Artificial Intelligence Usage Policy **2026**

Artificial Intelligence (AI) has tremendous potential to help a mid-market business. However, there are potential legal, ethical, and privacy issues. That's why you need a corporate IT usage policy – a set of guidelines that both illuminates potential risks and provides a clear framework for problem-solving.

The right IT usage policy will help your business:

- Comply with legal and regulatory standards
- Encourage ethical and responsible use of AI
- Ensure data privacy
- Prevent bias and discrimination

We provided this AI usage policy template to help you craft a policy for your own business. You are free to edit or simply add your company name in the <appropriate field>.

The information provided in this AI Usage Policy document does not, and is not intended to, constitute legal advice; this document is for general informational purposes only. With respect to any particular legal matters raised by your company's use of AI, consult a lawyer.

FREEMAN CLARKE

The largest and most experienced team of IT leaders

www.freemanclarke.com

1. Purpose

This policy sets out how Artificial Intelligence (AI) tools can be used responsibly and safely within <organisation>. The aims are to support productivity and innovation, reduce risks, ensure ethical and compliant use, and promote transparency and accountability. It applies to all forms of AI, including generative AI, machine learning systems, automation technologies, and AI-assisted software.

2. Scope

This policy applies to all employees, contractors, temporary staff, and third parties. It covers all AI tools used for work purposes, whether accessed through organisation-owned devices or personal devices used for work. It applies to any situation where AI tools influence decisions, content, processes, or outcomes.

3. Permitted uses

AI tools should be on an approved list or explicitly authorised. If on the list, AI tools may then be used when they support legitimate business activities and improve productivity, creativity, or analysis. They may be used to create draft content that is reviewed by a human, to support research, summarisation, or planning, and to automate routine tasks. Even with approved tools, AI must not be used with sensitive or personal data unless this has been agreed in advance.

Examples of acceptable use include drafting internal or marketing content, generating ideas or summaries, automating administrative processes, analysing non-confidential information, and supporting customer service or internal operations.

4. Prohibited uses

AI must not be used for the following:

- Uploading or processing personal data without a proper legal basis and approval
- Uploading confidential, sensitive, or commercially valuable information into external AI tools
- Replacing human judgement in critical or legally significant decisions, including hiring, performance reviews, legal work, financial analysis, or safety-related decisions
- Producing content that is misleading, harmful, discriminatory, or unethical
- Creating deepfakes or impersonating individuals
- Activities that infringe copyright, licensing, or intellectual property rights
- Personal projects using <organisation> devices or accounts
- Any task whatsoever, if the AI being used is an unapproved or unverified system, website, app, extension, or browser plugin

5. Ethical use principles

AI use must follow the principles below.

- **Fairness:** Avoid generating or using outputs that are biased or discriminatory
- **Transparency:** Clearly identify when content has been created or significantly assisted by AI, especially when shared externally
- **Accountability:** Humans remain responsible for the accuracy and appropriateness of all outputs and decisions
- **Accuracy and quality:** AI-generated content must be reviewed and verified by a human before use or publication
- **Respect for intellectual property:** Do not enter copyrighted or proprietary material into AI tools without permission

6. Data, privacy and security

Users must protect organisational and personal data when using AI tools. Personal, confidential, or sensitive data must not be entered into external AI systems unless explicitly approved and in a legally compliant manner. AI tools must comply with relevant data protection laws such as UK GDPR, EU GDPR, or regional equivalents. Users should understand how each AI tool stores, processes, and retains data. Only tools with transparent data handling and acceptable security practices should be used. <Organisation> should keep records of the AI tools in use, along with permitted usage for these tools, and review regularly.

7. Tool approval and procurement

New AI tools must be assessed for risk before using. The assessment should cover security, compliance, data handling, and reliability. Licensing terms and provider guarantees must also be reviewed.

Only approved tools should be used for business purposes. Free or unverified AI tools should not be used unless formally authorised.

8. Training and awareness

<Organisation> should provide training on safe, ethical, and compliant AI usage. Staff should receive guidance on identifying risks, biases, and inaccurate outputs. Training should cover how to review AI-generated content responsibly. Updates should be shared as technology and regulation evolve. Staff are responsible for understanding the risks associated with AI and following this policy.

9. Monitoring and accountability

<Organisation> may monitor the use of AI tools to ensure compliance. AI-related risks should be reviewed as part of broader risk management. Approved tool lists should be updated as technologies develop. AI systems may be audited for accuracy, fairness, and security. Responsibility for oversight may sit with IT, HR, Compliance or other leadership depending on organisational structure.

10. Incident reporting

Users must promptly report any of the following:

- Accidental input of personal or sensitive data into an AI tool
- Outputs that appear biased, harmful, or inappropriate
- Unexpected or unsafe behaviour from an AI system
- Security incidents or suspected misuse of data
- Complaints or concerns raised by clients or external parties regarding AI usage

Reports should be made to <organisation's> nominated contact, such as IT or a Data Protection Officer.

11. Consequences of non-compliance

Breaches of this policy may result in disciplinary action in line with <organisation's> HR procedures. Serious misuse may also lead to legal or regulatory consequences.

12. Review and updates

This policy should be reviewed at least annually and whenever there are significant regulatory or technological changes. It should also be updated following any AI-related incident.

13. Glossary

- **Artificial Intelligence (AI):** Technologies that perform tasks requiring human-like intelligence
- **Algorithm:** Rules or instructions used to process data or solve problems
- **Automation:** Use of AI or software to complete tasks without human intervention
- **Big data:** Large datasets analysed to identify patterns or insights
- **Chatbot:** Software that simulates human conversation
- **Cognitive computing:** Systems that mimic human reasoning and learning
- **Data analytics:** Examination of data to extract insights
- **Deep learning:** Machine learning using multi-layered neural networks
- **Generative AI:** AI that creates new content such as text, images, or code
- **Large language model (LLM):** AI trained on large text datasets to produce human-like outputs
- **Machine learning (ML):** AI that learns from data to improve performance
- **Natural language processing (NLP):** AI that understands and generates human language
- **Neural network:** Computational model inspired by the structure of the human brain
- **Predictive analytics:** Using data to forecast outcomes
- **Reinforcement learning:** AI that learns through trial and error
- **Robotic process automation (RPA):** Software for automating repetitive tasks
- **Supervised learning:** Machine learning using labelled data
- **Unsupervised learning:** Machine learning that identifies patterns in unlabelled data

14. Linked documents

The Artificial Intelligence Usage Policy is within the <organisation> policy suite and is related to the following policies:

- Data Protection Policy
- Information Security Policy

15. Additional considerations

Every business is different. Some industries have stricter privacy and data compliance regulations than others. These should always be taken into account.

It is good practice for every business to maintain a risk register at Board level. Good use of AI, and how to mitigate for the risks of compliance issues should be considered as part of that process.

Version Control

Track your changes to the policy here.

Version	Date	Author	Summary of Changes
0.9	1 January 2026	Freeman Clarke	Template Policy Creation