STAFF PROTOCOL FOR SAFE AND SECURE USE OF AI

1. Introduction

The Trust recognises staff may choose to use approved AI systems to support their day-to-day working. Whilst AI offers significant benefits, it also brings an array of risks which require careful management.

Ivy Education Trust has created this protocol to outline essential guidelines for ensuring safe and secure use of AI. Your adherence to this protocol is crucial for safeguarding our school community, protecting data, and upholding professional standards.

The Trust will ensure you are provided with necessary training to understand and safely use AI.

It is your responsibility to read and comply with the following protocol when using our approved AI systems.

2. Key principles for responsible AI use

Prioritise Human Judgment
AI should assist, not replace human decision-making.

Staff must ensure that final judgments, particularly those affecting individuals, are made by humans. This approach allows AI to compliment your professional judgment and expertise rather than replacing them.

Fact-check and critically evaluate
Always fact-check and critically evaluate AI-generated content for accuracy, bias and discrimination before sharing or endorsing it, especially for external communication. AI content is not always accurate or appropriate and may contain inherent biases. Generative AI tools have limited regard for truth and can output biased or harmful information.

Transparency
Be transparent about AI-generated content by including clear labels or notes indicating AI assistance in documents, emails, presentations, and other outputs. Clearly marking AI-generated content helps build trust and ensures others are informed when AI has been used in communications or documents.

The Trust expects the following disclaimer to be used where AI has assisted you with a task:

This task/communication has been supported by AI tools in line with the Trust's Safe and Secure AI Protocol. All content is subject to human oversight and professional judgment.

Use approved systems
You must only use AI systems and AI accounts that have been approved and provided by the Trust for work purposes. These accounts are configured to comply with organisational security and oversight requirements, reducing data breach risks. Staff should ensure that any AI systems used in teaching or administration are vetted prior to implementation.

Should you wish to implement an AI system, you need to notify the Trust's DPO who will undertake a check of the system and seek advice from the data protection officer as required.

Training and development
Staff will receive necessary training and support to effectively integrate AI into their work, including professional development opportunities focused on AI tools and their ethical integration. The Trust will provide relevant training for staff and governors in the advantages, use of and potential risks of AI. Staff have a responsibility to identify their own training and development needs and communicate this with relevant staff within the school to seek support where required.

3. Data privacy and personal information risks

Do not input personal data
You must not input identifiable personal information into AI systems without authorisation and a proper legal basis to do so.

This includes full names, addresses, email addresses, phone numbers. Any information input to a generative AI system may not remain private or secure.

Avoid inputting special category data
Do not input special category information without appropriate authority and legal basis.

Special category data includes but is not limited to health, ethnicity, religion and safeguarding. These data categories require higher levels of care and security.

Entering special category data, or even non-special category data that infers it (e.g. postcode inferring race) is a risk. Children are considered vulnerable data subjects and any process involving their personal data is likely to be 'high risk', meaning that suitable safeguards must be in place.

Sensitive information risk
Do not input sensitive internal documents such as strategic plans, private or commercially sensitive contracts into third-party AI tools unless explicitly vetted and approved for that purpose.

Staff must always recognise and safeguard sensitive data.

Cyber-crime risk
Entering confidential information or personal data into AI system can contribute to a larger picture

that could be used to commit cyber-crime, such as voice impersonation or financial fraud.

Copyright and intellectual property
Take care not to infringe copyright or intellectual property (IP) conventions. This includes avoiding the use of IP, including that of learners, to train generative AI models without appropriate consent.

Deskilling risk
Be aware of the risk of deskilling yourself by over-relying on AI which can lead to automation bias or automation-induced complacency. Generative AI tools cannot replace the judgment and deep subject knowledge of a human expert.

4. Professional responsibility and accountability

Professional judgment
AI tools should complement your professional judgment and expertise; they must not replace them. You remain professionally responsible and accountable for the quality and content of any output generated by AI.

Comply with policies
Adhere to all relevant Trust and school policies, including this AI protocol, the staff IT acceptable use agreement, and data protection policies. Failure to comply could breach UK GDPR, data protection obligations and your employment contract.

Avoid unauthorised software
Do not install or attempt to install unauthorised AI systems on a trust/school device or alter settings on an issued device.

Professional conduct
All digital communications with students, parents and carers, and other members of the Trust community should be of a professional manner when assisted by AI. The communication should only be carried out using official Trust systems and devices.

5. Reporting concerns

Report incidents immediately
You must report or communicate any suspected misuse or concerns to the appropriate individual within the school immediately.

This includes incidents involving AI misuse, data breaches, or inappropriate outputs generated by AI. Instant reporting helps mitigate risks and facilitates a prompt response.

Escalation
If an incident involves any illegal activity or the potential for serious harm, it must be escalated through the Trust's safeguarding procedures. Where AI is used to support monitoring and incident reporting, human oversight must be maintained to interpret nuances and context that AI might miss.

Seeking advice and clarification

If you are unsure about the appropriate use of an AI tool, particularly regarding data privacy, compliance, or potential risks, seek advice from the designated GDPR lead who will liaise with the Trust's Data Protection Officer (DPO) accordingly.

DPIA Process:

For any AI system where personal data is being share, a Data Privacy Impact Assessment (DPIA) must be considered before implementing the system. You must refer the system to the designated GDPR Lead who will seek the appropriate advice from the DPO.

By following this protocol, we can collectively ensure that AI is used safely, ethically, and effectively to enhance learning and administrative processes in our Trust.

AMENDMENT RECORD

Date	Reviewed by	Nature of change	Next review due
5.5.2026	PHP Law/DPO/FAR Committee	New privacy notice.	January 2028 and as required.