



Artificial Intelligence (AI) Policy

Contents

1.0 Purpose	3
2.0 Scope	3
3.0 Governance & Roles	3
4.0 Approved AI Tools	3
5.0 Responsible Use Rules	4
6.0 Data Protection & GDPR	4
7.0 Risk Classification & Approval Workflow	5
8.0 AI-Assisted and Automatable Processes	5
9.0 Other Suggested Reading	5
10.0 Documentation Control	6
Appendix A	6

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:** The AI Taskforce is accountable to the IT Strategy Committee and monitors implementation guidance on Data (Use and Access) Act 2025 as it matures.
- **Data Protection Officer (DPO):** Approves tools for processing personal data, including any AI application, monitors GDPR compliance, reviews and signs off any applicable Transfer Risk Assessments and Data Protection Impact Assessments.
- **IT Strategy Committee:** Approves AI software and shared company wide/departmental agents suggested/developed by AI Taskforce, and 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.
- Approved tools:
 - CoPilot accessed via gbpartnerships Microsoft 365 licence, (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.
 - Claude AI, by assigned seat
- 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 IT Strategy Committee. 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 commercial and regulatory 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, when accessed via Microsoft 365 licence via MS Teams, and Claude AI are currently the only authorised tools for gbpartnerships. Whilst neither of these tools 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. 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.
- **Client disclosure:** Consider to what extent AI may be utilised on client work and ensure this is reflected in the engagement.
- **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. Human review and the right to challenge must always be available (UK GDPR Article 22; Equality Act 2010).
- **Staff training:** All staff must complete AI awareness training before using approved tools, covering data protection, recognising inaccurate outputs, and escalation.

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.
- **Data subject rights:** UK GDPR rights apply in full to AI-processed data, including the rights of access, erasure, and objection. Do not use AI in a way that prevents gbpartnerships from honouring those rights. Escalate any data subject request involving AI-processed data to the DPO.
- **Data quality:** AI outputs are only as reliable as the data entered. Do not use outdated or unverified data and do not treat AI outputs as fact without checking, particularly for client advice or regulatory submissions.
- **AI incident reporting:** Report AI incidents to the AI Taskforce, not only data breaches. This includes materially incorrect outputs, suspected bias, undisclosed AI

use affecting a deliverable, and unexpected tool behaviour. The Taskforce escalates significant incidents to the IT Strategy Committee.

7.0 Risk Classification & Approval Workflow

gbpartnerships operates as a **Deployer** under the EU AI Act, using AI systems from third-party providers. The Act applies where our outputs affect EU individuals, regardless of our UK base. As Deployer we must use tools as the provider intends, maintain human oversight, and carry out fundamental rights impact assessments for High Risk uses. The AI Taskforce must monitor provider compliance communications as the Act phases in.

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, Conformity Assessment, model card¹, IT Strategy Committee 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 AI-Assisted and Automatable Processes

The following processes are suitable for AI assistance, subject to Sections 5.0 and 7.0. A human must review all AI outputs before use.

- **Document drafting and editing:** First drafts of reports, proposals, bids, policies, job adverts, and correspondence; also proofreading, summarising, and reformatting. Human review required before use.
- **Meeting transcription and summarisation:** Teams transcription (the only approved tool) generates transcripts; AI may then summarise or extract actions. Participants must be informed. Transcripts with personal data must be handled per the GDPR Policy.
- **Data analysis and management reporting:** AI may assist with financial analysis, management accounts, data manipulation, and reporting (e.g. Power BI, Excel). Outputs informing board or client decisions require validation by the responsible lead.
- **Research and market intelligence:** AI may assist with research, horizon scanning, and competitor analysis. Verify all AI-generated facts and statistics before use; AI can produce plausible but inaccurate information.
- **Proposing new AI use cases:** Staff may propose new AI use cases to the AI Taskforce, covering the current process, proposed approach, data involved, and expected gain. The Taskforce assesses feasibility and compliance before recommending to the IT Strategy Committee.

9.0 Other Suggested Reading

- Data (Use and Access) Act (2025)

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.

- Data Protection Act (2018)
- 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)
- Algorithmic Transparency Recording Standard (Cabinet Office, 2023)
- Equality Act (2010)
- Freedom of Information Act (2000)

10.0 Documentation Control

Document Details	
Version	2.0
Reference	P89
Policy Prepared by	AI Taskforce
Approved by	IT Strategy Committee
Date of Approval	July 2026
Operational From	July 2026
Review Date	January 2027

Appendix A

Approved tools for use by gbpartnerships

- CoPilot accessed via gbpartnerships Microsoft 365 licence
- Claude AI (Anthropic), by assigned seat only

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 AI Taskforce prior to using any form of AI for work purposes. This includes any software which has AI built into the platform.
- Any AI tool that is used to train an AI model is banned
- Free 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