Avantwerk | LEGAL AI

FREE RESOURCE · FOR SOLICITORS

Before your firm adopts an AI tool: supplier due-diligence checklist

For solicitors and small firms in England and Wales. This educational checklist does not cover Scotland or Northern Ireland and is not a compliance certificate.

Start with a defined task: summarising attendance notes, researching a point of law or preparing a first draft. Approval should identify the task, permitted information and controls. A successful demonstration alone does not establish suitability for client work.

The SRA Code requires competent service, appropriate supervision and protection of client confidentiality. Those responsibilities remain relevant when work involves AI. See paras. 3.2, 3.3, 3.5 and 6.3 of the SRA Code of Conduct for Solicitors.

For each question, retain the evidence, record the answer and identify any unresolved condition.

1. What work are we approving?

Ask for evidence: Product documentation, known limitations and a demonstration using fictional information drawn from a representative task.

Record: Approved tasks, prohibited uses, permitted users and a named responsible lawyer. Specify whether approval covers a fictional-data trial or live matters. Treat research, drafting and autonomous external actions as separate decisions.

2. Where does information actually go?

Ask for evidence: A data-flow diagram covering uploads, prompts, retrieved documents, outputs, logs, backups, support access, model providers and optional integrations.

Record: Each recipient, processing location and access route. Establish what leaves the firm's systems. Local installation can still involve external services; cloud hosting requires examination of its actual controls. Neither description settles suitability.

3. Can we protect client confidentiality?

Ask for evidence: Contractual confidentiality commitments, staff-access restrictions, support procedures and controls against disclosure to other customers.

Record: Permitted information categories, exclusions and whether redaction or pseudonymisation is required. Under para. 6.3 of the SRA Code, client affairs remain confidential unless disclosure is required or permitted by law or the client consents. Record the basis for any proposed disclosure; avoid assuming blanket consent.

4. Have we assessed legal professional privilege separately?

Ask for evidence: The supplier's access and disclosure terms, onward-sharing arrangements and procedures for legal demands.

Record: The responsible lawyer's assessment before privileged material is submitted. Confidentiality and legal professional privilege are distinct. A confidentiality clause does not itself establish that privilege will be preserved. Identify uncertainty about disclosure or waiver and keep affected material outside the trial until resolved.

5. What are the parties' data-protection roles?

Ask for evidence: A description of each processing purpose, including account administration, service delivery, security monitoring and any reuse of information.

Record: The firm's and supplier's roles for each activity. Where processing is carried out on the firm's behalf, obtain the contract required by art. 28 UK GDPR. Do not assume every provider is a processor for every purpose. Separately assess any processing for the supplier's own purposes.

6. Can information be reused or retained?

Ask for evidence: Binding terms and settings covering model training, service improvement, human review, abuse monitoring and retention of prompts, documents and outputs.

Record: Which uses are permitted, which are disabled, who can change settings and what evidence confirms the configuration. Clarify whether contractual promises cover all relevant services and plans. "No training" does not answer questions about logging, access or retention.

7. Who else processes the information?

Ask for evidence: Relevant subcontractors and model providers, processing and support locations, change-notification arrangements and documents addressing international transfers.

Record: Whether the proposed arrangements are acceptable for the intended information and matters. Identify any applicable transfer requirements and the evidence supporting their satisfaction. A UK storage address alone does not describe overseas support access or every onward disclosure.

8. How will access and incidents be controlled?

Ask for evidence: Authentication options, permissions, separation between firms and matters, encryption arrangements, security testing summaries and the incident-contact process.

Record: Required settings, the administrator and the escalation contact. Test a departing user's access removal using fictional material. Establish how the supplier will give the firm enough information to assess an incident and take necessary action.

9. What risk assessment does this use require?

Ask for evidence: Information about data categories, affected people, scale, intended outputs and how the tool influences decisions.

Record: The firm's risk assessment and whether a data protection impact assessment is required. Under art. 35 UK GDPR, a DPIA is required where the proposed processing is likely to result in high risk to individuals' rights and freedoms. Document the reasoning; AI use alone does not answer that question.

10. Can lawyers check the output properly?

Ask for evidence: Source links, document references, jurisdiction controls, currency information and examples of known failure modes.

Record: Who checks facts, calculations, legal propositions and citations before reliance or external use. Open cited authorities and confirm that they support the proposition. Check the underlying documents for summaries. The SRA's warning on misuse of AI addresses risks including inaccurate material and confidentiality.

11. Will the controls survive everyday use?

Ask for evidence: Training materials, administrative controls, change notices and test results using fictional matters, incomplete facts and misleading instructions embedded in uploaded documents.

Record: Training completed, test failures and required corrections. Include a test for information from one matter appearing in another. Define who may approve new features, providers or integrations and what changes require reassessment.

12. Can we stop using it safely?

Ask for evidence: Export formats, cancellation terms, account closure procedures and deletion arrangements covering working copies, logs and backups.

Record: What the firm must preserve on the matter file, how exports will be checked and what deletion confirmation is available. Distinguish account closure from completed deletion. Test the exit process with fictional information before relying on it for live work.

Keep a short approval record

Use this in the firm's existing procurement or risk file:

- **Supplier, service, plan and version:**
- **Responsible lawyer and decision date:**
- **Approved tasks, users and information:**
- **Evidence reviewed, including dated terms and settings:**
- **Fictional-data tests and results:**
- **Decision:** approved / approved with conditions / further evidence required / declined.
- **Conditions, owner and completion evidence:**
- **Review date and triggers:** changed terms, models, recipients, integrations, incidents or intended use.

Unanswered questions should become explicit conditions or restrictions. The resulting record should explain why this particular use is acceptable and how the firm will supervise it.

Edition 1.0.0 (first edition). Law and guidance checked: 8 November 2026. Native content reviewed: 8 November 2026. Next planned review: 8 February 2027.

Check for a newer edition before relying on this checklist. Changes to law, guidance or the proposed use can require an earlier review.