

SAMPLE REPORT

Every AI tool in the firm, and what passed through each.

Sample Firm LLP, a fictional London law firm

FIRM	18 people: 4 partners, 6 solicitors, 1 trainee, 3 paralegals, 4 support staff
PRACTICE	Residential conveyancing, wills and probate, family
SYSTEMS IN PLACE	Microsoft 365 Business Premium, Clio Manage, Xero, Docusign, Teams and Zoom
FIELDWORK	14 to 25 September 2026
ASSESSED AS AT	25 September 2026, against UK GDPR, the Data Protection Act 2018, ICO guidance and the SRA Code of Conduct

Illustrative. Sample Firm LLP does not exist. The firm, its people and its findings are invented to show exactly what a client receives on day fourteen. Every statement about a vendor's terms is real and was checked against the vendor's own pages on 16 September 2026.

1. The slide	2. The register	3. Findings	4. Roadmap
What the partners see first	All 14 systems, scored	The five that matter most	Stop, replace, govern

1 · THE SLIDE

What the partners see first.

Which AI tools are the people at Sample Firm LLP using, and what client information has gone into them?

14

AI systems in use across 18 people

12

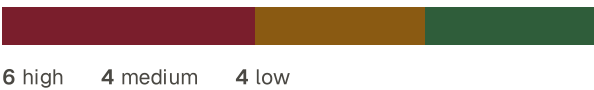
never approved by anyone at the firm

6

rated high exposure: client data reaches a provider that may train on it, with no contract

- 1 Client call transcripts, including family matters, sit in two partners' **personal Otter accounts**.
- 2 **9 of 18** people use personal ChatGPT accounts for matter summaries, letters and attendance notes.
- 3 A will and French probate correspondence went through **free DeepL**, which trains on text with no opt-out.

EXPOSURE ACROSS THE REGISTER



IN THIRTY DAYS, IF THE ROADMAP IS FOLLOWED

The 6 high-exposure systems are switched off or replaced with tools the firm already pays for. Every system left on the register has a partner's recorded decision. Direct cost of the replacements: one DeepL Pro licence.

2 · THE REGISTER

Register of AI systems in use.

REF.	SYSTEM	USED BY	CLIENT DATA PASSING THROUGH	VENDOR'S TRAINING POSITION	APPROVED	EXPOSURE
R01	ChatGPT Personal Free and Plus accounts	9 of 18 staff	Matter summaries, draft letters, attendance notes	Trains on inputs unless the user switches it off; the switch is on by default	☐	HIGH
R02	Microsoft Copilot Personal Microsoft accounts	3 staff	Draft client emails, lease extracts	UK personal accounts are trained on by default unless switched off	☐	HIGH
R03	Microsoft 365 Copilot Chat Firm sign-in	11 staff active	Documents inside the firm's tenancy	Does not train on prompts or firm data under a work sign-in	☒	LOW
R04	Otter.ai (OtterPilot) Two personal accounts	2 partners	Client call transcripts, including family matters	Trains on de-identified recordings and transcripts; no opt-in step	☐	HIGH
R05	Read.ai meeting notes Arrived through a client's invite	4 firm meetings	Meeting summaries emailed to every attendee	Unclear: marketing page and privacy policy disagree	☐	MEDIUM
R06	Grammarly Free browser extension	5 support staff	Everything typed in the browser, including Outlook and Clio	Trains on individual accounts by default; can be switched off	☐	HIGH
R07	DeepL Translator Free web version	1 solicitor	A will and correspondence with a French notaire	Free tier trains on submitted text, with no opt-out	☐	HIGH
R08	AI sidebar extension Vendor not on our list	1 paralegal	Every page viewed, including the case management system	Unknown: terms could not be verified	☐	HIGH
R09	Clio Duo Firm licence	4 fee-earners	Matters, documents, emails and billing inside Clio	Does not train external models; own-model position to confirm	☒	LOW
R10	Docusign AI Firm account, default settings	Firm-wide	Signed engagement letters, transfer deeds	AI training licence is on until an admin switches it off	☐	MEDIUM
R11	JAX in Xero Firm subscription	Cashier, practice manager	Office account ledgers	Does not train; included in every UK plan with no off switch	☐	LOW
R12	Apple Writing Tools with ChatGPT Linked to a personal Plus account	1 partner, personal iPhone	Client emails rewritten on the phone	Once linked to a personal account, ChatGPT consumer terms apply	☐	MEDIUM
R13	Claude Personal Pro account	1 trainee	Research questions containing client facts	Trains when 'Help improve Claude' is on, which is pre-selected	☐	MEDIUM
R14	Canva Magic Studio Free account	Practice manager	Newsletters and marketing; no client data found	Uses content to improve AI features unless switched off	☐	LOW

Vendor positions as published by each vendor on 16 September 2026. A filled square means a partner made a recorded decision to allow the system. Exposure combines two things: whether client information reaches the system, and what the vendor may do with it. High: client data reaches a provider that may train on it or whose terms are unknown, with no contract with the firm. Medium: limited client data, or a default setting that one admin change removes. Low: firm contract in place, or no client data found. Vendor positions change; each row is re-checked before a report is issued.

