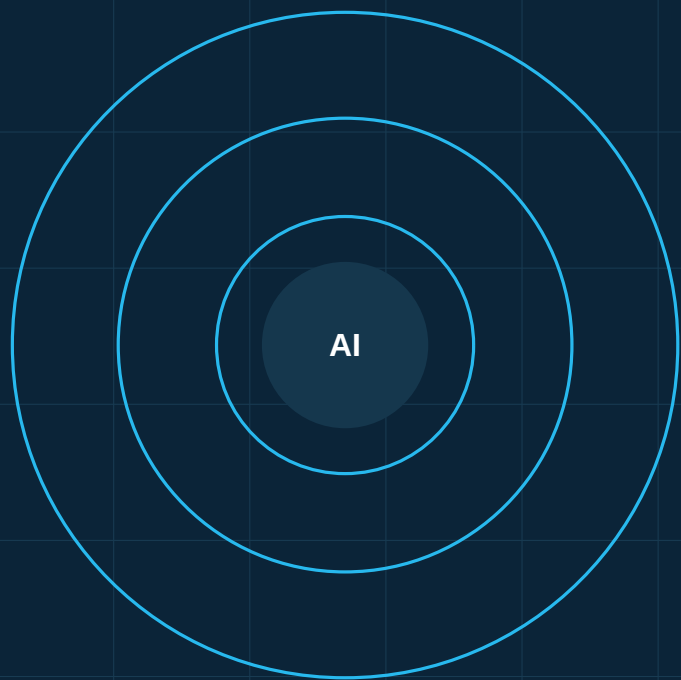


# PROFESSIONAL AI GUIDE FOR ACCOUNTANTS & BUSINESSES

## AI Governance, Data Protection & Practical Safety

Protect sensitive information. Approve AI use intelligently.

Review outputs. Respond properly when something goes wrong.



### PROTECT

Sensitive data

### APPROVE

AI use

### REVIEW

Outputs

### RESPOND

To incidents

# HOW TO USE THIS GUIDE

Practical. Visual. Actionable.

| Who it's for                                                                                                                             | How to use it                                                                                                     | What it includes                                                                                    |
|------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| Accountants, bookkeepers, payroll/tax teams, professional practices and small businesses handling sensitive or confidential information. | Make faster decisions about when AI is suitable, what must be protected and what to do if information is exposed. | Decision tools, risk signals, scenarios, incident steps and five separate implementation resources. |

## Three key takeaways

- **Use AI with confidence:** know what is GO, what needs a CHECK and when to STOP.
- **Protect information:** apply the 5-Gate AI Check and clear data boundaries.
- **Be prepared:** approve tools, keep proportionate evidence and respond quickly when something goes wrong.

**30-MINUTE ACTION**

Before using the guide with staff, identify one person who owns AI approvals, one person who owns information incidents, and one escalation route that everybody can actually use.

## The implementation pack

| Resource                             | Purpose                                                                |
|--------------------------------------|------------------------------------------------------------------------|
| AI Acceptable-Use Policy             | Sets internal rules and responsibilities.                              |
| Approved AI Tool & Use-Case Register | Records exact products, workspaces, data permissions and review dates. |
| AI Data Incident Response Record     | Provides a structured record when information has already been shared. |
| Client & Business AI Wording Pack    | Adaptable client/customer, privacy and communication wording.          |
| AI Staff Quick Check                 | Two-page desk guide for safer day-to-day use and escalation.           |

# THE 5-GATE AI CHECK

Use this before any material AI use. It is the core decision method used throughout the guide.

| 1 DATA                                                | 2 PURPOSE                       | 3 TOOL                                                   | 4 ACTION                     | 5 EVIDENCE                                                   |
|-------------------------------------------------------|---------------------------------|----------------------------------------------------------|------------------------------|--------------------------------------------------------------|
| What information are you using?                       | What are you trying to achieve? | Is the exact tool/workspace approved?                    | What will the AI do with it? | How will the decision and review be recorded?                |
| GO                                                    |                                 | CHECK                                                    |                              | STOP                                                         |
| Lower risk, approved use. Proceed with normal review. |                                 | Clarification, approval or stronger controls are needed. |                              | Do not proceed with real data until specifically authorised. |

