The approved AI tools policy: a guide, then the template

Most AI incidents in small firms trace to one gap: staff using tools nobody approved, because no approved alternative was named. This guide walks you through writing the one-page policy that closes the gap, then gives you the fill-in pages.

01 Why a policy, and why one page

Your staff already use AI, whether or not a policy exists; the risky usage is the invisible kind in personal accounts. A short, generous policy with a fast route for proposing new tools brings usage into the light. A ban drives it underground. One page is enough, provided it is enforced and reviewed; ten pages nobody reads is worse than none.

Start with an amnesty, not an audit: ask everyone what they already use, without blame, on day one. The answers are your first register entries, and the goodwill is worth more than the surprise.

02 The six decisions your policy must record

Each decision below is what the fill-in page at the back asks for. Take them in order.

1. Who owns it

One named senior person, not a committee. They approve new tools, review the register, and answer for it. In a regulated firm this maps to an existing accountability holder.

2. Which tools are approved, on which tiers

Name the exact product AND tier: "ChatGPT Team" is approved; "ChatGPT" is not a decision. Business tiers matter because they carry the commitments that protect you: no training on your data, admin controls, contractual terms. Free consumer tiers generally carry none of these.

3. The one rule

Suggested wording, used by real firms: "Client personal data may only be entered into tools on the approved register, on business terms. It must never be entered into personal or free accounts of any AI tool." Most incidents this policy exists to prevent are a violation of exactly this sentence.

4. What each tool may be used for

Per tool, one line of approved uses and any forbidden ones. Example: "Claude Team: drafting, summarising, document review. Not for final advice sign-off." Keep it honest and short; the register holds the detail.

5. How staff propose a new tool

A fast, named route: "Email the owner with the tool, the tier, and what you want to use it for; answer within a week." If proposing takes longer than sneaking, staff will sneak.

6. When it gets reviewed

Quarterly is the working default: tools change tiers and terms faster than annual review catches. Put the first review in the diary the day the policy is approved.

03 The regulations that may apply to you

You do not need to be a lawyer to write this policy, but know which regimes are in play so nothing in it contradicts them.

UK GDPR and the Data Protection Act apply to every UK firm the moment client personal data enters any AI tool: you need a lawful basis, a processor agreement with the vendor, and, for most client-data uses, a data protection impact assessment (our DPIA starter template covers this). The Data (Use and Access) Act 2025 changed the rules on automated decisions from February 2026: decisions made about people without meaningful human involvement need specific safeguards.

FCA-regulated firms carry the existing framework: the Consumer Duty makes the firm own AI-assisted outcomes, the Senior Managers regime puts a named person on the hook, and record-keeping rules extend to AI-assisted client outputs. There is no separate AI rulebook, which means these apply now, not at some future date.

Professional duties bite regardless of sector: solicitors' confidentiality and duties to the court, accountants' professional standards, and every firm's duty of competence extend to AI-assisted work unchanged. If you serve EU-resident clients, EU rules travel with the client: GDPR, and the EU AI Act's transparency obligations, live since August 2026.

The knowledge base at cordrey.co/knowledge carries plain-English guides to each of these, by jurisdiction and firm type.

04 A worked example

A fictional 12-person advice firm's completed policy, to show the size and register shape to aim for. Yours will differ in content, not in shape.

POLICY (one page): "Owner: Sarah Okafor (Operations Director). Approved tools: ChatGPT Team (drafting, summarising, internal analysis; not client advice); Claude Team (long documents, report drafting; not client advice); Copilot for Microsoft 365 (email, meetings, documents); Otter Business (meeting transcription, with client notice). The one rule: client personal data only ever in the tools above, on our business accounts, never in personal or free accounts. Proposing a tool: email Sarah with tool, tier and intended use; answer within five working days. Reviewed quarterly; next review 1 December 2026."

REGISTER (one row per tool): "Claude Team | training on our data excluded per Anthropic commercial terms, confirmed in writing 12 Sep 2026 | DPA signed, stored in Legal/Vendors | approved: drafting, document review; forbidden: unreviewed client sends | owner Sarah O., added 12 Sep 2026."

05 Your policy, ready to fill in

The six decisions from section 02, as fields. Fill them here, then transfer to your own letterhead, or use this page as the policy itself.

Firm name

Policy owner (named senior individual)

Approved tools and tiers, with approved uses per tool

The one rule (adapt the suggested wording from section 02)

How staff propose a new tool, and response time

Review cadence and next review date

06 Your register

One row per tool. The register is the gate: a tool goes on here before first use, never after.

Tool + tier

Training on our data excluded? Evidence and date

DPA in place? Where stored

Approved uses / forbidden uses

Owner + date added

Tool + tier

Training on our data excluded? Evidence and date

DPA in place? Where stored

Approved uses / forbidden uses

Owner + date added

07 Adoption checklist

- ☐ Amnesty first: staff asked what they already use, without blame
- ☐ Business tiers confirmed in writing for every approved tool: training exclusion, DPA, retention
- ☐ The one rule circulated, and free consumer accounts clearly forbidden for client data
- ☐ Register linked from wherever staff actually look
- ☐ First quarterly review in the diary