



Artificial Intelligence Staff Policy

Version: 1.0

Date: 16/10/2024

thesovereigntrust.uk

The Sovereign Trust is a Multi Academy Trust registered in England No. 09666511. Registered Office: Manor Academy Sale, Manor Avenue, Sale M33 5JX



Chatsworth Futures
Specialist College




Document Control

Title	AI Staff Policy
Supersedes	1.0
Owner	CEO
Circulation/Distribution	All
Review Period	Annually

The Sovereign Trust is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with Trust's policy review schedule.

A current version of this document is available to all interested parties [The Sovereign Trust Website](#)

Signature: 

Date: 16/10/2024

Version History

Next Review Date		16/10/2025		
Version	Date	Amendments	Author	Status
1.0	16/10/2024	Initial Issue	CEO	Approved

AI Staff Policy

Background to the policy

Although Data Protection law does not specifically define or discuss the guidelines for Artificial Intelligence ('AI'), the guidance from the Information Commissioner's Office and the UK government defines it as using non-human systems to imitate human intelligence.

In this time of constant development and increased usage, there is a need to provide staff with guidelines for use and to recognise an employer's right to monitor such usage. We have also set out expectations for AI usage by pupils.

Introduction

AI is transforming the way individuals work. Informed and responsible use of AI has the potential to increase efficiency and improve decision-making.

With these benefits come potential risks, including data protection breaches, the protection of confidential information, ethical considerations, and compliance with wider legal obligations.

We permit the informed and responsible use of authorised AI applications by staff in carrying out specific and authorised tasks. This policy must be complied with when using AI to carry out such tasks.

This policy sets out our rules on using AI in the workplace and how staff should adopt it to ensure we maximise the benefits of AI while minimising any risks or concerns.

Where personal data is used with AI applications, an ICO risk assessment and/or data protection impact assessment ('DPIA') has been carried out to ensure transparency in how AI will be used and what mitigating steps have been taken to reduce any potential risk of harm to pupils, staff and any other data subjects whose data might be shared with the authorised systems.

This policy covers all employees, officers, consultants, contractors, volunteers, interns, casual workers and agency workers.

Pupil usage of AI

As part of this policy, staff should be aware of how the school permits limited pupil usage of AI applications in accordance with the AI policy for pupils. It is important to monitor pupil usage in class and for homework to ensure compliance with this policy or to learn how to monitor when reviewing homework.

Pupils must sign an Acceptable Use Statement to ensure appropriate use of AI. They are reminded of the permitted usage and given an outline of what classes are considered AI misuse.

The school permits pupil usage of AI in the following circumstances:

- (a) As a research tool

- (b) Idea generation for projects
- (c) For use with coursework or homework with the above requirements fulfilled
- (d) [List any other authorised usage]

Examples of AI misuse include, but are not limited to, the following:

- Copying or paraphrasing sections of AI-generated content so that the work is no longer the pupil's own;
- Copying or paraphrasing whole responses of AI-generated content;
- Using AI to complete parts of the assessment so that the work does not reflect the pupil's own work, analysis, evaluation or calculations;
- Failing to acknowledge the use of AI tools when they have been used as a source of information;
- Incomplete or poor acknowledgement of AI tools; or
- Submitting work with intentionally incomplete or misleading references.

Authorised AI applications

The school allow access to the following AI applications for business purposes.

The listed AI applications may be updated at any time. Should staff wish to use another AI application not listed, they must contact the Chief Information Officer to review permission to do so.

Authorised Usage of AI for Staff

Authorised AI applications must only be used by staff for the following business purposes:

- (a) Drafting internal guidance, training and presentations;
- (b) Lesson planning
- (c) Conducting research
- (d) Developing code
- (e) Providing summaries
- (f) Idea generation
- (g) [List any other authorised use]

All other purposes must be authorised in advance by the Chief Information Officer.

Before using any AI applications, staff will be provided training to ensure human reviewers (those who conduct monitoring of these applications) have a correct understanding and do not add any bias into the AI systems.

Monitoring

We reserve the right to monitor all content on any AI applications used for business purposes. This will only be carried out by the school to comply with a legal obligation or for our legitimate business purposes in order to:

- (a) prevent misuse of the content and protect confidential information (and the confidential information of our pupils, staff or other stakeholders);
- (b) ensure compliance with our rules, standards of conduct and policies in force;
- (c) monitor performance at work;
- (d) ensure that staff do not use AI for any unlawful purposes or activities;
- (e) comply with legislation for the protection of intellectual property rights;

The Trust will also conduct monitoring under our IT and Communications Systems Policy and Bring Your Own Device to Work policy.

Breach of this policy

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 appropriate, disciplinary action may be taken whether the breach is committed during or outside normal work hours, whether or not the AI is used on an individual's own device or one of our devices, and whether at home, in the office, or from a remote working location.

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, whether or not this is an authorised application and any relevant passwords and login details.

You must report any breach of this policy immediately to the Chief Information Officer in the first instance. We advise referring to the Trust's current data breach policy, which can be found on the Trust's website.

Related Policies

Staff should refer to the following policies that are related to this AI Staff Policy: -

- Bring Your Own Device (BYOD) Policy
- Diversity, Equity and Inclusion Policy
- Code of Conduct and Ethics Policy
- Data Protection Policy
- Privacy Policy for staff.
- IT and any related communications policies

These are available on the Trust's website.