications that are then reviewed and edited
- Summarising long documents, e.g., policies
- Creating templates, checklists, timelines, schedules, and procedures
- Generating first drafts of reports or briefings
- Drafting job descriptions, adverts, and person specifications
- Creating interview questions or competency-based prompts for HR staff to review
- Summarising anonymised feedback from staff surveys
- Drafting policy summaries or internal guidance for staff
- Generating template letters
- Automating repetitive admin (with approved enterprise tools only)
- Drafting guides and user instructions for staff Generating code snippets or automation concepts without inputting secure system information
- Drafting newsletters, website content, or social media posts for staff to edit
- Creating visual ideas, slogans, or copy for staff to edit
- Producing publicity drafts or event descriptions
- Generating project timelines

Student use of AI and AI literacy

The Trust recognises that the use AI must be carefully differentiated based on developmental stage and strict adherence to age restrictions. Learners must declare where AI has been used to support homework, coursework or assessed work, where this is allowed.

Primary (Reception – Year 6)

- No direct student access to general purpose generative AI tools
- Teacher mediated AI interactions only
- Focus on foundational digital literacy and developing an understanding that technology is not infallible
- Use restricted to vetted, closed AI applications designed for primary age
- Strict adherence to age restrictions

Secondary (Years 7-13)

- Years 7-9: Supervised exploration with teacher supervision and vetting of outputs

- Years 10-11: Structured access to specific approved tools, under clear guidelines
- Year 12-13: Guided autonomous use for research and learning under clear guidelines

Preventing misuse of AI tools by pupils

The Trust acknowledges that misuse of AI tools can happen both accidentally and intentionally. Preventing misuse requires a combination of clear boundaries, effective supervision, and ongoing digital literacy education. The Trust will take the following actions to prevent the misuse of AI tools by students:

Technical and Access Controls

- Restrict access to online AI platforms and generative AI tools on school devices and networks, particularly on devices used for assessments, examinations, or coursework.
- Ensure that filtering and monitoring systems are configured to block known high-risk or unapproved AI services.
- Provide access only to approved, enterprise-safe AI tools that meet the Trust's data protection and safeguarding standards.

Task Design and Supervision

- Set clear deadlines for the submission of work and provide regular reminders so that students have structured timeframes that discourage last-minute AI-generated submissions.
- Allocate sufficient in-class, supervised time for students to complete parts of their work, ensuring their progress reflects their own effort.
- Design tasks that emphasise process as well as output, reducing the likelihood that AI-generated work can replace genuine student understanding.
- Incorporate activities that rely on knowledge gained during lessons, giving teachers confidence that students understand core concepts.

Verification of Student Understanding

- Engage students in verbal discussions, conferences, or questioning about their work to confirm that they understand the content they have produced.
- Use a range of assessment methods—such as class discussion, oral presentations, practical demonstrations, reflective writing, or project-based tasks—to verify genuine comprehension and discourage over-reliance on AI tools.
- Investigate any work that appears inconsistent with a student's usual level, style, or prior progress where misuse of AI is reasonably suspected.

Education, Awareness, and Responsible Use

- Provide ongoing training for staff, students, and parents on what AI tools can and cannot do, the risks associated with their use, and the school's expectations for responsible behaviour.

- Help students develop AI literacy, including understanding when AI is appropriate, how to use it ethically, and how to critically evaluate AI-generated content.
- Where suitable, incorporate transparent and declared AI use into certain tasks, helping students learn how to use AI as a supportive tool without crossing boundaries of academic integrity.

Culture of Integrity and Accountability

- Reinforce the importance of honesty, authenticity, and academic integrity in all work submitted.
- Make expectations for AI use explicit within subject areas, outlining what is allowed, what is not permitted, and how students should reference AI assistance where required.
- Clearly communicate the consequences of misuse, ensuring students understand that dishonest use of AI undermines learning and may lead to disciplinary action.

Identifying misuse of AI tools by pupils

The Trust acknowledges that detecting inappropriate or unauthorised use of AI is essential for maintaining academic integrity and ensuring that students' work reflects genuine understanding. Misuse may be intentional or unintentional, and identifying it requires a combination of professional judgement, observable indicators, and structured verification. Staff will use the following strategies to identify potential AI misuse:

Monitoring Patterns in Work Quality and Progress

- Noting sudden or unexplained changes in a student's written style, vocabulary, structure, or accuracy compared to their usual classroom work.
- Identifying work that appears inconsistent with earlier drafts, planning notes, or demonstrated ability.
- Flagging submissions that demonstrate knowledge beyond what has been taught, without evidence of learning progression.
- Observing work that appears unusually polished, generic, or lacks errors typical of the student's level.

