AI Explained · Confidentiality and Privacy, Part 2

Can I Put a Client's File into AI?

By Dr Peter Fields

THE 2-MINUTE SUMMARY

Sending client material to an AI service without authority can breach confidentiality even if nobody opens the file. Find out who could read it, for what purpose and under what duty of confidence.[1,2,8]

Clients and lawyers are already using AI to research, review and draft. Some law firm professionals say they use tools their firms have not authorised. That tells us something about practice, but leaves the rate of actual confidentiality breaches unknown.[9,10]

In my view, the strict duty is justified. Meeting it can be expensive and can limit what a tool does. A policy that makes the approved route too difficult under deadline pressure gives people a reason to take the shortcut.

A client emails you about a dispute at work. You want to paste the email into a chatbot to help draft a reply, much as you might with the private email in Part 1. You have a decision to make before pressing Send. May you entrust the email to this service on its terms?

What the rules actually say

Solicitors must keep current and former clients' affairs confidential unless disclosure is required or permitted by law or the client consents. Barristers have a corresponding duty under CD6 and rC15.5, which expressly refers to informed consent. The Bar Standards Board treats use of AI as outsourcing under rC86. The barrister remains responsible for the work and must be satisfied that the arrangement protects confidentiality. A provider's terms may tell you what it can do with a file. Your authority to let it do those things must come from elsewhere.[1]

In practice, ask three questions. **May I send it?** Check who can authorise the disclosure, any client restrictions or court orders, and whether the supplier must keep it confidential. **Is it privileged?** Privilege protects qualifying material from compulsory disclosure. It belongs to the client, and a disclosure inconsistent with maintaining confidence can put it at risk. **Does it contain personal data?** Identify a lawful basis and any extra condition needed for special category data. Where the supplier is a processor, the UK GDPR requires a contract covering documented instructions, confidentiality and subprocessors. Assess the risks beforehand, with a data protection impact assessment where processing is likely to pose a high risk to people.[1,2,3]

When does possible access matter?

Suppose the provider's terms let reviewers read a client's email for model improvement. The lawyer needs authority to make the email available for that purpose, regardless of whether a reviewer opens it. Limited access by support staff bound to keep the material confidential calls for a different assessment. Ask what each person is allowed to do with the file and what prevents them using it for another purpose.[1,2,5,6,7]

In *UK and Munir*, the Upper Tribunal said that putting client letters and Home Office decisions into ChatGPT put the information into the public domain, breached confidentiality and waived privilege. Those were observations in a hearing about professional conduct. The reasons identify no public reader and give no analysis of human-review terms. The SRA warns of a likely breach and possible waiver in the circumstances described. The Tribunal cited Microsoft Copilot as a tool it considered free of those risks. In practice, check which Copilot account and features are in use, including where web search sends the material.[1,8,13]

Property Alliance Group v RBS illustrates why the terms of a disclosure matter to privilege. RBS showed or supplied six privileged documents to regulators on confidential terms. The court held that the regulators' reserved powers, including possible publication, left privilege intact on the facts. A separate issue arose when RBS relied on gaps in the regulators' findings to argue that its misconduct went only so far. The court then ordered inspection of the same six documents.[2]

What clients and lawyers are doing

Clients may have consulted a chatbot before their first conference. About one in six (233 of 1,428) UK participants with a recent legal dispute in a study by JUSTICE and the Administrative Fairness Lab said they had used a chatbot for help. One participant shared a conversation in which they had pasted an email from their own lawyer to have it explained. In *Al-Haroun*, a solicitor relied on citations his client said came from public AI tools and other online sources. The case concerned accuracy. The Divisional Court said lawyers must check AI-assisted legal research against authoritative sources before relying on it, whoever did the research.[4,9]

Thomson Reuters identified document review, summarising and drafting among the uses reported by legal professionals. In a separate 2026 survey, 34% of law firm respondents said they used AI tools their firms had not authorised for work. The sample included non-lawyers and most respondents were in the US. The SRA has reported seeing confidential client information entered into public AI systems. How often unauthorised use leads to a breach remains unknown.[1,10]

What changes with a different account

The same task can carry different risks on different accounts. Here is what to check before sending the client's email.

Account used	Could this breach a duty or regulation?	Who might read or obtain it?
Personal AI account Free or paid general-purpose chatbot	Check whether you have authority to share the material on the provider's consumer terms. Switching off training changes one of the permitted uses.[1,5]	Provider staff or contractors may be allowed to review content. Anyone given a share link may be able to read or copy the exchange.[5]
Managed business or enterprise workspace Such as ChatGPT Business or Enterprise	An appropriate contract and configuration can make approved work possible. Check the actual plan, retention, permissions and connected tools against the matter's requirements.[3,6]	OpenAI's business products exclude training by default. Provider access can still be permitted for limited reasons that vary by plan. Authorised staff within your organisation may have access through administrative or compliance tools.[6]
Specialist legal AI Harvey, Vincent, Legora or CoCounsel	Check whether the order form protects the material for this matter, including what other suppliers and optional features may do with it.[1,7,11]	Check who can see or download files within a matter team, what support staff can access and what outside services receive.[7,11]

Where does the work go?

