

AI Starter Kit for UK SMEs

A free taster from Operating Bench. Two essentials to get your team using AI safely today: a one-page set of ground rules, and a quick guide to what data is safe to put into AI tools. The full AI Safe-Use Pack turns this into a complete, editable system.

Part 1: Six AI ground rules

Share these with your team as a starting point.

1. **Use approved tools only.** Use the AI tools your organisation has approved, through your work account. That also rules out the AI you might not notice you are using: unapproved browser extensions and grammar or search sidebars, AI meeting recorders, phone keyboard predictors, and assistants built into your software or device (such as Windows Copilot or Apple Intelligence). If it is not approved, do not put work data in it.
 2. **Mind what you put in.** Never paste confidential, client, or personal information into a tool that is not approved for it. When unsure, leave it out and ask.
 3. **Check what comes out.** AI is a fluent writer, not a reliable source: it invents facts, figures and references that look entirely real. You are responsible for the accuracy of anything you send. The bigger the impact, the more checking, and check twice when it goes to a client or involves personal data.
 4. **No solo AI decisions about people.** Never let AI make the final call on hiring, performance, credit or similar decisions on its own. A person decides.
 5. **Be transparent.** Be honest about material AI use, internally and with clients where they would reasonably expect to know.
 6. **Report mistakes early.** If something goes wrong, say so straight away. Early reporting is encouraged and helps contain harm.
-

Part 2: What data can go into AI tools

Before entering anything, work out what kind of data it is.

Level	Everyday examples	Rule
Public	Published marketing, public web pages, public job adverts	Fine in approved tools
Internal	Office memos, draft procedures, non-sensitive templates	Fine in approved tools (where the tool does not train on your inputs)
Confidential	Client briefs, contracts, management accounts, supplier terms, passwords and logins	Only in tools approved for confidential data. Never free or personal accounts
Personal / special category	A customer complaint, an employee grievance, CVs and payroll, customer lists; health data	Only where approved and lawful. Special-category data needs specific approval

The gut check: would I be comfortable if this exact text appeared somewhere outside the business? If not, either the tool must be approved for that data, or strip out the identifying details first.

Want the full system?

This starter covers two pieces: the habits. The full **AI Safe-Use Pack** is the rest of the system, the part you would point to if a client's due diligence, or the ICO, ever asked how you govern AI: a complete, editable AI Acceptable Use Policy, an approved-tools matrix and an AI risk register as working spreadsheets, a vendor assessment checklist, an incident response plan, a DPIA starter template, ready-to-paste privacy and disclosure clauses, a staff one-pager and literacy tracker, the verification-tiers visual, and a glossary. Built for UK GDPR, the ICO and the EU AI Act, in editable Word and Excel plus polished PDFs. Sector editions for training providers, recruitment and accountancy go deeper still.

See it at operatingbench.co.uk.

Disclaimer. General information and a practical starting point, not legal advice. Adapt it to your circumstances and take professional advice where appropriate.