3 · FINDINGS

The five that matter most.

1

R04

HIGH

Client call transcripts sit in two partners' personal Otter accounts

WHAT WE FOUND

Calendar review: OtterPilot attended 37 meetings in the last 90 days, 11 of them calls with family-law clients. Both accounts were opened with firm email addresses and paid on personal cards.

THE VENDOR'S POSITION

Otter's privacy policy (16 June 2026) lists training its own AI on de-identified recordings and transcripts, with no opt-in step and no carve-out for paid plans. On 13 August 2026 a US federal court allowed a privacy class action against Otter to proceed.

WHY IT MATTERS

No processing contract exists between the firm and Otter (UK GDPR Art. 28). Family matters routinely carry health and other special category data (Art. 9). The SRA Code requires client affairs to be kept confidential (para. 6.3).

ACTION

Stop today. Export what the partners need, then delete both accounts. Teams transcription is already in the firm's licence and does not train.
Managing partner · Day 2

2

R01

HIGH

Half the firm uses personal ChatGPT accounts for client work

WHAT WE FOUND

Seven people said so in the questionnaire. The mailbox search found nine ChatGPT welcome emails sent to firm addresses; card statements show three Plus subscriptions claimed as expenses.

THE VENDOR'S POSITION

OpenAI's help centre (checked 16 September 2026): content from Free, Plus and Pro may be used to train its models, and the 'Improve the model for everyone' switch is on by default. Memory is on by default and keeps facts across chats.

WHY IT MATTERS

Matter summaries and attendance notes are client confidential information sent to a provider with no contract with the firm and a right to train on it.

ACTION

Move the work to Microsoft 365 Copilot Chat under the firm sign-in, already licensed at no extra cost. Adopt the AI usage policy. Ask the nine to switch training off and delete client chats while the move happens. Practice manager · Day 7

3

R07

HIGH

A will and French probate correspondence went through free DeepL

WHAT WE FOUND

Interview with the private client team: one solicitor translates correspondence with a French notaire on the free DeepL website, around twice a month.

THE VENDOR'S POSITION

DeepL's privacy policy for free services: submitted text is processed 'to train and improve our neural networks', and free users are told not to submit personal data. DeepL Pro deletes text after translation and excludes training.

WHY IT MATTERS

Wills and estate correspondence identify beneficiaries, assets and family circumstances. There is no opt-out on the free tier.

ACTION

Move to DeepL Pro or to Microsoft Translator, which does not store text. One licence covers the need. Head of private client · Day 3

4

R08

HIGH

A browser extension can read every page a paralegal opens, including Clio

WHAT WE FOUND	Extension review on the paralegal's laptop: an AI sidebar with permission to 'read and change all your data on all websites', installed eight months ago.
THE VENDOR'S POSITION	The developer is not on our list of 134 verified vendors and its terms could not be confirmed. We treat it as training until the vendor confirms otherwise in writing.
WHY IT MATTERS	Anything visible in the browser, including matter records in Clio, is available to a party the firm has never assessed.
ACTION	Remove today. Ask the IT supplier to turn on an extension allow-list through Intune, which Business Premium already includes. IT supplier · Day 1

5

R06

HIGH

Free Grammarly runs inside Outlook and Clio on five machines

WHAT WE FOUND	Extension review: the free Grammarly extension on all four support staff machines and one fee-earner's.
THE VENDOR'S POSITION	Grammarly (now Superhuman): 'Product Improvement and Training is on for individual users by default.' When switched off, typed content is not used for training.
WHY IT MATTERS	The extension sees every email and document typed in the browser, including completion statements and client letters.
ACTION	Switch training off on all five accounts today, then replace with Microsoft Editor, already in the licence. Practice manager · Day 7

Legal reading shown for illustration. In a client report, every legal conclusion is reviewed by an independent solicitor or data protection officer before it reaches the partners. Technical findings are signed by Riserbo.

Also on the register. Docusign's AI training licence is on by default in the firm account (R10): one admin switch. A client's Read.ai bot joined four firm meetings and emailed summaries to every attendee (R05): the Teams lobby setting stops it. JAX in Xero cannot be switched off on any UK plan (R11): it does not train, so the action is a recorded partner decision.

4 · REMEDIATION ROADMAP

Thirty days, in order.

Every action has an owner and a day. Most replacements are already in the firm's Microsoft licence.