## Five questions that stop most avoidable mistakes

- What exact information will leave our normal systems?
- Why is AI needed for this task?
- Is the exact product, plan/workspace and use case approved for this data?
- What do the supplier terms and settings say about retention, training/evaluation, access, subprocessors, transfers and deletion?
- Who will check the output, and what evidence of that review should be retained?

**RED FLAG**

A familiar AI brand is not an approval. Consumer and business products can have different terms, retention, administration and security controls.

# AI USE SIGNAL GUIDE

The signal tells you what to do next. It does not replace professional or management judgement.

| GO                                                       | CHECK                                                    | STOP                                                         |
|----------------------------------------------------------|----------------------------------------------------------|--------------------------------------------------------------|
| Lower risk, approved use.<br>Proceed with normal review. | Clarification, approval or stronger controls are needed. | Do not proceed with real data until specifically authorised. |

| Situation                                                                          | Likely signal | Why                                                                        |
|------------------------------------------------------------------------------------|---------------|----------------------------------------------------------------------------|
| Researching a public HMRC or professional-body page                                | GO            | No client data; verify the source and date.                                |
| Rewriting generic marketing text with no confidential facts                        | GO            | Lower information risk; still review accuracy and tone.                    |
| Drafting an email using a client/customer-specific fact pattern                    | CHECK         | Confidentiality and accuracy need review.                                  |
| Uploading a complete trial balance, payroll file or HR dataset to a public chatbot | STOP          | Sensitive information leaves controlled systems without an approved route. |
| Using a firm-approved business workspace with an authorised limited data extract   | CHECK         | Approval still depends on the exact use, data and controls.                |
| AI agent posting entries or sending external messages                              | CHECK / STOP  | Action permissions create a materially higher control risk.                |

## PRACTICAL INSIGHT

When in doubt, choose CHECK. If the required facts or approval cannot be established, choose STOP rather than experimenting with real data.

# DATA RISK BOUNDARIES

Know what you can - and cannot - use in AI tools.

| LOW RISK                                                                                                                                                        | MEDIUM RISK                                                                                                                               | HIGH RISK                                                                                                                                                        |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Public/general information with no client or personal data.<br><br>Public websites<br>General guidance<br>Fictional examples<br>Non-sensitive internal policies | Some sensitive elements or context.<br><br>Limited client/customer context<br>Draft documents<br>Pseudonymised data<br>Internal summaries | Highly sensitive, confidential or personally identifiable information.<br><br>Payroll/HR<br>ID documents<br>Tax returns<br>Bank details<br>Passwords/credentials |

**RED FLAG**

Pseudonymised is not anonymous. Replacing a name with 'Client A' does not automatically remove UK GDPR or confidentiality obligations.

## Minimise before you prompt

- Use public, fictional or abstracted facts where real client/customer data is not needed.
- Remove identifiers that are not needed for the answer.
- Do not upload a whole file when a narrow approved extract is enough.
- Never include passwords, API keys, recovery codes or authentication secrets.
- Do not connect a mailbox, drive, ledger, CRM or client portal merely because an AI product offers a connector.

**PRACTICAL INSIGHT**

Ask: 'Would I be comfortable sending this information to this supplier under the same contractual controls?' If not, stop and assess the use properly.

