Where your AI runs is a confidentiality decision.

Not an IT one. Cloud vs your office vs a private server — for a firm that cannot leak one client file.

PUBLIC CLOUD AI — $0 upfront, paid per use

A MACHINE IN YOUR OFFICE — ~$1,000 once

A PRIVATE SERVER — ~$6 / month

WHAT ACTUALLY HAPPENED

A partner pasted a client’s file into a public chatbot to save twenty minutes.

Deadline at six. The draft was good enough to “just ask the AI to tighten it.” Paste. Done.

THE UNCOMFORTABLE PART

No rule was broken — there was no rule. The privileged file left the building the moment it was pasted. Nobody decided that on purpose.

ASK THIS FIRST

Does the privileged text leave your walls — yes or no?

Every AI choice your firm makes collapses to this. Everything else is detail.

IF IT LEAVES →

confidentiality is now a **contract** with a vendor — configured, opted out of, re-checked at every terms change, forever.

IF IT STAYS →

confidentiality is a **property of the setup**. It holds because the data never left — not because someone promised.

OPTION 1

The public cloud AI — rented, shared, off-site

$0 UPFRONT · PAID PER USE

- You type into a site or app; the answer is computed on the **vendor's** machines. Your words travel to them.
- Cheapest, fastest start. Genuinely excellent for **non-confidential** work.
- But privileged text **leaves your walls** — safety now rests on the vendor's terms and your settings, forever.

Brilliant for the 60% that was never confidential. The wrong place for the 40% that is.

OPTION 2

A machine in your office — a computer on a desk

~$1,000–1,600 ONCE · NO MONTHLY BILL

- A quiet, capable computer that **runs the AI itself**, in your office. The file never travels anywhere.
- One purchase, then no per-use bill. Privileged text **stays inside the building**.
- Honest trade: set up once; its private AI is capable but **not as sharp** as the big cloud models on hard reasoning.

Confidentiality you can point at — it is the box on that desk.

OPTION 3

A private server — your own rented box, off-site

~$6–50 / MONTH

- A computer **only you** rent in a data centre — a safe-deposit box where you alone hold the key. Not shared.
- Cheap, isolated from your office network, wiped and rebuilt on demand.
- Honest trade: best for always-on **plumbing** (intake, reminders, routing). Heavy private reasoning still wants the office machine.

A keyed box you can burn down and rebuild — useful, not the heavy lifter.

SIDE BY SIDE

The honest comparison

	CLOUD AI	OFFICE MACHINE	PRIVATE SERVER
UPFRONT	$0	~$1,000–1,600	$0
ONGOING	per use	electricity	~$6–50/mo
PRIVILEGED TEXT LEAVES YOUR WALLS?	**YES**	NO	NO — isolated
STRONG ON HARD WORK	Highest	Good	Light only
WHO CONTROLS IT	**Vendor**	You	You
SETUP	None	One afternoon	One afternoon

Illustrative ranges for orientation, not a quote. One row decides everything — the third.

DECIDE IN TWO MINUTES

Five questions, honestly answered.

01 Do you handle privileged or client-confidential material? → **that work must not touch a public cloud AI.**

02 Bound by outside-counsel guidelines or data-residency terms? → **office machine or private server.**

03 Is most of your AI use non-confidential — research, marketing, admin? → **public cloud is fine for that slice.**

04 Want one predictable cost, not a metered bill? → **office machine.**

05 No in-house tech help yet? → **start on a managed private server.**

Split it: public cloud for the non-confidential 60%, a private setup for the privileged 40%. That split is the strategy.

THE HONEST PART

Private AI is not magic. Here is the trade.

≈60%

EVERYDAY WORK
PRIVATE AI HANDLES
CLEANLY

≈40%

GENUINELY HARD
STILL WANTS THE CLOUD

THE LOAD-BEARING POINT

The goal isn't "never use the cloud." It's deciding on purpose which work may leave the building — instead of finding out after it already did.

UK precedent — Munir [2026] UKUT 81 (IAC): pasting privileged material into a public AI tool waives privilege, irrecoverably.

YOUR MOVE

Decide it on purpose.

The principle is the whole brief. The setup is a one-afternoon decision, not a research project.

> CONFIDENTIALITY YOU CAN VERIFY —
> NOT CONFIDENTIALITY YOU HAVE TO TRUST.

Score your firm’s exposure — donnaoss.com/quiz