AI Use Policy

[Company Name]

Version 1.0 Adopted: [date] Review due: [date + 6 months] Owner: [name / role]

This policy sets out how our business uses AI tools. Its purpose is simple: get the benefit of AI without leaking client information, breaching UK data protection law, or publishing something wrong under our name.

1. The three golden rules

1. **Client and personal data never goes into public AI tools.** Names, addresses, financial details, contracts, case details, payroll: none of it is pasted into ChatGPT, Gemini, Copilot chat, or any tool that has not been approved for confidential data. Assume anything typed into a public tool may be stored, reviewed, or used for training by the provider.
2. **A human owns every output.** AI drafts; a named person checks facts, figures and tone before anything is sent to a client, published, or relied on. "The AI said so" is never a defence.
3. **If in doubt, ask [owner] before, not after.**

2. How we classify our information

Class	Examples	Public AI tools?	Approved private AI?
Public	Published website copy, brochures, open pricing	Yes	Yes
Internal	Process documents, templates, staff handbook	Only with care: nothing identifying	Yes
Confidential	Client names and files, contracts, financials, HR, supplier terms	Never	Yes, if the tool is on our approved list
Special category	Health, criminal records, immigration status and similar (UK GDPR Article 9)	Never	Only with [owner]'s sign-off, case by case

3. Approved tools

Tool	Approved for	Notes
[e.g. ChatGPT or Claude, personal accounts]	Public-class drafting, research, general writing help	No client data, ever

Tool	Approved for	Notes
[Private AI, e.g. our Noetava assistant]	Internal and confidential-class questions	Trained only on our own documents; data not shared with third-party AI providers
[Add your own rows]		

Anything not listed is not approved. Ask [owner] to evaluate new tools. The answer is often yes, but the list stays current.

4. Everyday rules that keep us safe

- **Anonymise first.** If you must use a public tool on internal material, strip names, amounts and anything identifying before you paste.
- **Check outputs for made-up facts.** AI states wrong things confidently. Verify names, numbers, dates, citations and legal or tax statements against a real source before use.
- **Mark substantial AI involvement where it matters.** Client deliverables that are largely AI-generated are reviewed line by line by the responsible person, and we are honest with clients if they ask how we work.
- **No AI decisions about people.** We do not let AI decide hiring, firing, lending, pricing for an individual, or anything else with a legal or similarly significant effect on a person (UK GDPR Article 22). AI may inform; a human decides.
- **Accounts and keys.** Work AI accounts use work emails. API keys are secrets: server-side only, never in a shared document or a web page.

5. Our obligations, in short

- **UK GDPR and the Data Protection Act 2018** apply whenever personal data touches an AI tool: we need a lawful basis, we honour rights requests, and providers processing personal data for us must be under a data-processing agreement.
- If we adopt a tool that processes personal data at any scale, [owner] records it in our processing register and checks whether a data protection impact assessment is needed.
- Client confidentiality terms in our engagement letters bind us regardless of what any AI provider’s terms say.

6. When something goes wrong

Pasted the wrong thing into a public tool? Sent an unchecked AI answer that was wrong? Tell [owner] the same day. The first hour is for fixing, not blame: delete what can be deleted, correct what was sent, and record what happened. If personal data was exposed, [owner] assesses whether it is reportable to the ICO (the 72-hour clock) and whether the people affected must be told.

7. Acknowledgement

Each team member reads this policy and confirms:

> *I have read the AI Use Policy and I understand the three golden rules.*

Name: _____ Date: _____

Name: _____ Date: _____

Name: _____ Date: _____

Template provided free by Noetava (noetava.com), a private AI trained on your own documents, so the confidential-class questions in section 2 have somewhere safe to go. Operated by MRD Assets Limited, company number 15731565, ICO registration 00015098067. This template is general guidance, not legal advice: adapt it to your business and take advice where you need it.