# BEFORE YOU USE ANY AI TOOL

Five plain-language checks before sensitive information leaves your normal systems.

| 1 TOOL                                                | 2 ACCOUNT                      | 3 DATA                                                   | 4 SETTINGS                                      | 5 REVIEW                                                     |
|-------------------------------------------------------|--------------------------------|----------------------------------------------------------|-------------------------------------------------|--------------------------------------------------------------|
| Exact product, plan and workspace approved?           | Firm-managed business account? | Information allowed for this use?                        | Retention, sharing and supplier use understood? | Who checks the output and what is recorded?                  |
| GO                                                    |                                | CHECK                                                    |                                                 | STOP                                                         |
| Lower risk, approved use. Proceed with normal review. |                                | Clarification, approval or stronger controls are needed. |                                                 | Do not proceed with real data until specifically authorised. |

## If client, customer, employee or other personal data will be involved

| Where is the information processed?                   | Processing locations and any international-transfer safeguards.                                     |
|-------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| How long is it retained?                              | Retention period, deletion process and what happens to backups.                                     |
| Can the supplier use it to improve/train the service? | Whether content is used for training, evaluation or human review - and which settings control that. |
| Who else can receive it?                              | Relevant subprocessors and integrations.                                                            |
| How is access controlled?                             | Business account administration, MFA where available, roles and leaver controls.                    |
| Does the use need a DPIA?                             | Record whether a Data Protection Impact Assessment is required or why it is not.                    |

### WHAT THIS MEANS IN PRACTICE

Do not approve 'ChatGPT', 'Copilot' or another brand in the abstract. Approve the exact product, account/workspace, intended task and data categories - then set a review date.

# AI AUTOMATIONS: EXTRA POWER, EXTRA RISK

When AI does more than suggest, the control requirements change.

**What does 'AI can act' mean?** Some tools can send emails, create or edit files, update ledgers, access systems, trigger workflows or chain several tasks together. A mistake can therefore become an action before a person notices it.

| PURPOSE            | HUMAN GATE                      | ACCESS          | LOGS                  | REVIEW                       |
|--------------------|---------------------------------|-----------------|-----------------------|------------------------------|
| Only defined tasks | Approval before material action | Least privilege | Every action recorded | Monitor, test and re-approve |

## Higher-impact examples

| AI action                              | Control expectation                                                                   |
|----------------------------------------|---------------------------------------------------------------------------------------|
| Posting bookkeeping entries            | Defined transaction types, limits, review sampling, audit trail and rollback.         |
| Sending client/customer communications | Human approval before material or specific messages are sent.                         |
| Accessing mailboxes or drives          | Least-privilege access, restricted folders, logging and connector review.             |
| Creating/submitting documents          | No submission of filings, legal forms or returns without authorised human review.     |
| Triggering payments or record changes  | Strong segregation of duties; AI should not independently authorise financial action. |

**RED FLAG**  
Do not allow an AI agent to post entries, send material external communications, make payments, submit filings or change master data merely because the product technically permits it.

## SCENARIO TESTS - 1 TO 5

Choose GO, CHECK or STOP - then compare with the suggested signal.

| Scenario                  | Facts                                                                  | Signal | Why                                                                                  |
|---------------------------|------------------------------------------------------------------------|--------|--------------------------------------------------------------------------------------|
| 1. Public tax research    | Summarise a current public HMRC page; then open the source and verify. | GO     | Public source, no client data; still verify currency and accuracy.                   |
| 2. Draft client email     | Use a client-specific fact pattern to draft a reply.                   | CHECK  | Confidentiality and accuracy depend on approved tool, data and review.               |
| 3. Trial balance upload   | Upload a client trial balance to an unapproved public chatbot.         | STOP   | Client information leaves approved systems with no documented approval.              |
| 4. Payroll anomaly review | Analyse employee payroll data for unusual movements.                   | CHECK  | Sensitive personal/financial data needs an exact approved route and strong controls. |
| 5. AI ledger assistant    | AI posts routine entries directly into the ledger.                     | CHECK  | Action needs approval, limits, logs and human oversight.                             |

### SCENARIO RULE

The signal is a starting point, not a universal legal answer. Apply the 5-Gate Check to the exact data, account/workspace, supplier settings, instructions and action involved.

