

[Company name] AI acceptable use policy

Policy owner: [name or role and contact]

Approved by: [name or role] | Effective date: [date] | Next review: [date]

Approved tools and uses: [link to your AI tool register]

This policy applies to everyone using AI for [Company name] work. We use AI to support useful work while protecting company information and keeping people responsible for the results.

1. Approved tools and uses

Use only the tools, account plans and tasks in our approved AI tool register. Ask the policy owner before adopting a new tool, adding an integration or starting a paid subscription. Approval for one task or type of information does not cover every use.

2. Protect information

Never enter passwords, API keys or other access secrets. Use personal, client or confidential information only where the tool and task are explicitly approved for that type of information. Follow our existing privacy, security and client requirements. If unsure, use public or fictional material and ask before uploading.

3. Accounts and automated actions

Use company-approved work accounts and settings for company work. Do not use personal AI accounts. Get approval before giving an AI agent or integration access to company systems, and keep its access and actions within the agreed scope.

4. Check the result

The person using AI is responsible for the final work. Check important facts, sources, calculations, code and rights before relying on or sharing output. Consequential decisions about people need a separately approved process and accountable human review.

5. Be open about AI use

Disclose material AI assistance when it matters to the recipient, is required by a client, or falls under [company disclosure rule]. Do not present unverified AI output as checked expertise or another person's original work.

6. Report problems and hand over work

If information is shared incorrectly, an output is unsafe, or an agent acts unexpectedly, stop the affected activity and report it promptly to [incident contact or reporting route]. When someone leaves or changes role, hand over shared work, remove access through our leaver process and review subscriptions and integrations.

7. Keep the policy current

The policy owner maintains the approved tools register, answers questions and arranges a review by the date above, or sooner after a significant tool, use or risk change. Everyone using AI must read this policy and follow updates.