



WHITEPAPER

Shadow AI & Data Leaks

Securing ChatGPT and Generative AI in the
Workplace

01 · THE PROBLEM

Your Staff Are Already Using AI

Shadow AI is the use of AI tools at work without approval or oversight. It rarely starts with bad intent. People want to save time, so they paste in what they are working on: emails, contracts, spreadsheets, code.

71% of UK employees have used unapproved consumer AI tools at work

Source: Microsoft and Censuswide, 2,000+ UK employees

51% of UK businesses fear staff are feeding sensitive data to unauthorised AI

Source: Turbotic, 1,004 UK senior decision-makers, July 2026

How Data Leaks Through AI



Pasted Straight In

Customer details, contracts and code go into a prompt to save time



Personal Accounts

Work data lands in accounts you cannot see, audit or close



Consumer Defaults

Personal plans may use conversations for training unless the user opts out

57% of professionals using AI at work in one survey said they had entered sensitive information into public tools

Source: TELUS Digital, reported by Decision Marketing

2023

Engineers at Samsung pasted internal source code into ChatGPT. The company restricted generative AI use afterwards.

Source: Bloomberg, May 2023, widely reported

02 · IS IT SAFE?

Is ChatGPT Safe for Company Data?

It depends which ChatGPT. Personal plans and business plans are treated differently by default, and staff often use the personal one for work.

	 Personal plans Free, Plus and Pro	 Business plans Business, Enterprise, Edu and API
Used for training by default	Yes, until the user opts out	No, not by default
Who controls the setting	Each individual user	Your organisation
Contract terms	Consumer terms	Business terms, with a data processing agreement
Our view for customer data	Not suitable	Suitable with a lawful basis and settings checked

Source: OpenAI Help Centre, "What is the ChatGPT Enterprise and Team data policy?" Contract terms and our view are NetMonkeys guidance.

⚠ **Opting out is not the same as safe.** Switching off training stops your chats being used to improve models. It does not make a personal account suitable for personal or confidential data.

1 rule

The NCSC's advice is simple: do not include sensitive information in queries to public AI tools, and understand the terms of use before you do.

Source: NCSC, "ChatGPT and large language models: what's the risk?"

03 · FREE TOOLS AND BREACHES

Can Using Free AI Tools Cause a Data Breach?

Yes. Pasting personal data into a tool you have no contract with can be an unauthorised disclosure, which UK GDPR treats as a personal data breach.

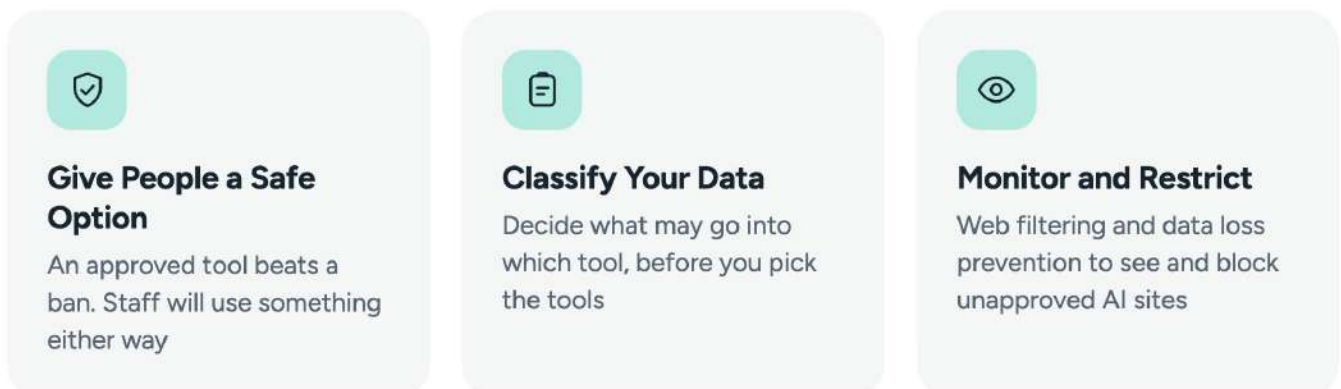


What Leaks Most



Source: TELUS Digital survey; Bloomberg, May 2023.

Three Controls That Work



04 · THE POLICY

How to Write an AI Policy for Employees

A good policy fits on two pages and answers four questions: which tools, which data, which accounts, and what to do when something goes wrong.

1

Purpose and Scope

Who it covers, including contractors

2

Approved Tools

A short, named list, kept current

3

Data Rules

What may and may never go in

4

Accounts

Work accounts only, never personal logins

5

Checking Outputs

A person reviews anything customer-facing

6

Training

Short, recorded and repeated each year

7

Reporting

Tell IT at once if something sensitive was pasted

8

Review

Revisit every six months as tools change

Sort Your Data Into Three Tiers

Open

Public information and general drafting. Any approved tool.

Restricted

Internal documents and plans. Approved business tools only.

Never

Personal data, client confidential material, passwords and keys. No AI tools.

The ICO expects organisations to give staff clear guidance on whether and how they may use generative AI. Source: ICO, summarised by Brodies LLP.

05 · SECURING AI

Ten Checks for Safe AI at Work

Tick what is true today, then give each gap an owner and a date. Start with the policy and one approved tool.

- | | |
|---|--|
| ☐ AI policy written, signed off and shared with every employee | ☐ Approved AI tools named, on business-grade accounts |
| ☐ Personal AI accounts barred for company data | ☐ Data tiers defined: open, restricted, never |
| ☐ Web filtering or data loss prevention covers AI sites | ☐ Data processing agreement in place for each approved tool |
| ☐ DPIA completed where personal data is involved | ☐ Short staff training delivered and recorded |
| ☐ A no-blame route to report a mistaken paste | ☐ Policy and tools list reviewed every six months |

→ Three Steps This Week

1

Ask staff, anonymously, which AI tools they already use

2

Choose and roll out one approved business tool

3

Publish a one-page policy using the tiers on page 5

Book an AI Security Review

We will find the shadow AI already in your business and put guardrails around it

0161 834 9345 | 0115 822

1860

contact@netmonkeys.co.uk