## SCENARIO TESTS - 6 TO 10

Five more situations covering business records and higher-risk use.

| Scenario               | Facts                                                                                                              | Signal       | Why                                                                                                                        |
|------------------------|--------------------------------------------------------------------------------------------------------------------|--------------|----------------------------------------------------------------------------------------------------------------------------|
| 6. Tax return records  | Full tax-return pack including bank interest, employment and investment records uploaded to a consumer AI account. | STOP         | Highly identifying financial information; use an approved secure process instead.                                          |
| 7. HR/legal form       | Employee or ID documents uploaded so AI can suggest what to enter.                                                 | STOP / CHECK | Do not upload identity or employment documents to an unapproved tool. Limited non-identifying questions may be lower risk. |
| 8. Receipt capture     | Approved accounting product uses an AI receipt-capture feature under existing processing controls.                 | GO / CHECK   | Potentially appropriate if the feature and data use are actually approved and output is checked.                           |
| 9. Pseudonymised query | Names removed but facts still make the person or business easy to recognise.                                       | CHECK        | Pseudonymised data can still be personal/confidential.                                                                     |
| 10. AI sends email     | Assistant drafts and automatically sends external messages without human approval.                                 | STOP / CHECK | Automated external action needs explicit approval, limits and usually a human gate.                                        |

### Human review should test

- Facts, arithmetic, dates, tax rates and deadlines.
- Primary sources and whether citations actually exist.
- Assumptions, omissions and invented content.
- Whether the result is suitable for the task and consistent with the engagement or business purpose.

# IF SOMETHING GOES WRONG - ACT FAST, STAY CALM

Not every mistake is reportable, but every mistake should be contained, assessed and documented.

| When                           | Immediate priorities                                                                                                        | Evidence to keep                                             |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|
| First 10 minutes               | Stop the activity; secure/revoke live exposure; preserve key evidence.                                                      | Conversation/file ID; account; timestamps; visible settings. |
| First hour                     | Escalate internally; identify what left, where it went and who could access it.                                             | Internal timeline; access/sharing state; named owners.       |
| Within 24 hours                | Assess likely impact; contact supplier if needed; document known facts and uncertainties.                                   | Vendor ticket; response; preliminary risk assessment.        |
| Within 72 hours where relevant | Complete breach-risk and notification assessment; decide whether regulator/people/client/customer notification is required. | Reasoned decision; approvals; copies of notices.             |
| After stabilising              | Confirm deletion/retention facts; correct controls; brief staff; update register/policy.                                    | Corrective actions; owner; due date; closure evidence.       |

## The four facts

| What                                                       | Where                                                                 | Who                                                                | When                                                               |
|------------------------------------------------------------|-----------------------------------------------------------------------|--------------------------------------------------------------------|--------------------------------------------------------------------|
| Exact data, people, sensitivity, identifiers, attachments. | Product, account/workspace, region, IDs, integrations, sharing links. | Supplier staff/reviewers, users, subprocessors, public recipients. | Training/evaluation, retention, exports, actions, deletion status. |

**DO NOT MAKE IT WORSE**

Do not conceal the incident, forward sensitive screenshots unnecessarily, retry the prompt in another tool, or promise that information is deleted merely because a user clicked delete.

## 72-HOUR DECISION PATH

Use this as a navigation aid - then document the assessment.

| Question                                                     | IF YES                                                                                                        | IF NO / UNCERTAIN                                                                       |
|--------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| Could personal data or confidential information be involved? | Contain and establish the four facts.                                                                         | Record why the incident is outside this route; still consider confidentiality/security. |
| Could the incident create risk to people?                    | Complete a reasoned breach-risk assessment promptly.                                                          | Record the reasons and any mitigations.                                                 |
| Is regulator notification required?                          | Where UK GDPR threshold is met, notify without undue delay and, where feasible, within 72 hours of awareness. | Record the decision not to notify and keep evidence.                                    |
| Is the risk to people high?                                  | Consider whether affected individuals must also be informed without undue delay.                              | Record why individual notification is not required.                                     |
| Are there separate contractual/professional duties?          | Assess client/customer, contractual, professional and insurance obligations separately.                       | Do not assume 'not reportable to ICO' means 'nothing else to do'.                       |

### Vendor questions that matter

- Was the content used for training, evaluation or human review?
- Who or what accessed it, including subprocessors?
- Where was it processed and what residual copies or backups remain?
- Can the supplier confirm containment and deletion status with evidence?
- What incident or audit logs can the supplier preserve?

