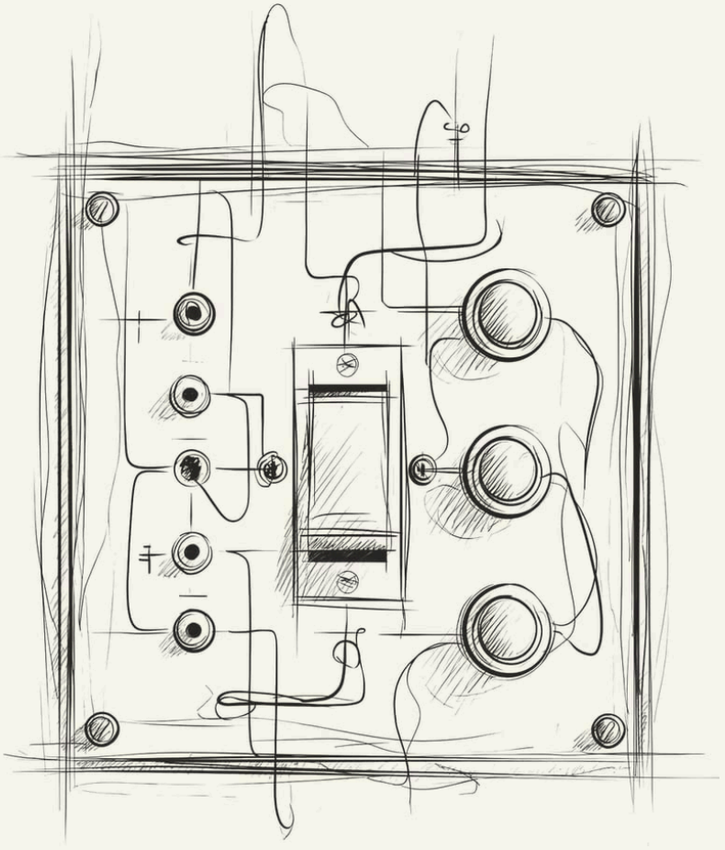
AI and tooling

MCP

An open protocol for connecting AI applications to sources of information and tools.



MCP

AI and tooling

MCP, the Model Context Protocol, is an open standard for connecting AI applications to outside systems such as document stores, databases and business tools. Developers build to one shared specification instead of a bespoke integration for every pairing. Anthropic introduced it in November 2024, and OpenAI and Google have since adopted it.

Why it matters for content

MCP lets assistants consult live content systems while they work. A style guide or terminology list becomes a source they check during drafting, instead of a document pasted into a prompt and gradually forgotten. That raises the value of maintained content. Tool descriptions are writing too: vague ones lead models to the wrong choice, so content people should help write them.

How MCP changes the picture

MCP moves AI from isolated chat towards agents that work inside organisational systems, finding information and taking actions across tools. The more an agent can do, the more its sources and permissions matter. Content can carry hidden instructions as well, and a page saying “ignore previous instructions” can steer an agent. The protocol supplies a route, but it doesn’t make every use of it safe.