

## PRACTICAL AI DATA GUIDE

# Your data and AI

A practical guide to what your team may be giving away when business or customer information is entered into AI tools.

**Treat the prompt box like a place your data actually goes.**

Use less information, check the current terms and give staff a clear boundary.

**01**

## Classify first.

Public, internal, confidential and customer data are not the same.

**02**

## Minimise the input.

Remove identifiers and detail the task does not genuinely need.

**03**

## Standardise the rule.

Staff should know what is allowed, restricted and prohibited.

**Before pasting the full document, ask whether less data will work.**

Use this guide →

## MISSION & SCOPE

# The chat window is still a place your business information goes.

AI is useful because people can paste in real material. That convenience creates a simple question: what is appropriate to share with the provider?

### THIS GUIDE IS USEFUL IF

- Staff use AI for drafting, summaries or analysis.
- Real business material is entering prompts.
- No clear data boundary exists yet.

### THIS GUIDE WILL NOT

- Describe any named provider's current policy.
- Replace legal or privacy advice.
- Ban every useful AI task.

## How to control the boundary

01

### Classify

Decide whether the information is public, internal, confidential or customer-related.

02

### Minimise

Use less detail, redact identifiers or create a safer summary.

03

### Approve

Check the current tool, account and terms before sensitive use.

## Using AI can involve sharing data with a third-party service.

Think of a photocopier in a shared office. Before placing sensitive pages on the tray, you would want to know who operates it, what happens to copies and whether it is appropriate for that material.

## BEFORE SENDING

# Six questions that set a safer data boundary.

The most useful control happens before information leaves the business workflow.

## Decide what can cross.

Do not rely on the chat-like appearance of the interface.

01

### Classification

Is the material public, internal, confidential or customer-related?

02

### Necessity

Does the task genuinely require this level of detail?

03

### Minimisation

Can names, identifiers or sensitive specifics be removed?

04

### Current terms

What does this exact provider, account and setting say today?

05

### Authority

Is the person using the tool allowed to share this information?

06

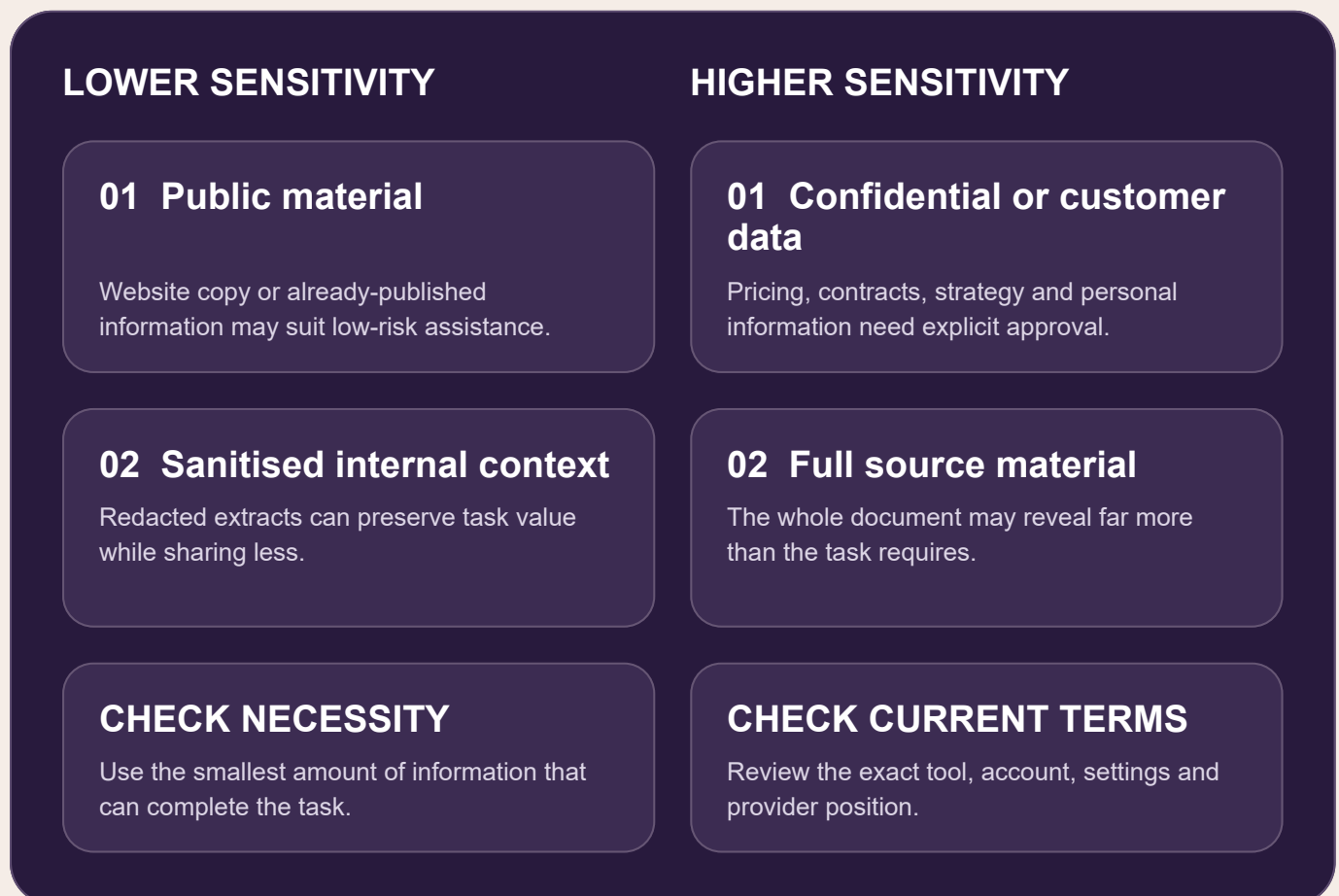
### Review trigger

What change in tool, terms or use case should reopen the decision?

