AI Tools and Client Data Policy

Document	Owner	Version	Approved on	Next review
AI Tools and Client Data Policy	[Name, role]	1.0	[date]	[date, at most 12 months later]

How to use this template
Replace every yellow field. Delete rules that do not apply to your business and add the ones that do. Delete this box and the appendix at the end before you publish or hand the document to a client.
Have the owner approve it and keep the signed copy. This is a template, not legal advice: where a law or a client contract applies, check it.

1. Why this policy exists

People at [Company name] use AI assistants and similar tools. Used well they save time. Used carelessly they send client or personal data to a third party, or put invented facts in front of a client. This policy sets simple rules for both risks.

2. Which tools are allowed

Only tools on this list may be used with company information. The owner adds a tool only after checking, for that plan and account type, what the provider's terms say about **training on your inputs**, **how long inputs are kept**, **where they are processed**, and **who can see them**.

Tool	Plan / account type	Checked on	Training on inputs	Retention	Highest data class allowed
[Tool name]	[Business plan, company account]	[date]	[Yes / No, link to the sentence]	[period]	[Internal]
[Tool name]	[...]	[date]	[...]	[...]	[Confidential]

Personal and free accounts are **never** used with Internal, Confidential or Restricted information, even for a quick question; only Public information may go into any tool. Business terms cover only the business plan they come with.

3. What may go in: data classes

Class	Examples	Approved AI tool (company account)	Any other tool
Public	Published website text, marketing copy that is already public	Yes	Yes

Internal	Internal procedures, meeting notes without client or personal data	Yes	No
Confidential	Client files, contracts, financial records, personal data about clients or staff	Only if the tool's row above allows it and the client contract does not forbid it	No
Restricted	[Health data, children's data, credentials, keys, anything law or contract restricts]	No	No

4. Rules for everyone

1. Check the data class before you paste or upload. If you are not sure, treat it as Confidential and ask [contact].
2. Always send the least information that can answer the question: ask for a clause to be explained, not for the whole file, and remove names, numbers and other identifying details the question does not need. Approval of a tool is a ceiling, never a reason to send more. Removing details by hand is slow and one missed line is enough, so check what you are about to send.
3. Never put passwords, access keys, or the contents of a restricted file into any AI tool.
4. If a client contract, engagement letter or professional rule limits third-party processing of the client's files, it overrides this policy. [List where such limits are recorded.]
5. Where the client agreement or the law requires it, tell the client that an AI tool is used on their work. [Decide and write your rule.]
6. Do not use AI to make or support a decision about a person (hiring, firing, pay, credit, discipline) without a human who understands and owns the decision.
7. **A person checks every AI output before it leaves the company.** Check it against the inputs and its purpose, not only for added facts: summaries can leave things out or change a meaning, and calculations and recommendations can be wrong. Treat any figure, date, name, quotation or reference that the AI added and you did not provide as unverified until you have checked it against the source. If you cannot check it, remove it.
8. Do not present AI output as your own checked work when it is not, and do not use it to copy someone else's material.

5. If something goes wrong

If you pasted something you should not have, tell [security contact] immediately, within one hour of noticing. Say which tool, which account, what data and when. Do not try to hide it or delete it quietly: the owner may need the account's history to ask the provider to delete it, and to decide whether a client or authority must be told (see the Incident Response Plan).

6. Review

The tool list is checked at least every [6] months and whenever a provider changes its terms. The policy is reviewed yearly.

Appendix: notes for the person adapting this template (delete before use)