

CLIENT & BUSINESS AI WORDING PACK

Adaptable client/customer, privacy, due-diligence and incident wording

BEFORE USE

Do not copy these clauses into every contract or engagement unchanged. Align them with the actual AI tools, controller/processor position, privacy notice, supplier arrangements, services and instructions.

1. General AI-enabled technology clause

DRAFT CLAUSE

We may use appropriately controlled technology, including AI-enabled software, to support administrative and analytical aspects of our work. We remain responsible for our work and apply human review and confidentiality controls. We will not use your information in a way that is inconsistent with our agreed services, applicable law, our privacy information or a specific instruction you give us. Please tell us if you have a specific restriction concerning AI use so that we can record and apply it.

2. More specific controlled-use version

DRAFT CLAUSE

To help deliver services efficiently, we may use approved AI-enabled functions within software and business workspaces that we have assessed for the intended use. Where confidential or personal information is involved, we apply appropriate access, confidentiality, security and human-review controls and remain responsible for the final work. We do not permit staff to place confidential information into unapproved public AI services. Further information about our use of technology and information is available in our privacy notice.

3. Privacy notice - technology and AI paragraph

DRAFT PARAGRAPH

We use technology to provide and administer our services. Some approved systems may include AI-enabled functions that assist with tasks such as drafting, summarising, searching or analysing information. We assess the intended use, access controls and supplier arrangements before approving material use with personal or confidential information, and we apply human review to material work. Our suppliers may process information on our behalf under their contractual arrangements. Further details about recipients, transfers, retention and your rights are set out elsewhere in this privacy notice.

4. Client/customer restriction acknowledgement

DRAFT ACKNOWLEDGEMENT

We have recorded your instruction that [Business/Practice name] must not use your information with [AI-enabled tools / specified tool or use]. We will apply this restriction to the services we provide from [date]. This may affect how some tasks are completed and may require an alternative process. Your contact is [name/role]. Please tell us if the instruction changes.

5. Response to 'Do you use AI with our data?'

DRAFT RESPONSE

We use approved technology, including some AI-enabled functions, where it is suitable for the service and our controls allow it. We do not treat public AI tools as a place to paste confidential files. We assess the product and intended use, use controlled business accounts where appropriate, restrict unapproved sharing, and require human review of material work. If you have a specific restriction concerning AI use, we can record and apply it.

6. Tender / due-diligence response

Question	Draft response
Governance	We maintain an AI acceptable-use policy and an approved tool/use-case register with named ownership and periodic review.
Confidential / personal data	Such data may only be used where the exact tool, account/workspace and use case have been approved for that information.
Access controls	Approved business accounts use managed access controls and MFA where available; personal accounts are not permitted for controlled business work unless specifically authorised.
Supplier checks	Our approval process considers contractual/data-processing terms, retention, training/evaluation use, subprocessors, processing locations, security and deletion.
Human review	AI does not replace responsibility. Material output is reviewed by a competent person before reliance or external communication.
Incidents	We maintain an escalation and incident-record process covering containment, supplier contact, risk assessment, notification decisions and corrective action.

7. Holding statement after an incident

USE ONLY WHEN ACCURATE AND AUTHORISED

We are investigating an information-handling incident involving [brief factual description]. We have taken immediate steps to contain it, including [steps]. We will provide a further update by [date/time].

8. Follow-up update structure

Section	What to cover
What happened	Concise factual description; date/time; affected service or process.
Information involved	Categories of information; avoid unnecessary repetition of sensitive data.
Containment	Actions taken and supplier response.
Risk assessment	What is concluded so far and what remains uncertain.
Notifications	Any regulator/individual/client/customer notifications made or under assessment.
Corrective action	Control changes, future restrictions and review.
Contact	Named person/role for questions.

9. Internal checklist before issuing wording

- Does the statement describe the systems and use that actually occur?
- Is it consistent with the contract/engagement and privacy notice?
- Have specific restrictions been checked?
- Does it accidentally promise that no AI is used anywhere in the software stack?
- Does it imply deletion, confidentiality or security outcomes the business cannot evidence?
- Has the appropriate owner/privacy/engagement lead approved the wording where needed?

TEMPLATE STATUS

Adaptable drafting aids, not legal advice. Review against actual processing, contracts, privacy information and professional obligations.