## DATA-FLOW MAP

# One prompt can carry different data risks.

The handling varies by provider, account type and settings. The classification must happen before sending.



Need the verification rule too? [Read AI Hallucination →](#)

## COMMERCIAL EFFECT

# Convenience changes behaviour faster than policy does.

If the easiest path is pasting the whole document, people will do it unless the business creates a clearer rule.

**Minimal data used****Reduced exposure**

The task keeps useful context without names or confidential detail.

**Whole source pasted****Unnecessary sharing**

The provider receives information the task never needed.

**Terms checked****Informed choice**

The business chooses based on the current account and settings.

**Privacy assumed****Unknown handling**

The chat interface is mistaken for a private internal system.

**Staff rule exists****Repeatable control**

Allowed, restricted and prohibited uses are clear.

**Everyone decides alone****Inconsistent judgement**

One person's idea of safe enough becomes the standard.

## Would you send this to a supplier without checking their data handling?

The chat interface is not a privacy promise.

## FIVE SIGNS THE BUSINESS HAS NO REAL AI DATA BOUNDARY

# Problems to catch before AI use expands.

These patterns create privacy, confidentiality and supplier risk even when the task itself looks harmless.

**Critical**

**Sign 1**

### Customer personal information is pasted without an approved arrangement

Real customer details are used because they make the task easier.

#### WHAT IT COSTS

Privacy exposure and uncertainty about where customer information travelled.

**Major**

**Sign 2**

### Confidential business data enters a consumer tool

Useful context is shared before data handling has been checked.

#### WHAT IT COSTS

Loss of control over pricing, contracts, strategy and sensitive plans.

**Major**

**Sign 3**

### Staff have no approved-use rule

Each person invents their own definition of sensitive and safe enough.

#### WHAT IT COSTS

Inconsistent behaviour and problems that are difficult to trace.

**Moderate**

**Sign 4**

### “Free” and “private” are treated as the same thing

Easy access is mistaken for an approved confidential environment.

#### WHAT IT COSTS

Decisions are made from interface cues rather than actual terms.

**Moderate**

**Sign 5**

### No one checks current terms before adoption

Usefulness becomes the only approval test.

#### WHAT IT COSTS

A tool spreads before anyone knows whether its data handling fits.

## A chat interface does not explain what happens behind it.

Check the current provider, account and settings before sensitive information is entered.

## CORRECTION AND SELF-ASSESSMENT

# Five questions before business data enters an AI tool.

Common myth: “It is just a chat window, so nothing is really stored.” Better framing: handling varies by tool, account and settings; the interface proves nothing.

01

## What will staff realistically paste into this tool?

Assess urgent, convenient behaviour, not only the ideal use case.

02

## What do the current terms say about submitted data?

Review the exact provider, account type and settings being considered.

03

## Can the task be completed with less sensitive information?

Remove identifiers, confidential detail or the full source where possible.

04

## Who is authorised to approve an exception?

Staff need a clear route when useful work sits outside the normal rule.

05

## What triggers a review of the policy?

New tools, changed terms, settings and new use cases should reopen it.

## WORKING AI DATA STANDARD

# A reusable boundary staff can follow in real work.

The aim is useful AI with less unnecessary information crossing into external services.

## 01 Classify

Mark information public, internal, confidential or customer-related.

## 02 Test necessity

Ask which details the task genuinely needs.

## 03 Minimise

Remove names, identifiers and unnecessary sensitive data.

## 04 Check terms

Review the current provider, account and settings.

## 05 Confirm authority

Make sure the user is allowed to share that information.

## 06 Record approval

Document exceptions and when the boundary must be reviewed.

## INSTEAD OF

**“It looks private.”**

No classification, terms check or approval.

## Reusable data-use check

**TASK:**

---

**DATA CLASS:**

---

**DETAIL REQUIRED:**

---

**DETAIL REMOVED:**

---

**CURRENT TERMS CHECKED:**

---

**APPROVED ACCOUNT:**

---

**AUTHORISED BY:**

---

**REVIEW TRIGGER:**

---

**DISCUSS THE RULE →**

**Build a practical staff rule.**

Map data classes, approvals and review.

## DUE DILIGENCE

# Classify before you paste.

Three rules and two next steps for safer AI data use.

01

## Use less data

Remove names, identifiers and confidential detail where the task allows.

02

## Check the terms

Review the current provider, account type, settings and terms.

03

## Set a usable rule

Document allowed, restricted and prohibited uses in plain language.

## Default to less data and an approved arrangement.

If a provider cannot explain data handling, controls and account differences plainly, keep digging.

## CONTINUE LEARNING

## AI Hallucination

See why plausible output still needs evidence before use.

[Read next →](#)

## AI Foundations

Continue through the rest of this collection.

[Explore collection →](#)

# Treat the prompt box like a place your data actually goes.

Classify before sending. Minimise what the task does not need. Check the current tool, account and settings rather than assuming privacy.

## PRIMARY NEXT STEP

### AI Hallucination

Build the verification checkpoint for AI-assisted output.

[Continue →](#)

### AI Foundations

See every guide in this collection.

[Explore collection →](#)

### All guides

Browse every topic and problem.

[View library →](#)

### Need a practical staff data rule?

Bring the tools and workflows already in use. Map where customer or confidential information enters and what should change.

[Discuss the boundary →](#)