(Where appropriate) Reviewing Drafts, Stages, and Workflow Evidence

- Checking for missing or incomplete planning, draft stages, brainstorming, or process work where these are expected.
- Reviewing timestamps, version history, or digital footprints (where appropriate) to confirm a natural working process.
- Comparing final outputs with earlier phases of work to ensure consistency and developmental progression.

In-class Verification

- Asking students to explain aspects of their work in class, in their own words, without prompts.

- Setting short, supervised in-class tasks linked to their submissions to verify understanding.
- Using quick verbal questioning, quizzes, or reflective activities to check that students can articulate the concepts they supposedly learned.

Observing Content Signals Suggesting AI Generation

- Identifying overly formal or unfamiliar writing patterns that do not match the student's typical tone.
- Detecting factual inaccuracies, invented references, or "hallucinations" typical of generative AI output.
- Recognising broad, vague, or surface-level responses lacking personal insight or contextual detail from class learning.

Collaboration and Investigation

- Discuss concerns with relevant staff for context
- Request clarification if misuse is suspected
- Educate students where misuse is unintentional; apply sanctions where appropriate

Use of AI in Assessment and Examinations

No AI tool will be used in any examination without written approval from the JCQ. All AI-based assistants and software will be subject to the regulations as set out by the JCQ. AI-based assistants and software may only be used for qualification-specific non-examined assessment if it is authorised by the JCQ. This will be subject to specific guidance from the relevant awarding body of the qualification. All use permitted will be in accordance with the regulations.

AI-based assistance or software may be used for in-class, low-stakes informal assessment, such as recall quizzes. Any such use should comply with the Acceptable Use of AI Policy and take into considerations the practices set out by JCQ.

Misuse of AI in Assessments and Examinations

Students must ensure that work submitted for assessment is demonstrably their own. This means ensuring that the final product is in their own words and is not copied or paraphrased from another source, e.g., an AI tool, without acknowledgement. For example, using AI to help generate ideas may be acceptable if the teacher has allowed it and the learner declares it. Submitting AI-generated writing as their own work would not be acceptable.

Safeguarding

Students will be taught about the risks of using AI tools and how to use them safely. Students will be clearly informed about reporting routes and support available if they experience or observe concerns linked to AI use.

The Trust will maintain technical controls, including filtering and monitoring arrangements (following the DfE's Filtering and Monitoring Standards), to reduce the risk of students encountering harmful AI-generated content.

All staff will receive training on the safe use of AI as part of their online safety training, including specific modules on identifying AI facilitated safeguarding risks.

In line with the Trust Safeguarding Policy and Protocol for Acceptable Use of Digital Technology for Staff, staff must take a proactive stance regarding AI-related safeguarding risks, including but not limited to:

- Deepfake bullying
- Impersonation of staff or students
- Sexualised image generation
- Harassment and bullying
- Criminality, AI-enabled coercion, grooming chatbots, and exploitation
- Note that AI may be an aggravating factor in safeguarding and child protection cases

Staff should understand that failure to comply with the policy will be considered under the staff disciplinary policy.

Data Protection and cybersecurity

All use of AI tools within the Trust must comply with UK GDPR, the Data Protection Act 2018, safeguarding requirements, and the Trust's existing data protection, staff and student privacy, cyber security, and acceptable use policies.

- Staff and students must not input confidential, personal, sensitive, safeguarding, or commercially sensitive information into public AI platforms unless the platform has been formally approved by the Trust.
- Personal data relating to students, staff, parents, or Trust operations must only be processed through AI systems that have been assessed for security, privacy, and legal compliance.
- The Trust will ensure that any AI tools used within schools are subject to Data Protection Impact Assessment which includes, review of:
    - Data storage and retention practices
    - Data sharing arrangements
    - Security controls and encryption
    - Supplier compliance with UK data protection legislation
    - Age restrictions and safeguarding measures
- Staff must exercise professional judgment when using AI-generated outputs and must verify the accuracy and appropriateness of all content before use or distribution.
- AI tools must not be used in ways that could compromise safeguarding, confidentiality, examination security, or the integrity of Trust systems and networks.

