

AI usage policy template

This template is designed to help small businesses create an AI policy tailored to their operations.

It provides general guidance only and should not be considered financial, legal, cyber security, IT or professional advice. You should adapt it to reflect your business's circumstances, requirements and AI risks, and seek independent professional advice where appropriate. The controls included within your policy should be proportionate to the nature, size and AI risks of your business. You remain responsible for deciding whether the completed policy is suitable for your business and compliant with any applicable legal or regulatory requirements.

Completion of this template does not guarantee protection against AI-related incidents and does not in itself affect the availability, terms or operation of any insurance policy. Markel Direct will not review, verify or approve policies completed using this template and does not accept responsibility for decisions made based on its contents.

Review the completed policy regularly to ensure it remains appropriate for your business, technology and AI risks.



MARKEL

Document information

Business name: _____

Policy owner: _____

Date implemented: _____

Review date: _____

Policy version: _____

Policy purpose and scope

Use this section to explain why your organisation needs an AI policy and who and what it covers.

Consider the benefits you want to achieve and the risks the policy is intended to manage, such as inaccurate outputs, confidential information, personal data, copyright and reputational risk.

Who does this policy apply to?

☐ Employees

☐ Directors

☐ Contractors and freelancers

☐ Temporary workers

☐ Volunteers

☐ Suppliers or third parties using AI on your behalf

☐ Other: _____

List the teams, processes, products, services and AI-enabled features covered by this policy.

PAGE 2

Approved AI tools

List the AI tools approved for work purposes. Include AI features built into existing software, not only standalone platforms.

Tool/provider	Approved users	Approved purpose	Account/version	Restrictions
Example: [tool name]	Example: Marketing team	Example: Brainstorming and first drafts	Example: Business account	Example: No personal or confidential data

Approval process for new tools:

Who will assess requests? What security, privacy, contractual, data-handling and licensing checks must be completed before a tool is approved?

☐ Unapproved AI tools must not be used for work.

☐ Employees must use approved business accounts where specified.

☐ Employees must follow any tool-specific restrictions listed above.

☐ Other requirement:

Permitted and prohibited uses

Select the activities your organisation permits, then add any conditions or approval requirements.

Permitted uses:

- ☐ Brainstorming and idea generation
- ☐ Creating outlines or first drafts
- ☐ Proofreading or improving clarity
- ☐ Summarising non-sensitive information
- ☐ Research support, subject to source verification
- ☐ Creating images, audio or video
- ☐ Writing or reviewing code
- ☐ Analysing approved data
- ☐ Other: _____

Conditions that apply to permitted uses:

For example: manager approval, approved data only, use of a business account, or mandatory review before publication.

Prohibited uses

- ☐ Making final legal, financial, regulatory, employment or safety-critical decisions without appropriate human review
- ☐ Impersonating a person or misleading others about the origin of content
- ☐ Creating unlawful, discriminatory, offensive or deceptive material
- ☐ Circumventing security controls or access restrictions
- ☐ Uploading information restricted on page 5
- ☐ Using AI output as a verified source without checking it
- ☐ Relying on AI-generated legal, regulatory, tax, employment or professional advice without appropriate verification from a suitably qualified individual
- ☐ Other: _____

Data protection and information handling

Identify information that must not be submitted to AI tools unless its use has been expressly authorised and appropriate safeguards are in place. This includes information that is entered, uploaded, pasted or spoken.

- ☐ Customer, client, beneficiary or supplier personal data
- ☐ Employee or applicant personal data
- ☐ Special category personal data or criminal offence data
- ☐ Financial account, payment card or banking information
- ☐ Passwords, authentication codes, security keys or access credentials
- ☐ Confidential customer or client information
- ☐ Contracts, legal advice or legally privileged material
- ☐ Non-public financial information, forecasts or pricing
- ☐ Trade secrets, proprietary methods, source code or product designs
- ☐ Unpublished content or copyrighted material the business does not have permission to use
- ☐ Security vulnerabilities, incident details or system configurations
- ☐ Other: _____

Additional requirements:

List any organisation-specific data classifications, client restrictions or contractual obligations. Where personal data is processed using AI tools, organisations should consider their UK GDPR obligations, including lawful basis, transparency requirements, contractual arrangements with providers and any international data transfers.

Authorisation and safeguards:

State who can approve exceptions and what controls must be used. Consider access, retention, deletion, provider use of inputs and outputs, international transfers and record keeping.

