SARACENS
MULTI-ACADEMY
TRUST

# ARTIFICIAL INTELLIGENCE (AI) POLICY

| | |
|---|---|
| Responsibility of *(see policy tracking sheet):* | CFOO |
| Approved by: | Trust Board |
| Date Approved *(by above):* | 11 December 2025 |
| Next Review due by: | December 2026 |

This policy creates the framework of the mandatory principles and requirements for the safe, ethical, and effective use of Artificial Intelligence (AI) across all schools within the Saracens Multi-Academy Trust (the Trust). Individual schools must develop local procedures and protocols that align with these Trust-level requirements.

## 1. Statement of Intent, Scope, and Legal Framework

The purpose of this policy is to ensure that appropriate procedures are in place regarding the use of Artificial Intelligence. The policy aims to **enhance learning outcomes while ensuring data privacy**.

The policy applies to the **whole school community**, including pupils, and where relevant their families, staff, visitors, volunteers, job applicants, contractors, governors, and trustees.

This policy is compliant with, and gives consideration to, the **UK General Data Protection Regulation (UK GDPR)**, the **Data Protection Act 2018**, *Keeping children safe in education* (DfE), and *Generative artificial intelligence in education* (DfE).

## 2. Mandatory Rules for Implementation (The Non-Negotiables)

The default position across the Trust is that **all staff are prohibited from entering any Trust or school data** (including pupil data, staff data, or confidential information) into any AI tool. Use of AI is only permitted if **all three** of the following mandatory conditions have been met:

1. **Contractual Relationship:** The Trust or school must have a formal, **written contractual relationship** with the AI service provider.

2. **No Data Training Guarantee:** The contract or an explicit, unambiguous written statement from the provider must confirm that **Trust data (inputs and outputs) will not be used to train the AI model**.

3. **Data Protection Impact Assessment (DPIA):** A **Data Protection Impact Assessment** must be completed and signed off by the Data Protection Officer (DPO) before the tool is implemented. This assessment must confirm that the tool meets cyber security and safeguarding standards.

## 3. Data Security and Governance

**Prohibited Data Input and Data Breach Risk: As a general rule, and unless explicitly approved under Section 2**, any data entered into AI must not be personal data that is confidential and/or sensitive in nature. Staff are reminded that the submission of such data into an AI tool without consent and/or a legal basis may constitute a **data breach**.

**Pupil Work Prohibition:** Pupils' work should **not be used to train AI tools**. Pupils' work should **not be entered into AI tools without the consent of the owner and the school**.

**Cyber Security:** All implementations must consider **appropriate cyber security procedures** in line with the DfE digital and technology standards where possible.

**4. Ethical Principles and Trust Expectations**

All AI use must adhere to the following principles, aligning with Ofsted's expectations for safety and integrity:

- **Safety and Security:** AI solutions must be safe and secure, protecting users' data.
- **Transparency and Understanding:** Staff must be **transparent** about their use of AI. They must fully **understand the suggestions** it makes and ensure pupils declare AI use within their work.
- **Accountability and Override:** The staff member remains fully responsible for AI outputs. Staff must **review, correct and overrule** suggestions made by AI to ensure accuracy.
- **Fairness and Bias Monitoring:** Schools must **closely monitor the AI used for bias** and must **identify and compensate for any bias or problems**, where appropriate.
- **Academic Integrity:** Staff will consider the potential pupil misuse of AI tools when assessing pupils' work. AI must be a tool, not a substitute for learning.

**5. Roles and Responsibilities**

The Saracens MAT Board is responsible for ensuring the school follows the DfE's digital and technology standards where possible and reviewing the policy on a regular basis.

| *Role* | *Key Responsibilities* |
|---|---|
| **Principal** | Ensuring the appropriate implementation of any necessary AI tools. Ensuring effective monitoring of AI tools takes place. To consider cyber security and safeguarding. |
| **Data Protection Officer (DPO)** | Providing advice on the implementation of AI. Mandatory sign-off on all DPIAs. |
| **Designated Safeguarding Lead (DSL)** | Working with the IT team to ensure appropriate **filtering and monitoring of AI**. Ensuring online safety in relation to AI. |
| **SLT AI Lead (New Role)** | Acting as the figurehead and first point of contact for all AI-related queries, suggestions, and concerns within the school. Overseeing the maintenance and communication of the School Approved AI Tools List. |
| **IT Provider** | Ensuring appropriate **security measures** are implemented. Providing appropriate technical support to implement, monitor, and block AI tools as appropriate. |
| **Staff** | Obtaining permission for responsibly implementing necessary AI tools. The **safe use of AI tools and awareness of associated risks**. **Reporting AI misuse** to the SLT. |

| *Role* | *Key Responsibilities* |
|---|---|
| **Pupils** | **Familiarising themselves** with any AI tools used by the school and the risks they pose. **Reporting AI concerns** and any abuse relating to AI. |
| **Families** | Schools will work with parents to improve their understanding of the benefits and risks of using AI |

**6. Approved AI Tools List**

Each school must **mandatorily maintain a clear, current, and easily accessible list of AI tools** that have been approved for staff and/or pupil use within the school. No AI tool may be used in lessons or for the processing of sensitive data unless it appears on this list.

**7. Appropriate Use, Curriculum, and Safeguarding**

**Curriculum Integration:** Schools must ensure pupils are taught about the safe use of AI, including **familiarising pupils with tools and risks** and fostering critical thinking.

**Learning Enhancement:** Approved AI tools may be used to personalise learning pathways based on pupil progress and use AI analytics to support school improvement planning, and as a research tool.

**Staff Workflow:** Staff must obtain permission for responsibly implementing necessary AI tools for their own workflow within the curriculum and administration.

**Safeguarding Consideration:** The Principal, IT Provider, DPO, and DSL must all consider **cyber security and safeguarding** when implementing AI.

**8. Conduct, Misuse, and Sanctions**

**Assessment Security:** School devices used for assessments and exams **should not have access to the internet or AI tools**.

**Investigation:** Staff should **investigate the inappropriate use of AI tools and report the use to the SLT**.

**Sanctions:** Pupils may be subject to **sanctions** in accordance with the Behaviour for Learning Policy regarding the inappropriate use of AI, including online safety and the submission of work. Schools must clearly communicate these sanctions in their local policy.

**9. Monitoring and Review**

This policy will be **reviewed regularly** by the CFOO in conjunction with the data protection team, the IT team, and Trust leadership. Schools must **respond appropriately to any concerns or complaints about errors made by AI**.

## 10. Links with other policies

This policy links with the following Trust's policies and procedures:

Data Protection Policy

Data Security Policy