

FIELD GUIDE 03

A UK field guide
Current to June 2026

THE IGNITE ALMANACK OF **SHADOW AI**

The AI your team already uses, and how
to bring it into the light.

A FIELD GUIDE FOR UK SMES

IGNITEAI SOLUTIONS

THE PROBLEM

Your team is already using AI. You just haven't been told.

Whether you approved it or not, people are pasting work into free chatbots to get their day done. That is shadow AI. It is running in your business right now, and the part that should worry you is where the data goes.

This is not people going rogue. They have targets and a tool that helps, so they use it. A sales lead pastes a client list in to draft an email. Someone in HR pastes a grievance note in to soften the wording. The work gets done faster, and nobody thinks to mention it.

The catch is what happens to what they paste. Most free tools keep it, and some train on it. Client names, contract terms, staff records, all going into a system you do not control and cannot pull back.

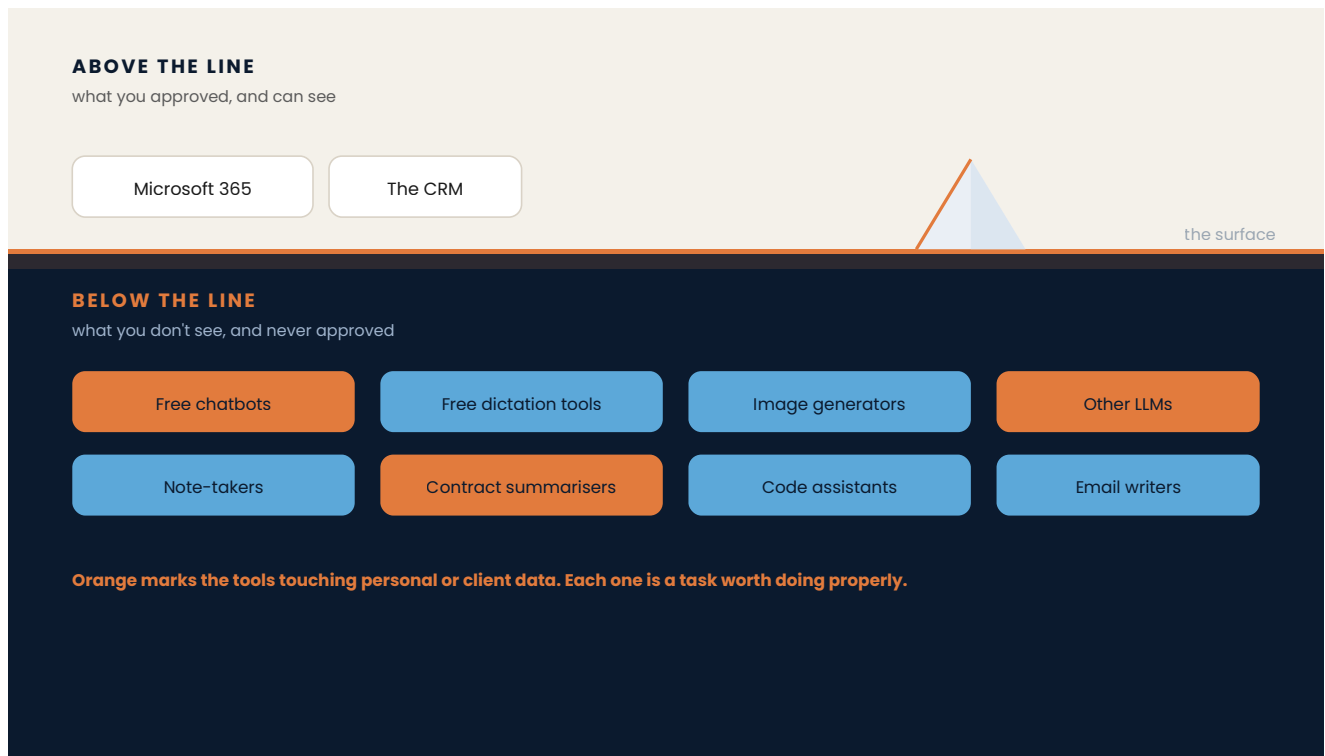
WHY THIS MATTERS

A free consumer chatbot processing personal data, with no Data Processing Agreement behind it, is a UK GDPR problem waiting to be reported. You carry the liability for data your team handed over, even when you never knew it left the building.

THE IDEA

Shadow AI is a map of your real pain.

