CM Security

0203 3070370
info@cmsecurity.co.uk

FREE CHECKLIST · AI READINESS

Is your business ready for AI tools?

Ten questions to find out whether your company data is going into AI accounts you own, or accounts your staff own.

ChatGPT · Microsoft Copilot · Claude · Google Gemini · Grok

Page 2
Personal vs company AI, and what leaks

Page 3
The 10-question check

Page 4
Your score and what to fix first

PERSONAL VS COMPANY

Every major AI tool comes in two versions

They look the same on screen. Staff sign in with whatever account is to hand, often a personal one, on a work laptop, with company data.

AI tool	Personal version	Company version
ChatGPT (OpenAI)	Free, Plus, Pro	Business, Enterprise
Copilot (Microsoft)	Signed in with a personal Microsoft account	Microsoft 365 Copilot, Copilot Chat with a work account
Claude (Anthropic)	Free, Pro, Max	Team, Enterprise
Gemini (Google)	With a personal Google account	Gemini in Google Workspace
Grok (xAI)	Personal X or Grok account	Grok business plans

What changes between the two

	Personal version	Company version
Who owns the account and chat history	The employee	Your company
Chats can train the vendor's models	Often yes, depending on settings	No, under business terms
Access removed when someone leaves	No	Yes
Admin controls and visibility of use	None	Admin console, audit on higher tiers
Sign-in with company identity (SSO)	No	Yes, on most business plans

What ends up in personal AI accounts

01

Client personal data

Names, addresses and case notes pasted in for a summary. Unrecorded processing under UK GDPR.

02

Commercial information

Pricing, bids, contract terms and supplier deals, pasted in to be tidied up.

03

Credentials and code

API keys, config files and scripts dropped in for debugging help.

04

HR and board papers

Disciplinary notes, salary reviews and board minutes condensed into summaries.

Plan names and data terms based on each vendor's published terms at [DATE CHECKED]. They change often, so check current terms before relying on them.

THE CHECK

Ten questions. Answer honestly.

Tick one box per question. "Not sure" counts as a gap: if you can't answer it, you can't control it.

#	QUESTION	YES	NOT SURE	NO
01	**Do you have a written policy on which AI tools staff may use?** Without one, every employee is making their own call.	☐	☐	☐
02	**Have you bought company licences for the AI tools staff use?** ChatGPT Business, Microsoft 365 Copilot, Claude Team, Gemini for Workspace, Grok business plans.	☐	☐	☐
03	**Could you tell if someone was using a personal AI account on a work device?** Shadow AI is the starting point for most exposure.	☐	☐	☐
04	**Do staff know what they must never paste into an AI tool?** Client personal data, credentials, contracts, HR records.	☐	☐	☐
05	**Is sign-in to AI tools tied to company identity, so leavers lose access?** A personal login walks out of the door with the employee.	☐	☐	☐
06	**Have you tidied file permissions before connecting AI to company files?** Copilot, Gemini and Claude connectors surface anything the user can already open.	☐	☐	☐
07	**Do you block or monitor uploads to unapproved AI sites?** Web filtering or a CASB can stop data leaving in the first place.	☐	☐	☐
08	**Do your UK GDPR records cover the AI tools you use?** Records of processing and DPIAs for any tool that handles personal data.	☐	☐	☐
09	**Have staff been trained on AI-written phishing and voice cloning?** Attackers use the same tools to impersonate your directors and suppliers.	☐	☐	☐
10	**Do you hold a current Cyber Essentials certificate?** The baseline that insurers and public sector buyers expect.	☐	☐	☐

Count your ticks

Your score is the number of "Yes" answers, highlighted. Turn over to see what it means.

YOUR RESULT

What your score means

0 to 3

Exposed

Company data is very likely already in personal AI accounts you can't see or recover. Find out what's in use before adding more tools.

4 to 7

Partly exposed

Some controls are in place, but staff can still move data into tools you don't manage. This is where most leaks happen.

8 to 10

Mostly in control

You've covered most of the basics. Confirm the controls work in practice before rolling out more AI tools.

What to fix first

For every question you answered "No" or "Not sure", here is the action to take.

#	Action	Done
01	Write and circulate an AI use policy naming the approved tools.	☐
02	Move staff off personal AI accounts onto company licences.	☐
03	Get visibility of which AI sites and apps are in use.	☐
04	Train staff on what data must stay out of AI tools.	☐
05	Put AI tools behind company sign-in (SSO) and your leavers process.	☐
06	Review SharePoint, OneDrive and Google Drive permissions before connecting AI assistants.	☐
07	Block or monitor uploads to unapproved AI services.	☐
08	Update your records of processing and DPIAs for AI tools.	☐
09	Train staff to spot AI-driven social engineering and fake voice calls.	☐
10	Get Cyber Essentials in place or renewed.	☐

Ticked "Not sure" three times or more? Not knowing is a finding in its own right. It usually means AI use is happening without anyone owning it.

CM Security

NEXT STEP

Book a free 30-minute AI exposure call

Bring this checklist. A CM Security consultant will go through your answers, tell you which AI tools your staff are likely using, and where your data could be going. No sales pitch, just a straight answer.

AI readiness review

Discovery of AI tools in use, a licence check across ChatGPT, Copilot, Claude, Gemini and Grok, data exposure findings mapped to UK GDPR, and an AI use policy ready to adopt.

Vulnerability review

External and internal scanning, every finding checked by a consultant, and a fix plan ranked by real risk to your business.

Call **0203 3070370**

Email **info@cmsecurity.co.uk**

Web **cmsecurity.co.uk**