

AI ACCEPTABLE-USE POLICY

Editable internal policy template for businesses, accountants and bookkeepers

HOW TO USE THIS TEMPLATE

Replace all [bracketed text]. Approve the policy at owner/director/partner level, link it to the approved-tool register, and issue it with practical staff training. A written policy does not replace supplier checks, account controls or incident procedures.

1. Purpose

This policy sets the rules for using generative AI and other AI-enabled tools in [Business/Practice name]. Its purpose is to protect confidentiality, personal data, professional judgement and work quality while allowing proportionate, approved use.

2. Scope

- Applies to directors, partners, employees, contractors, temporary staff and anyone using business information or systems.
- Covers standalone AI services, AI functions built into software, browser extensions, meeting assistants, transcription tools, document assistants, coding tools and connected agents.
- Applies whether the tool is free, paid, personally subscribed, supplied by the business, or included within another product.

3. Core rules

Rule	Required behaviour
Use approved tools only	Use only the product, plan, workspace and use case recorded as approved.
Protect information	Do not enter confidential, personal or sensitive information unless that exact use has been approved for that data.
Use managed accounts	Use business-managed sign-in/workspaces. Personal accounts must not be used for business work unless specifically authorised.
Human review	A competent person remains responsible for the output. Check facts, calculations, sources, assumptions and wording before use.
Record material use	Keep proportionate evidence where AI contributes materially to client/customer work or an internal decision.
Escalate mistakes	If information is shared with the wrong service or audience, stop further sharing and report it immediately. Do not conceal or silently erase evidence.

4. Risk bands

Band	Typical examples	Default position
GREEN	Public technical research; generic formulas; fictional text; public information.	Permitted only in an approved tool. Accuracy check required.
AMBER	Pseudonymised working notes; de-identified process data; generic customer/client patterns.	Use only after checking re-identification risk, settings and approval.
RED	Named client/customer records; payroll; bank data; tax returns; ID; health; disputes; privileged material; passwords.	Do not enter into public or unapproved AI. Use only where exact tool/use/data configuration is specifically authorised.

IMPORTANT

Pseudonymised information is not necessarily anonymous. Replacing a name with 'Client A' does not by itself remove confidentiality or UK GDPR considerations.

5. Permitted uses

- Explaining generic spreadsheet formulas or software concepts without confidential data.
- Summarising public guidance for later human verification.
- Drafting or improving generic internal procedures.
- Rewriting fictional or already-public text for tone or readability.
- Generating non-specific checklists or training examples.

6. Prohibited uses

- Uploading confidential files, bank statements, payroll data, tax returns, ID documents, working papers or private correspondence to an unapproved AI service.
- Using personal AI accounts, personal browser extensions or unapproved integrations for business work.
- Relying on AI as the final accounting, tax, payroll, legal, data-protection or other professional conclusion without competent review.
- Allowing AI to send material external communications, submit filings, make payments or change records without authorised controls and review.
- Entering passwords, access tokens, recovery codes or other authentication secrets.
- Concealing an AI-related error, data incident or unapproved use.

7. Approval of tools and use cases

- Record the business purpose, exact product/plan/workspace, data involved and owner.
- Check supplier terms, data-processing position, retention, training/evaluation use, deletion, subprocessors, processing locations and account controls.
- Record the DPIA decision where relevant.
- Assign Approved, Restricted, Pending or Prohibited status.
- Review at least [quarterly/annually] and after material supplier or feature changes.

8. Accounts, access and configuration

- Use business-managed sign-in and MFA where available.
- Apply least-privilege access and remove leavers promptly.
- Disable model-training/content-improvement use where the supplier provides that control and the business requires it.
- Restrict public sharing, connectors and integrations unless specifically approved.
- Do not connect mailboxes, drives, accounting systems, CRMs or client portals to AI without documented approval.

9. Human review

- Check source material rather than accepting citations at face value.
- Reperform or independently verify calculations affecting material work.
- Check that law, tax rates, deadlines and professional guidance are current where relevant.
- Remove invented, unsupported or irrelevant content.
- Ensure the final work is suitable for the purpose and consistent with the engagement or instruction.

10. Recordkeeping

- Purpose and approved tool/use case.
- Relevant prompt or input summary where appropriate.
- Output relied upon and source material checked.
- Reviewer, corrections and final conclusion.

11. Expectations and confidentiality

- Follow contracts, engagement terms, privacy information and specific client/customer instructions.
- Record and operationalise a restriction on AI use with a person's or client's information.
- Do not assume a general contract or engagement authorises every new AI-enabled processing activity.
- Escalate uncertainty about confidentiality, transparency or supplier role before use.

12. Incidents

- Stop further sharing and preserve key evidence.
- Notify [AI owner/privacy lead/director/partner] immediately.
- Record what left, where it went, who could access it and what happened next.
- Submit an urgent vendor deletion/incident request where appropriate.
- Complete the business breach-risk and notification assessment; document the decision.
- Apply corrective action before closure.

13. Roles

Role	Responsibility
Policy owner	Maintains the policy, register, review cycle and training.
Approving director/partner/manager	Approves/prohibits tools, use cases and significant exceptions.
Users	Follow approved uses, review outputs and escalate mistakes immediately.
Privacy/DPO lead	Supports data-protection assessments, incidents and notification decisions where applicable.
IT/security	Supports identity, access, configuration, logs, integrations and containment.

14. Breaches of this policy

Unapproved use may result in restriction of access, retraining, investigation or disciplinary action under [Business/Practice name]'s procedures. The priority after an error is prompt containment and accurate reporting.

15. Review and approval

Field	Completion
Business / practice	[Name]
Policy owner	[Name / role]
Approved by	[Director / partner / manager]
Effective date	[DD/MM/YYYY]
Next review	[DD/MM/YYYY]
Related documents	Approved-tool register; incident record; privacy notice; relevant engagement/IT/security policies

TEMPLATE STATUS

General information and an adaptable internal template, not legal, data-protection or professional advice. Review for your operations, suppliers, employment procedures and regulatory obligations.