Harvey says it stores uploaded originals and keeps their search indexes (embeddings) under the source documents' retention policy. That helps explain how work survives logout even where the model provider keeps no durable copy of the request. Harvey's data processing agreement allows for US transfers unless exclusive processing and storage elsewhere have been agreed in writing. At its September 2026 launch, Harvey said the opt-in Fable 5.1 model would process requests only in the US. Eligible customers could use it with zero retention under a time-limited exemption.[7,12]

Why does the US matter? If sending personal data amounts to a restricted transfer under UK law, check which legal route permits it. Follow the data through the first overseas recipient and any further transfers. US law can also compel a covered provider to produce records in its possession, custody or control, even if the records are stored abroad.[13]

What confidentiality costs in practice

I think the regulators are right to apply the duty strictly. Putting it into practice can cost substantially more than a personal subscription. A sole practitioner may have to bear the cost of licences, contract reviews and setting up access that a large firm can spread across hundreds of users. The choice also affects what the tool can do. Microsoft says Copilot's generated Bing queries fall outside the Microsoft 365 data processing addendum and EU Data Boundary. Turn web search off and you lose live web results.[1,6,7,13]

Picture a solicitor with a long bundle and a draft due that afternoon. A familiar tool can produce a useful first pass in minutes. If the approved route means waiting for permission or spending an hour preparing a safe extract, the gain from taking a shortcut is immediate and the risk feels remote. I suspect that some of the unapproved use reported in the survey begins with this sort of calculation.[10]

A short example with a witness statement

You want a short chronology from a witness statement. You replace the witness's name with W1, the company's with C1 and the manager's with M1, and keep the key locally. The extract still reads, 'I was the only night supervisor at C1's depot on 7 March. I saw the spill that night and reported it to M1 the next morning.' The rota and incident report could identify the witness. For a simple chronology, try 'On Day 0, W1 says they saw an incident. On Day 1, W1 says they reported it to M1.' Keep the key in a separate, access-controlled place and restore any names locally.[14]

If the firm can reconnect the codes to individuals, the information remains personal data in its hands. That is pseudonymisation. Even if the people cannot reasonably be identified, the witness's account may still be confidential. If the exact date or incident matters, use a service authorised for the real material. For a task about the format of a chronology, invented facts may be enough.[1,3,14]

Geek Box · Check what actually leaves your computer

A black shape laid over a name in a PDF can leave the underlying text available to search or copy. Use a clean extract or a redaction tool that removes the underlying material. Check the file you will send, including its filename, comments and tracked changes.[15]

How to use it better

- **Start with the task.** Decide whether it needs the real file, a short extract or only an example.
- **Approve the route for this matter.** Check your authority to share and the exact product, settings and recipients. Include any tool that can search, send or share on your behalf.
- **Treat the answer as client material too.** Check it against the statement and keep it within the matter's permissions. If a file went to the wrong service, use your incident procedure promptly and assess what reporting is required.[16]

Can the rules keep up with the work?

A policy has to work when someone is about to send a file. Can a solicitor on a deadline use the approved route without stopping the job? Firms can make that route easy to find and use. Regulators can spell out what acceptable arrangements look like in practice, including what a sole practitioner or a small firm should look for when buying a service. That would give the strict rule more force at the moment it matters.

Sources and notes

1. BSB *Handbook*, CD6, rC15.5 and rC86, and *AI guidance* (May 2026), pp. 2–3, 7–9 and 11–13. SRA Codes, para. 6.3, and *Misuse of AI* (August 2026). Source 1 · Source 2 · Source 3 · Source 4 · Source 5

2. *Property Alliance Group Ltd v Royal Bank of Scotland plc* [2015] EWHC 1557 (Ch), [102], [113]–[115]. Source

3. UK GDPR, arts 5, 6, 9, 28 and 35. Source

4. *Ayinde and Al-Haroun* [2025] EWHC 1383 (Admin), [7]–[8], [73]–[81]. Source

5. OpenAI, consumer data handling and shared links. Google, *Gemini Apps Privacy Hub*, human review. Source 1 · Source 2 · Source 3

6. OpenAI, *Enterprise privacy*, Business and Enterprise FAQs, and managed account access. Source 1 · Source 2

7. Harvey, *Platform Agreement* §§7.4 and 11.6–11.8, DPA §§4, 12 and 14, and *Service Terms* §§4–9. Source 1 · Source 2 · Source 3

8. *UK and Munir* [2026] UKUT 81 (IAC), [12], [16], [21], [60]. Source

9. JUSTICE and the Administrative Fairness Lab, *What AI Chatbots Can Teach Us About Unmet Legal Needs* (2026), dataset and examples. Source

10. Thomson Reuters Institute, *2026 AI in Professional Services Report*, legal use cases, and *Future of Professionals 2026*, law firm survey (736 responses from 46 countries, 421 from the US). Source 1 · Source 2

11. vLex, *Security by Design*. Legora, *Global Terms* §§4.3.2, 7.2, 8.3.3 and 9. CoCounsel FAQs and UK product terms §§1–2 and 4.3.2.3. Source 1 · Source 2 · Source 3 · Source 4

12. Harvey, customer data and embeddings articles (March and April 2026), and Fable 5.1 launch announcement (September 2026). Source 1 · Source 2 · Source 3

13. ICO, restricted transfers and UK Extension to the EU–US Data Privacy Framework. 18 U.S.C. §§2703 and 2713. Microsoft, *Data, privacy, and security for web search in Microsoft Copilot*. Source 1 · Source 2 · Source 3 · Source 4 · Source 5

14. UK GDPR, art. 4(5) and recital 26. ICO, *Pseudonymisation* and *How do we ensure anonymisation is effective?* Source 1 · Source 2 · Source 3

15. ICO, *Disclosing documents to the public securely*, guidance on hidden information and redaction. Source

16. UK GDPR, arts 4(12), 33 and 34. See also the Dutch DPA's examples of reported workplace uploads. Source 1 · Source 2