Artificial Intelligence (AI) Policy

Contents

1.0 Purpose

This policy sets out how gbpartnerships will use Artificial Intelligence (AI) tools safely, responsibly, and in compliance with UK law, data protection requirements, and sector best practice. It aims to ensure that all AI systems used, procured, or developed by gbpartnerships are safe, lawful, ethical, environmentally responsible, and aligned with our organisational goals and values.

The policy also aims to articulate the desired behaviours of individual colleagues.

2.0 Scope

This policy applies to:

- All employees, contractors, and third-party partners working for gbpartnerships.

- Any use of AI systems or tools for business purposes, including (but not limited to) text-generation, image/video creation, data analysis, automation, and generative AI.

- All modalities of AI (text, vision, audio, structured data).

3.0 Governance & Roles

- **AI Taskforce:** Oversees policy development, sector intelligence, action planning, and impact measurement. Responsible for frequent reviews of approved tools. The AI taskforce is simultaneously accountable to the individual Boards of the divisions of gbpartnerships and the Quality Team. The AI taskforce will provide appropriate reports for the quarterly groupwide Quality meetings.

- **Data Protection Officer (DPO):** Approves tools for processing personal data, including any AI application, monitors GDPR compliance.

- **Quality Team:** Quarterly review of AI risk assessments, incidents, and policy updates. The Quality Team is accountable to the Executive Team.

4.0 Approved AI Tools

- Only company-approved tools may be used for work-related purposes and on any gbpartnerships owned device. CoPilot accessed via gbpartnerships Microsoft 365 licence is currently the only approved tool, (this can be accessed via MS Teams). Refer to how-to section on staff comms if you are unsure.

  - Note, CoPilot web/app version is prohibited as this is not within our Microsoft 365 enterprise security and data uploaded via the app is used to train the AI model. This would breach GDPR if any sensitive data is uploaded.

- Staff may propose the use of new/additional tools by tabling a request to the AI taskforce for consideration. The AI Taskforce will review the proposal and assess risks and benefits associated with the tool before making a recommendation on the tool's use to the Quality Team. In conjunction with the Sustainability Working Group, the risk and benefit assessment will include a review of the energy efficiency of the proposed model and its associated cloud provider.

- Do not use unapproved or personal AI tools for any work-related task or on a gbpartnerships owned device. Use of unauthorised tools exposes gbpartnerships to serious risk, and breach of this policy may lead to a disciplinary process.

5.0 Responsible Use Rules

- **Protect confidential data:** Never enter customer names, financial information, personal data, or commercially sensitive material into public AI tools. CoPilot is the only authorised tool for gbpartnerships, when accessed via Microsoft 365 licence via MS Teams. Whilst Copilot does not use the data entered into it to train its model, it is expected that staff will still apply due diligence when entering any data of a sensitive nature into Copilot. If there is any doubt, staff are to consult with the DPOs prior to entering information.

- **Check accuracy:** AI output must be reviewed by a human before use or publication. Review and edit all AI-generated content; label drafts "AI-assisted" until verified.

- **Transparency:** Disclose AI use where outputs materially influence decisions.

- **Respect copyright:** Do not use AI to generate or reuse content that infringes intellectual property rights.

- **Avoid bias and harm:** Do not use AI to make automated decisions about people or groups.

6.0 Data Protection & GDPR

- Personal data must only be used with AI tools that comply with UK GDPR and are approved for use by gbpartnerships. Please refer to the gbpartnership GDPR Policy for definitions of personal data. To the furthest extent possible, personally identifiable data should be anonymised prior to being entered into AI models.

- Any proposed processing of client-provided data needs to be detailed and approved by the client before action.

- The DPO must approve any tool that processes personal data.

- Staff must immediately report any suspected data loss, leak, or unauthorised disclosure to the DPO immediately. Serious incidents are notified to the Information Commissioner's Office (ICO) within 72 hours.

7.0 Risk Classification & Approval Workflow

For any use of AI, staff are expected to assess the risk, and categorise as one of the three following levels:

- **Minimal/Limited Risk:** Productivity tools (e.g. grammar correction). Self-service approval if data is non-sensitive.

- **High Risk:** Affects hiring, healthcare, financial decisions. Requires DPIA, model card[1], Board sign-off, and human-in-the-loop.

- **Unacceptable Risk:** Manipulative techniques, real-time biometric categorisation. Synthetic media representing real individuals without consent. Prohibited.

8.0 Other Suggested Reading

- EU AI Act (2024)

- UK ICO "AI & Data Protection" Guidance (2023)

- NIST AI Risk Management Framework 1.0 (2023)

- ISO/IEC 42001 (2024)

- NHS Code of Conduct for Data-Driven Tech (2022)

- NICE Evidence Standards Framework v2.2 (2023)

---

[1] **A model card** is a short, structured document that provides key information about a machine learning (ML) model to promote transparency and responsible AI development. It typically includes the model's intended uses, limitations, and performance metrics, along with details about the data used for training and evaluation, and any relevant ethical considerations, and performance metrics, along with details about the data used for training and evaluation, and any relevant ethical considerations.

- Algorithmic Transparency Recording Standard (Cabinet Office, 2023)

9.0 Documentation Control

Document Details	
Version	1.0
Reference	P89
Policy Prepared by	AI Taskforce
Approved by	Quality Team
Date of Approval	January 2026
Operational From	January 2026
Review Date	July 2026

Appendix A

Approved tools for use by gbpartnerships

- CoPilot accessed via gbpartnerships Microsoft 365 licence

Approved transcribing tools which may be used by third parties

- Microsoft Teams' built in functionality

Banned tools for use by gbpartnerships

- This list is not exhaustive and approval should be sought from Quality team prior to using any form of AI for work purposes.
- Any AI tool that is used to train an AI model is banned
- CoPilot web/app version is prohibited as this is not within our Microsoft 365 enterprise security and data uploaded via the app is used to train the AI model. This would breach GDPR if any sensitive data is uploaded.
- Chat GPT
- Deepseek

Banned transcribing tools which may be used by third parties

- Current status is for all staff to decline any tool other than Microsoft Teams' built in functionality