A PRACTICAL CHECKLIST

The 10-Minute AI Agent Check

Use this before you introduce any AI agent, or now for any agent you already use. No technical knowledge needed, only honest answers. Tick each question you can answer clearly.

Agent: _____ Owner: _____ Date: _____

PART 1 · ACCESS (Data Security)

- ☐ 1 What information can this agent see? Client records, emails, financial data, internal documents?
- ☐ 2 Does it need all of that to do its job, or did we give it more than necessary?
- ☐ 3 Where does the information go once the agent has it? Do we know what the provider does with it?

Can't answer question 3? Find out before going further.

PART 2 · THE RULES (Compliance)

- ☐ 4 Does the agent handle personal information about clients, staff or prospects?
- ☐ 5 If so, are we confident we have a lawful basis for using it this way, and would our privacy notice cover it?

"I'm not sure" to either? That is your first action, not something to sort out later.

PART 3 · CONTROL (Governance)

- ☐ 6 Who in the business owns this agent? One name, not "the team".
- ☐ 7 What can the agent do on its own, and what needs a person to approve it first?
- ☐ 8 How often does someone check what it is actually producing?

PART 4 · RESPONSIBILITY (Accountability)

- ☐ 9 If the agent gets something wrong, such as a quote, a promise or a message to a client, how would we find out?
- ☐ 10 Who would put it right, and who would explain it to the client?

How did you do?

All 10 clear	You are in a stronger position than many businesses adopting AI.
Stuck on 2–3	That's normal. Those gaps are your to-do list.
Stuck on most	Pause before giving the agent more access or responsibility. Not abandoning AI, but introducing it on your terms.

AI can take on the task. You still own the outcome.

This checklist is a starting point, not legal advice.