Stop Building and Start Managing: Five Practical Skills for Working with AI Agents

Ryan Watson | Watson Strategy Consulting
watsonstrategyconsulting.com

If you've been experimenting with AI tools to automate tasks or streamline your business, you've probably noticed something has shifted. The AI tools that used to simply suggest answers now go off and do things on their own. They read files, make changes, install software, and run tasks without checking in. That's the shift from AI as a helper to AI as an agent. For Gold Coast SMEs, understanding how to manage these agents properly could save you serious time and money.

It's Not About Better Prompting Anymore

Through 2025, getting good results from AI was mostly about asking the right question the right way. That still matters, but it's no longer enough. Today's AI agents take action. They'll restructure your database, redesign your checkout page, or reorganise files across multiple steps. If something goes wrong at step four of a twelve step process, everything that follows makes it worse. One researcher recently had an AI agent delete a huge chunk of her email inbox despite clear instructions not to, and she had to unplug the computer to stop it.

Working with AI agents isn't a prompting problem. It's a supervision problem. Think of yourself as a site manager overseeing a capable but forgetful subcontractor. You don't need to lay the bricks, but you'd better know what a straight wall looks like.

Save Your Work Before Everything Goes Sideways

The most common disaster with AI agents is losing work that was fine before the agent touched it. You ask it to fix one thing and suddenly three other features are broken, with no way back to the version that worked. The fix is the same thing developers have used for decades: version control. Think of it like save points in a video game. Every time your project is working, save a snapshot. If the agent breaks something, one command takes you back. The tool most people use is called Git, and you don't need to be technical to learn the handful of commands that matter. Spend

an hour getting familiar. It's one of the highest value investments you can make before asking an AI agent to change anything.

Know When to Start Fresh

AI agents have limited memory. Everything you've said, everything the agent has done, every file it's read all competes for the same space. After a long session, older instructions get dropped. That's why your agent seems brilliant for the first thirty minutes then starts ignoring things you've told it three times. The simple fix is to start a new session. For bigger projects, create a small set of reference documents: a task list, a context summary, and a record of what's been completed. When you restart, the agent picks up where it left off. Think of it as leaving handover notes for the next shift.

Give Your Agent Standing Orders

Every new session, your agent forgets your preferences. It'll default to the wrong design style, ignore naming conventions, or repeat mistakes you've corrected five times. The solution is a rules file: a simple text document the agent reads at the start of every session. Think of it as an employee handbook. You don't write the perfect version on day one. Start with the basics and add a line every time the agent does something wrong. Over a few weeks, it becomes a precise set of instructions tailored to your project. Keep it concise though. A rules file that's too long eats into the agent's working memory.

Keep the Tasks Small

When you ask an AI agent to tackle a massive overhaul at once, you're rolling the dice. It might touch dozens of files, and if something breaks partway through, you won't know which change caused it. Give your agent small, focused tasks. Fix one form. Add one feature. Update one page. Verify it works, save your progress, then move on. This applies beyond software too. Even generating a large presentation works better fifteen slides at a time than a hundred in one go.

Ask the Questions Your Agent Won't

AI agents don't think about what happens when real people use your systems in unexpected ways. They won't ask about error handling, data security, or growth. Set those expectations upfront. Tell your agent to show friendly error messages instead of

blank screens. Insist on proper data security so customers can only see their own information. And never paste secret keys or passwords into an AI chat.

Know When to Call in a Professional

These skills will take you a long way. But when things get serious, whether that's handling payments, sensitive customer data, or systems slowing under real traffic, bring in a professional developer. That's not failure. Building something that works and proving the concept before spending on professional engineering is exactly what smart businesses do. For Gold Coast SMEs, that lean approach to AI is a genuine competitive edge.