- The use of unapproved AI applications, browser extensions, or external platforms on Trust devices or networks may be restricted or blocked where cybersecurity risks are identified.
- Staff should not upload copyrighted textbooks, paid-for resources, pupil work or third-party materials into AI tools unless the Trust has permission to do so.
- AI recording, transcription or summarising tools should not be used in meetings unless they have been approved, risk-assessed and everyone in the meeting has been told in advance.
- The Trust recognises that AI systems may be vulnerable to cybersecurity threats, including phishing, malicious code generation, data harvesting, and misinformation. Appropriate filtering, monitoring, and security measures will therefore be maintained.
- Staff and students will receive guidance and training on the safe, ethical, and secure use of AI technologies, including awareness of cyber risks and data protection responsibilities.
- The Trust reserves the right to monitor and review the use of AI systems on Trust-managed devices and networks to ensure compliance with this policy and to protect users and systems.
- AI tools should support teaching, learning, and operational efficiency while maintaining appropriate human oversight, accountability, and security at all times.

Incident reporting and data breach procedure

Breach of this policy may, where appropriate, result in disciplinary action up to and including dismissal or termination of your employment or engagement with us. Where disciplinary action is appropriate, it may be taken whether the breach is committed during or outside normal hours of work and whether or not use of AI is on an individual's own device or one of our devices, and whether at home, in the office or from a remote working location.

In the event of a suspected or confirmed data breach involving the use of AI tools or platforms, the Trust will take immediate action to protect individuals, secure systems, and comply with legal and regulatory obligations.

Any suspected data breach, cybersecurity incident, misuse of AI, or safeguarding concern relating to AI tools must be reported immediately to the School or Trust Data Protection Officer and designated safeguarding lead, in an event of safeguarding concerns, in line with the Trust's data breach procedures.

You are required to assist with any investigation into a suspected breach of this policy. This may involve providing us with access to AI applications and any relevant passwords and login details. You must report any breach of this policy immediately to your line manager, the Operations Manager or Head of IT in the first instance.

Examples of reportable breaches include

- Uploading personal or confidential information into an unapproved AI platform
- Unauthorised disclosure of student or staff data

- Loss, theft, or compromise of devices containing AI-generated or AI-processed data
- AI-generated phishing, malicious content, or cybersecurity incidents
- Inappropriate sharing or storage of sensitive information

Immediate actions

- The Trust will take steps to contain the breach as quickly as possible, which may include:
    - Restricting access to affected systems or accounts
    - Removing shared or uploaded content where possible
    - Resetting passwords or disabling compromised accounts
    - Blocking unsafe AI tools or applications
    - Securing affected devices or networks

Investigation and risk assessment

- The Trust will investigate the nature and scope of the breach to determine:
    - What data has been affected
    - Who may be impacted
    - Whether safeguarding risks are present
    - The likelihood and severity of harm
    - Whether the breach involves third-party AI providers

Notification requirements

- Where required by law, the Trust will report eligible personal data breaches to the Information Commissioner's Office (ICO) within the required statutory timescales.
- Individuals affected by a high-risk breach will be informed where appropriate and provided with guidance on protective actions they may need to take.

Recording and review

- All AI-related data breaches and near misses will be formally recorded and reviewed.
- The Trust will identify lessons learned and implement corrective actions to reduce the risk of recurrence, including:
    - Additional staff training
    - Policy updates
    - Technical security improvements
    - Restrictions on AI platform use

Staff responsibilities

- Staff must cooperate fully with any investigation relating to an AI-related data breach.
- Failure to follow Trust guidance on the safe use of AI tools may result in disciplinary action where appropriate.
- All staff must familiarise and refer to the Trust's current data breach policy which can be found on the IntraMET.

Ongoing protection

- The Trust will regularly review AI systems, cybersecurity controls, and data protection arrangements to ensure continued compliance, safeguarding, and security across all schools and services.

Parents and carers will be informed about the Trust's expectations around AI use, student safety and academic integrity. Parents are expected to sign our Trust Acceptable Use Agreement, and the Acceptable Use of Artificial Intelligence Policy will be published on the Trust website.

Review process

The Acceptable Use of Artificial Intelligence Policy will be reviewed by the AI and Systems Governance Panel on an annual basis. An earlier policy review may be triggered by a breach or cyber security event or when new technology requires approval.