#### PRACTICAL INSIGHT

Regulatory, contractual and client/customer relationship decisions are related but separate questions. Take specialist advice where the incident is significant, sensitive or uncertain.

## 30-DAY IMPLEMENTATION ROADMAP

| Week                     | What to do                                                                                                                  | Evidence at week end                                                      |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| 1 - OWN & INVENTORY      | Name the AI owner; stop unapproved personal accounts; list current AI tools/features and uses; issue an interim staff rule. | Named owner; inventory; interim instruction; escalation route.            |
| 2 - CLASSIFY & APPROVE   | Classify uses by risk; approve/restrict/prohibit each use; collect supplier terms and settings evidence.                    | Populated register; evidence links; unresolved-questions list.            |
| 3 - CONFIGURE & REHEARSE | Complete DPIA decisions where relevant; update wording/privacy information; configure accounts; run an incident rehearsal.  | DPIA decisions; approved wording; settings evidence; exercise notes.      |
| 4 - EMBED & REVIEW       | Publish the register and incident route; train staff; sample-check real use; close gaps; set next review date.              | Training record; sample check; corrective actions; quarterly review date. |

### 30-MINUTE ACTION

Run a fictional scenario: a bank statement or employee file was pasted into a personal chatbot account. Ask the team to show who they contact, what they preserve, what vendor questions they ask and what information is still missing before a notification decision.

### What a successful rollout looks like

- Staff know which account they may use and what they must never paste into an unapproved service.
- Managers can show the exact tool/use-case approval rather than saying 'IT said it was fine'.
- Client/customer restrictions can be found and applied in practice.
- A live incident can be escalated without searching for a process under pressure.
- The register has a next-review date and somebody is accountable for it.

# HOW TO REVIEW AI USE EACH QUARTER

A practical six-part review with a small set of measures to show whether controls are working.

| Measure                      |  | Response  |
|------------------------------|--|-----------|
| Approved tools in active use |  | [ ]       |
| Recorded active AI use cases |  | [ ]       |
| Staff trained / total staff  |  | [ ] / [ ] |
| AI incidents this quarter    |  | [ ]       |
| Tools/use cases reviewed     |  | [ ]       |
| Open governance actions      |  | [ ]       |

| Review area                      | What to ask                                                                     | Typical evidence/output                      |
|----------------------------------|---------------------------------------------------------------------------------|----------------------------------------------|
| Tools                            | Are exact products, plans, terms, settings and subprocessors still as approved? | Register updated; outdated approvals closed. |
| Use cases                        | Are staff using AI only for recorded purposes and data categories?              | Use-case register; new uses assessed.        |
| Access & integrations            | Are accounts managed, leavers removed and connectors still necessary?           | Access review; unused connectors removed.    |
| Clients/customers & transparency | Are restrictions and privacy/engagement wording still accurate?                 | Restrictions checked; wording updated.       |
| Incidents & lessons              | What incidents or near misses require a control change?                         | Incident log; corrective actions.            |
| Training & behaviour             | Do staff understand GO / CHECK / STOP and the escalation route?                 | Training status; scenario feedback.          |

HOW TO READ THE MEASURES

They are not performance targets by themselves. For example, '0 incidents' could mean strong controls - or poor reporting. Use the numbers to ask better questions and spot change over time.

