TIBSHELF COMMUNITY SCHOOL
ARTIFICIAL INTELEGENCE

Ratified: April 26
(DCC Policy)

Contents

Introduction
Scope and responsibility
Use of AI by Staff
Use of AI by Pupils
Potential misuse of AI and Risks
Data protection and AI
Cyber security and AI

Introduction

The purpose of this Artificial Intelligence (AI) Policy is to guide the ethical and effective use of AI technologies within the school environment. AI offers significant potential to enhance educational outcomes by: providing personalised learning experiences; improving teaching methodologies; and supporting administrative efficiency. At the same time, the risks that can be present when using AI dictate the need to have a policy and guidance on how the school should be using AI.

As AI becomes increasingly integrated into various aspects of education, it is essential to establish clear guidelines and practices that promote its beneficial use. Our AI Policy sets forth principles and procedures to ensure that AI is implemented in ways that align with our educational objectives, ethical standards, and legal requirements. Through this policy, we aim to foster a safe, equitable, and innovative learning environment that prepares our students for the future.

Scope and responsibility

This AI Policy applies to all AI-related activities and technologies used within our school. It will cover AI applications in: teaching; learning; administration; and student support services. The policy is relevant to all members of the school community, including: students; teachers; administrative staff; and external partners who choose to use AI in their roles.

The responsibility for implementing and overseeing this policy lies with the school's governing body overall and the Senior Leadership team to ensure the staff members in their teams read, understand, and follow this policy.

Teachers and staff are responsible for integrating AI into their practices following this policy's guidelines, while students and parents are expected to engage with AI tools responsibly.

Regular reviews and updates of the policy will be conducted to reflect technological advancements and feedback from the school community.
If you have questions about the use of AI within the school, please ask any of the following members of staff:

- Deputy Headteacher will act as the AI lead for the school, they will monitor the compliance of the AI use as well as provide and arrange training as and when is appropriate.

- Education Data Hub is the schools DPO, they will be responsible for advising and instructing about the responsibilities when personal data is incorporated.

- ICT team will provide technical support advice and guidance.

Use of AI by Staff

All use of AI by staff must be approved by Deputy Headteacher and align with the school's educational goals. Teachers should actively engage in professional development opportunities related to AI and contribute to a culture of continuous improvement. Additionally, staff should provide feedback on the effectiveness of AI tools to help refine and enhance their application within the school.

Staff members are encouraged to incorporate AI tools and applications to enhance teaching methods and administrative processes. AI can support personalised learning plans, automate routine tasks, and provide data-driven insights to improve educational

outcomes. Staff must receive adequate training to use AI technologies effectively and ethically, ensuring that they are familiar with the potential benefits and limitations of these tools.

Additionally, it is the responsibility of the staff member who is using AI to ensure that the content produced by the AI is of appropriate quality and accuracy.

Use of AI by Pupils

Parental consent is required for students to use AI applications that collect personal data. Teachers and staff will guide students in understanding the appropriate and ethical use of AI technologies, emphasising the importance of digital citizenship. Students should be encouraged to provide feedback on their experiences with AI tools, helping to ensure that these technologies are effective and beneficial to their learning.

Students are encouraged to utilise AI tools to support their learning, enhance their digital literacy, and prepare for future technological advancements. AI can offer personalised learning experiences, providing tailored content and support based on individual needs and progress. However, students must use AI responsibly, respecting the guidelines and data privacy considerations outlined in this policy.

Potential misuse of AI and Risks

While AI presents numerous benefits, there is also potential for misuse, which can have significant ethical and legal implications. Misuse of AI includes: using AI technologies to engage in unethical behaviour; infringe on privacy rights; or facilitate cheating and plagiarism. The school is committed to identifying and mitigating these risks through comprehensive guidelines, monitoring, and education.

Clear procedures will be in place to address any incidents of AI misuse. Students and staff are encouraged to report concerns or suspected misuse of AI technologies promptly. The AI Coordinator will investigate reported incidents, and appropriate disciplinary actions will be taken in accordance with the school's code of conduct. Education and awareness programs will be implemented to help the school community understand the potential risks and responsibilities associated with AI use.

AI also presents a range of risks that need to be carefully managed to ensure its benefits outweigh the potential drawbacks. Here are some of the most common risks associated with AI, along with explanations:

- Biases, AI systems learn from data, and if the training data includes biased information, the AI can perpetuate and even amplify those biases. This can lead to unfair treatment of individuals based on race, gender, age, or other protected characteristics.
- Hallucinations, AI hallucinations, also known as ‘hallucinations’, in the context of AI, particularly refer to instances where an AI system generates output that is not based on its training data or any real-world information, often producing incorrect, nonsensical, or fabricated responses.
- Lack of Transparency, Many AI systems, particularly those using deep learning, operate in ways that are not easily interpretable by humans, making it difficult to understand how decisions are made. This can be how they process the data or even where the data is stored.
- Security Vulnerabilities, AI systems can be vulnerable to attacks such as adversarial attacks, where malicious actors manipulate input data to deceive the AI system.
- Accuracy and Reliability, the quality of the data used to train and operate AI systems is crucial. Poor-quality data can lead to inaccurate or unreliable AI outputs.
- Data Privacy, AI systems often require large amounts of data, which can include sensitive personal information. Improper handling of this data can lead to privacy violations.

When using AI staff and students will need to keep these risks in mind and determine the appropriate methods to mitigate them.

Data Protection and AI

AI technologies often require the collection and processing of personal data, which raises important data protection considerations. Our school is committed to complying with the Data Protection Act 2018 (DPA) and the UK General Data Protection Regulation (UK GDPR) to safeguard personal data. Data minimization, anonymisation, and secure storage practices will be implemented to protect student and staff information.

When a new system that uses AI is considered for the school, the school will follow the guidance of bringing on new Controllers or Processors as stated in the data protection policy. Consent will be obtained from students and their guardians before any personal data is used in AI systems. Regular reviews and audits of data protection practices will be conducted to ensure ongoing compliance. Staff will be trained in data protection principles, and any data breaches or security incidents will be promptly addressed following established protocols.

Cyber security and AI

The integration of AI technologies in our school necessitates robust cybersecurity measures to protect against unauthorised access, data breaches, and cyber threats. A comprehensive cybersecurity framework will be established, including secure network infrastructure, regular security audits, and incident response plans.

Staff and students will receive training on cybersecurity best practices, including: password management; recognising phishing attempts; and safe internet use. The school will continuously update its cybersecurity measures to address emerging threats and vulnerabilities. By prioritising cybersecurity, we aim to create a safe digital environment that supports the effective and secure use of AI technologies in education.