Human oversight and output review

Define the level of review required before AI-assisted work is used, submitted, published or shared.			
Output or activity	Required checks	Reviewer/approver	Evidence to retain
Internal low-risk draft	Accuracy, relevance and confidentiality	Author/employee	As required
Customer-facing content			
Professional advice or technical output			
Legal, regulatory or compliance-related material			
Data analysis or business decision support			
Images, audio, video or code			
Other			

Minimum review checks:

- ☐ Accuracy and completeness
- ☐ Sources and references
- ☐ Bias, fairness and inappropriate content
- ☐ Confidentiality and personal data
- ☐ Copyright, trade marks and other intellectual property
- ☐ Applicable legal, regulatory and contractual requirements
- ☐ Brand, tone and accessibility
- ☐ Security risks, including unsafe code or links
- ☐ Other: _____

Accountability and responsibilities

Role	Named person/position	Responsibilities
Policy owner		Maintain and review the policy; coordinate approvals and guidance.
AI tool approver		Assess and approve tools and restrictions.
Data protection/security contact		Advise on data handling and incidents.
Managers		Ensure teams understand and follow the policy.
Employees and other users		Follow the policy and remain responsible for work they submit, approve or share.
Other		

Final accountability statement:
State clearly who holds responsibility for the accuracy, legality, quality and suitability of AI-assisted work.

Copyright and intellectual property

- ☐ Check AI-generated content for similarity to existing protected material.
- ☐ Confirm that licences and provider terms allow the intended use.
- ☐ Verify rights and permissions for generated images, audio, video, code and other assets.
- ☐ Do not upload the organisation’s intellectual property unless authorised.
- ☐ Record material use of AI and provide attribution where required by the organisation, contract or platform.
- ☐ Escalate uncertainty to: _____

Organisation-specific IP requirements:
Set out approval, attribution, originality-checking and record-keeping requirements.

Incident reporting and response

Anyone covered by this policy should promptly report suspected or confirmed AI-related incidents.

Incident contact	Details
Name	
Role	
Telephone	
Email or reporting channel	
Alternative contact	
Other	

Examples of incidents to report:

- ☐ Personal, confidential or commercially sensitive information submitted to an AI tool
- ☐ Inaccurate or fabricated content shared or relied upon
- ☐ Discriminatory, offensive, unsafe or otherwise problematic output
- ☐ Suspected copyright, trade mark or intellectual property infringement
- ☐ Unauthorised or unapproved AI use
- ☐ Security concern, malicious prompt, unsafe code or unexpected disclosure
- ☐ Customer complaint or potential professional error involving AI
- ☐ Other: _____

Response stage	Responsible person	Required actions
Stop or limit further use		
Preserve relevant records		
Assess the information and identify people affected		
Notify internal specialists or external advisers		
Correct, withdraw or contain the output		
Consider required notifications		
Review lessons learned and controls		

Insurance and risk management

Review your insurance arrangements to understand whether AI-related activities and liabilities may be covered and, if so, to what extent. Cover will depend on the terms, conditions and exclusions of each policy.			
Insurance arrangement	Provider/policy number	AI-related considerations reviewed	Review date/contact
Professional indemnity			
Cyber insurance			
Directors' and officers' insurance			
Technology or other specialist cover			
Other			
<div>Disclaimer: The existence or completion of this AI policy does not confirm that an AI-related claim will be covered. Discuss your circumstances and activities with your insurance adviser or insurer.</div>			

Training and awareness

- ☐ On induction
- ☐ Before access to approved AI tools
- ☐ Annually
- ☐ When tools or rules materially change
- ☐ Following an incident
- ☐ Role-specific training
- ☐ Other: _____

Training content and records:
Who will provide the training, what must it cover and where will attendance or completion be recorded?

Policy review and approval

☐ Annually

☐ After an AI-related incident

☐ When a new AI tool or material use is introduced

☐ Following a significant legal, regulatory, contractual or business change

☐ Other: _____

Approval	Details
Approved by	
Position	
Signature	
Date	
Next review date	

Final implementation checklist

☐ Approved AI tools and account types have been documented.

☐ Permitted and prohibited uses are clear.

☐ Restricted data and information have been identified.

☐ Human review requirements and approvers have been assigned.

☐ Final accountability is clear.

☐ Copyright and IP checks have been defined.

☐ Incident contacts and response steps are complete.

☐ Relevant insurance arrangements have been reviewed.

☐ Employees and other users have received a copy of the policy and completed the necessary training.

☐ The policy has been approved, dated and scheduled for review.

Additional actions before launch:

Record any outstanding decisions, owners and target dates.

Employee acknowledgement:

I confirm that I have read and understood this AI policy and agree to follow its requirements.

Name	Signature	Date



Discover help and guidance for small businesses and self-employed professionals in our [knowledge centre](#) and read more about our [small business insurance solutions](#).

Markel Direct
82 King Street, Manchester, M2 4WQ
T: 0800 640 6600 W: www.markeluk.com

