Avantwerk | LEGAL AI

FREE RESOURCE · FOR SOLICITORS

A working AI-use policy for a small law firm

For solicitors and small firms in England and Wales. Complete the fields and settle the decisions before adopting this template. It is an educational starting point, not a finding that the firm's arrangements comply with its obligations. It does not cover Scotland or Northern Ireland.

Firm: [name]. **Policy owner:** [name and role]. **Approver:** [name]. **Effective date:** [date]. **Next internal review:** [date chosen by firm]. **Existing policies linked:** [information security, supervision, procurement and incident procedures].

1. Scope and permission

This policy applies to [staff, partners, contractors and other users specified by the firm] using AI for firm business, including tools embedded in ordinary software. Users must obtain approval for the actual service, account, feature and task. A personal account or free trial is not approved merely because a similar paid service is approved.

Maintain the following table in the firm's existing software register:

SERVICE, ACCOUNT AND FEATURE	APPROVED TASK	PERMITTED INFORMATION	APPROVED USERS	RESPONSIBLE SOLICITOR	RESTRICTIONS AND EVIDENCE
[complete]	[complete]	[fictional only / specified live information]	[complete]	[complete]	[complete]

Until an entry is approved, use fictional information only. Approval for one matter or feature does not extend to another purpose, connected service or newly enabled model.

2. Information before input

Before submitting material, the user checks the approved information categories and the actual destination. Exclude passwords, access tokens and other credentials. Remove information that is unnecessary for the task; consider whether a generalised question can serve the same purpose.

Record the basis for any disclosure of client affairs. Para. 6.3 of the SRA Code permits exceptions for law and client consent; do not treat a policy acknowledgement as blanket consent. Assess legal professional privilege separately. Supplier confidentiality terms do not decide whether a

particular disclosure could affect privilege. Where that assessment is unresolved, keep the affected material out and refer it to the responsible solicitor.

Use the firm's approved data-protection assessment and supplier records. Replacing names may leave a person identifiable through context. Do not describe information as anonymous merely because direct identifiers have been removed.

3. Human review and responsibility

Every output remains a working draft until checked for its intended use. The preparer checks facts against the source documents, calculations independently, and legal propositions against authorities actually opened. Identify jurisdiction, relevant date, missing facts and contrary material. Use the separate research-checking checklist when legal research is involved.

A solicitor reviews every generated client, court or matter document before it is used, signed, filed or sent. Record the reviewer, date, version and material limits of the review. A tool must not send, file, accept terms, give an undertaking or make a decision for the firm under this policy. Any proposed automated action requires its own express assessment and authority.

4. Training and supervision

The policy owner records induction and refresher training appropriate to each role. Training includes invented citations, misleading summaries, unsafe disclosure and instructions concealed in uploaded material. Supervisors select checks appropriate to the work and the user's competence; pressing an approval button is not evidence of substantive review.

Paras. 3.2, 3.3 and 3.5 of the SRA Code address competent service, competence and supervision. The SRA AI warning reinforces the need for safeguards and human oversight.

5. Errors, records and changes

Users report suspected disclosure, cross-matter information, fabricated authority or unexpected external action immediately to [internal contact and route]. Stop the affected use, preserve relevant evidence securely and follow the existing incident procedure. The responsible person assesses correction, communication and any reporting obligations; this policy sets no universal reporting deadline.

Keep the evidence needed to explain work on the appropriate firm or matter record. Avoid unnecessary duplicate client material in an AI chat history. Apply the firm's assessed retention and access arrangements.

Reassess changed terms, recipients, features, uses and incidents. **Adoption record:** [completed fields; tested restrictions; staff informed; unresolved conditions and owners; approver and date]. Conditions remain visible until evidence closes them.

Edition 1.0.0. Law and guidance checked and native content reviewed: 9 November 2026. Next planned content review: 9 February 2027. Check for a newer edition; changes may require earlier review.