Stop **DAYS 1 TO 2**

ACTION	OWNER	REF.
☐ Remove the AI sidebar extension; turn on an extension allow-list	IT supplier	R08
☐ Export and delete the two Otter accounts	Managing partner	R04
☐ Switch off Docusign AI training in admin settings; record the change	Practice manager	R10
☐ Switch off training on all Grammarly accounts	Practice manager	R06
☐ Block external meeting bots in the Teams lobby	IT supplier	R05

Replace **DAYS 3 TO 14**

ACTION	OWNER	REF.
☐ Move ChatGPT and personal Copilot work to Copilot Chat under the firm sign-in	Practice manager	R01, R02
☐ DeepL Pro or Microsoft Translator for the private client team	Head of private client	R07
☐ Teams transcription replaces Otter for client calls	Managing partner	R04
☐ Microsoft Editor replaces Grammarly	Practice manager	R06
☐ Unlink the personal ChatGPT account from Apple Writing Tools on the partner's phone	Partner	R12
☐ Trainee moves research to Copilot Chat; personal Claude used for nothing client-related	Supervising partner	R13

Govern **DAYS 15 TO 30**

ACTION	OWNER	REF.
☐ Partners adopt the AI usage policy; every member of staff signs it	Managing partner	All
☐ Record a partner decision on JAX in Xero and Clio Duo's own-model position	Managing partner	R09, R11
☐ DPIAs for Copilot Chat and Teams transcription	Riserbo, then partners	R03
☐ 30-minute staff briefing: the approved list and what to do after a mistake	Riserbo	All
☐ Name the register owner; first quarterly re-scan booked	Managing partner	All

COVERAGE STATEMENT

What the scan looked at, and what it could not.

A register is only as good as its sources. This page says plainly where the scan was complete and where it was not, so nobody reads more certainty into it than it holds.

SOURCE	WHAT WAS CHECKED	COVERAGE	NOTES
1	Connected apps: Microsoft 365, Google, Clio, Xero	COVERED	Admin centre exports supplied by the IT supplier
2	Browser extensions and desktop apps	COVERED	All 18 machines; three by screen-share
3	Card statements and expense lines, 12 months	COVERED	Firm cards and expense claims; personal cards not seen
4	Mailbox, by sender and subject only	COVERED	No message was opened
5	DNS and web-filter logs	PARTIAL	The IT supplier holds 30 days, not 90
6	Meetings: bots, recording and AI settings	COVERED	Teams, Zoom and 90 days of calendars
7	AI built into tools the firm already pays for	COVERED	Eight products checked
8	Phones	PARTIAL	Questionnaire for all; one partner's phone reviewed with consent

Collected: tool names, account types, dates and settings. Never collected: message content, document content or client files.

ALSO IN THE PACK

AI USAGE POLICY · EXTRACT

Approved tools and five rules

Approved for client work: Microsoft 365 Copilot Chat under the firm sign-in; Clio Duo; Teams transcription; DeepL Pro.

1. Client information never goes into a personal AI account, free or paid.
2. No meeting bot records a client call unless the firm approved it and the client was told.
3. No browser extension is installed without the practice manager's sign-off.
4. A new AI tool is added to the register before anyone uses it on a matter.
5. If client information goes somewhere it should not, tell the practice manager the same day. Nobody is disciplined for reporting.

DATA PROTECTION IMPACT ASSESSMENTS

Two DPIAs, on the ICO template

Microsoft 365 Copilot Chat, which answers from anything a user can open, so over-shared folders surface. Teams transcription for client calls, including consent and retention.

PRESENTATION

One hour with the partners

The slide, the register and the roadmap, walked through with the people who decide.

AFTER DAY FOURTEEN

The audit is a photograph. Tools change every month.

In the fortnight the vendor terms behind this report were checked, one meeting notetaker changed owner and one coding tool rewrote its UK terms. A register is out of date within weeks unless someone keeps it. That is what Ongoing Oversight is for, and why it is proposed alongside the audit rather than after it.

ONGOING OVERSIGHT · THE MONTHLY EMAIL

From: Riserbo Assurance
To: Managing partner, Sample Firm LLP
Subject: AI register, month 3

14 8	12 0	0
Tools in use	Unapproved	Incidents

One request this month: a fee-earner asked to use a transcription app. Its terms allow training, so it was declined and Teams transcription set up instead. Next re-scan 12 January.

Illustrative figures for the fictional firm.

Ongoing Oversight

Keeps the register true after the audit.

- Quarterly re-scan of extensions, connected apps and expense lines
- Policy updates when ICO guidance or the SRA moves
- An incident line for the day someone pastes the wrong thing
- Annual staff refresher, and the monthly three-number email

AI Policy and Secure Setup

Puts the roadmap in place instead of handing it over.

- Copilot Chat set up under the firm sign-in, with over-shared folders fixed first
- Extension allow-list and meeting-bot controls with the IT supplier
- Policy adopted, signed and briefed to every member of staff

This report is an informational assessment of the firm's use of AI tools against UK GDPR, the Data Protection Act 2018, ICO guidance and the SRA Code of Conduct, as at the assessment date. It is not legal advice and does not state that the firm is compliant. Legal conclusions in client reports are reviewed by an independent solicitor or data protection officer, arranged per engagement.

The same register, for your firm.

Book a free 20-minute Exposure Check · riserbo.co.uk · hello@riserbo.co.uk