Here is the part most owners miss while they are worrying about the risk. The tools your team smuggled in tell you exactly where the work hurts. People reached for AI on those specific tasks because those tasks are the worst part of their week. That is a gift.



An iceberg is the right picture for it. The tip is what you approved. The mass below the line is what your team runs without telling you.

People will find a way to use AI whether you give them permission or not. That is shadow AI.

Chris Duffy, IgniteAI Solutions

What is actually at risk.

The exposure is not theoretical. It is whatever your team pasted in this week, sitting on a server you have no agreement with. Here is what tends to go in, and what it costs you if it surfaces.

What gets pasted in	The exposure
Client names, emails, contracts	Personal and commercial data into a tool with no DPA. A reportable UK GDPR breach if it leaks.
Staff records, HR and grievance notes	Special-category data. The highest-risk category to mishandle, and the one staff paste in most.
Source code, internal documents	Your intellectual property leaving the building, sometimes used to train a third-party model.
Financial figures, board material	Confidential data outside your control, with the regulatory exposure that follows in a regulated sector.

THE GAP UNDERNEATH ALL OF IT

A free or consumer tier has no Data Processing Agreement. Under UK GDPR you need one for any third party handling personal data on your behalf. No DPA means no lawful basis for that processing, and the liability sits with you, not with the member of staff who pasted it in.

Bring it into the light.

The instinct is to ban it. Ban it and people keep using it anyway, just somewhere you can no longer see. The behaviour moves out of sight and the risk stays exactly where it was. The businesses getting this right do the opposite. They run an amnesty, find out what is really being used, and make the useful tools safe.

BAN IT

- Tools go hidden
- You are blind to the risk
- Data keeps leaking
- The pain never gets fixed

GOVERN IT

- Tools are visible and known
- A safe option with a DPA
- Red lines everyone understands
- Pointed at the work that hurt

An amnesty turns a hidden risk into a known list in a single day. Once you can see it, you can make it safe, and you can point your people at a proper tool for the jobs they were already trying to do.

HOW TO START

Five steps, start to finish.

This is the sequence we run with clients. None of it needs new software on day one. It needs an honest list and a clear set of rules.

- 1 Run an amnesty.** Ask everyone what AI they use, with no blame attached. Make it safe to answer and you get an honest list in a day.
- 2 Sort by data risk.** Mark every tool that touches personal, client or financial data. Those are the urgent ones, the rest can wait.
- 3 Draw the red lines.** One page, plain English: what can and cannot go into a public chatbot. People follow rules they can actually read.
- 4 Give them a safe alternative.** A governed tool with a DPA, set up for the jobs they were smuggling. Take away the reason to go around you.
- 5 Point it at the pain.** The tasks they were sneaking AI onto become your first official use cases. The map drew itself.

TRY THIS ON MONDAY

Ask your team one question, and mean the no-blame part: **what AI are you using that I don't know about?**

The list you get back is two things at once. It is your risk register, and it is your roadmap for where AI should go first.

Three prompts to run the amnesty.

Paste these into Claude or ChatGPT. They turn the idea into something you can send and act on in about ten minutes. Replace the words in [brackets] with your own.

PROMPT 1: WRITE THE AMNESTY MESSAGE

Write a short, warm message from me to my team at a [type of business] with [number] staff. Ask them to tell me, with no blame and no consequences, which AI tools they currently use for work and what they use them for. Make clear I want this so I can make it safe and useful, not to stop them. Keep it under 150 words.

Sets the no-blame tone that gets you an honest list instead of silence.

PROMPT 2: SORT THE LIST BY RISK

Here is a list of AI tools my team told me they use: [paste the list]. For each one, tell me whether it likely touches personal, client, or financial data, whether the free tier has a Data Processing Agreement, and rank them from highest to lowest UK GDPR risk. Flag the three I should deal with first.

Turns the raw list into a priority order you can act on.

PROMPT 3: DRAFT THE RED LINES

Draft a one-page acceptable-use note for AI at a UK business of [number] people. Cover what staff can and cannot paste into a public chatbot, the data that must never go in, who to ask when unsure, and the safe tool we provide instead. Plain English a busy team will read and remember.

The guardrails that let people use AI freely, because they know where the edges are.

THE NEXT STEP

MAKE IT SAFE FIRST

Shadow AI is the signal. Governance is the answer. Before you roll out a single tool, you want the red lines