## READ FURTHER & KEY TERMS

Use authoritative live sources when you need current technical or regulatory detail.

| Source                                              | Why it matters                                                              |
|-----------------------------------------------------|-----------------------------------------------------------------------------|
| Information Commissioner's Office (ICO)             | AI and data protection; accountability; personal-data breach handling.      |
| National Cyber Security Centre (NCSC)               | AI security and secure system-development principles.                       |
| ICAEW / ACCA / AAT and relevant professional bodies | Professional ethics, AI adoption and practice considerations.               |
| HMRC / GOV.UK                                       | Current tax, regulatory and government guidance where relevant to the task. |

### Key terms

| Term         | Plain-English meaning                                                                                           |
|--------------|-----------------------------------------------------------------------------------------------------------------|
| AI           | Artificial intelligence.                                                                                        |
| ICO          | Information Commissioner's Office - UK data-protection regulator.                                               |
| UK GDPR      | UK General Data Protection Regulation.                                                                          |
| DPIA         | Data Protection Impact Assessment - a structured assessment for processing that may create high risk to people. |
| MFA          | Multi-factor authentication.                                                                                    |
| API          | Application programming interface - a method software uses to connect with another system.                      |
| Subprocessor | Another supplier used by your main supplier to process data.                                                    |

#### VERSION NOTE

Guidance reviewed for this inspection edition in August 2026. AI products, supplier terms and regulatory guidance can change. Check live authoritative sources before relying on time-sensitive detail.

# AI USE SUMMARY TREE

A one-page recap of the decision method.

| Step | Question                                        | If clear                  | If not clear         |
|------|-------------------------------------------------|---------------------------|----------------------|
| 1    | Is the data permitted for this use?             | Continue                  | CHECK or STOP        |
| 2    | Is the purpose legitimate and defined?          | Continue                  | CHECK                |
| 3    | Is the exact tool/account/workspace approved?   | Continue                  | STOP until approved  |
| 4    | Are the AI's actions limited and controlled?    | Continue                  | CHECK / STOP         |
| 5    | Is competent human review and evidence defined? | GO if all gates are clear | CHECK until resolved |

| GO                                                       | CHECK                                                    | STOP                                                         |
|----------------------------------------------------------|----------------------------------------------------------|--------------------------------------------------------------|
| Lower risk, approved use.<br>Proceed with normal review. | Clarification, approval or stronger controls are needed. | Do not proceed with real data until specifically authorised. |

THE PRACTICAL RULE

Use AI as a controlled supplier and assistant - not as a blank notepad, unquestioned expert or autonomous decision-maker.

## Your five implementation resources

- AI Acceptable-Use Policy
- Approved AI Tool & Use-Case Register
- AI Data Incident Response Record
- Client & Business AI Wording Pack
- AI Staff Quick Check

## FREE EDITION, PERMITTED USE & DISCLAIMER

This guide and its accompanying implementation resources are made available free of charge by [theperry.co.uk](https://theperry.co.uk).

### Permitted use

- You may download and retain the guide for personal reference or internal use within your own organisation.
- You may print reasonable copies and adapt the implementation templates for that permitted internal use.
- You may link other people to the official download page on [theperry.co.uk](https://theperry.co.uk).

### Not permitted

- Do not sell the files, present them as your own work, remove copyright notices, or use them to create a competing guide or template product.
- Do not upload the original pack to public or shared repositories. Share the official [theperry.co.uk](https://theperry.co.uk) download page instead.

### IMPORTANT DISCLAIMER

This publication provides general educational information about responsible AI use. It does not provide accounting, tax, legal, data-protection or other professional advice and is not a substitute for advice based on individual circumstances. AI products, law, professional requirements and supplier terms change over time; verify current requirements before implementation.

### Support, corrections and current information

Visit [theperry.co.uk](https://theperry.co.uk) for the current publication page, related articles, corrections and newer resources. This free edition does not include an entitlement to future editions or individual support.

**PROTECT | APPROVE | REVIEW | RESPOND | IMPROVE**