CONFIDENTIAL COMPLIANCE DOCUMENT

UK + EU Combined Compliance Framework

Prepared exclusively for Halstead & Rowe Solicitors

UK and EU Jurisdiction · 08 August 2026

CONTENTS

What is in this pack

Each document below is also attached to your delivery email as its own PDF and editable Word file, so you can circulate or sign any one of them on its own.

Document	What it is for
UK GDPR Gap Analysis for AI Tools	Your AI tools measured against UK GDPR: what is satisfied, what is not, and what closing each gap takes.
AI Acceptable Use Policy	Your formal AI policy. Sign it, circulate it to every member of staff, and review it annually or whenever your AI tool usage changes.
Employee AI Guidelines — Practical Dos and Don'ts	The working-level guidance that sits under the policy: concrete examples of good and bad AI use in this business.
ICO Framework Self-Assessment	The regulator's own framework, worked through and answered.
Compliance Roadmap	The sequence to work through. Do not start a phase until the one before it is complete — the order is deliberate.
Data Classification Matrix	Which categories of your data may go near an AI tool, and which may never. The one page staff refer to before pasting anything in.
GDPR Compliance Position	Your documented data protection position for each AI tool — what a customer's procurement team asks for.
Employee AI Policy Acknowledgement Form	Each member of staff signs one. Keep the signed copies — they are your evidence that the policy was communicated, which is the first thing asked for after an incident.
Full ICO AI Auditing Framework Assessment	The detailed assessment against the regulator's auditing framework — the document to produce if you are ever audited.
Employment AI Procedures	Using AI in recruitment, monitoring or management decisions — the highest-risk use in most businesses, and the most regulated.
Automated Decision-Making Notices and Opt-Out Procedures	The notices you give when a decision is made by a machine, and the route out that the law requires you to offer.
Data Subject Rights Procedures for AI-Processed Data	How you answer an access, correction or deletion request when the data has passed through an AI system.
Sector-Specific Obligations Review	The rules that apply because of the sector you are in, on top of the general AI and data regime.
AI Risk Register	The ongoing record of AI risks, their owners and their mitigations. A live document — review it on the cadence stated at the foot.
AI Incident Response Procedure	What happens in the first hour after an AI-related incident, and who does it. The regulator clock starts before anyone has decided who is in charge.

Document	What it is for
EU AI Act Risk Tier Classification	Each AI tool placed in its risk tier under the Act, with the reasoning written down. The tier decides every obligation that follows.
Annex III High-Risk Gap Analysis	Measured against the high-risk obligations: what is in place, what is missing, and what closing each gap requires.
Article 50 Transparency Assessment and Disclosures	Where you must tell people they are dealing with AI, and the exact wording to use.
Cross-Jurisdiction Compliance Position	Where the regimes agree, where they diverge, and which obligations you satisfy once rather than twice.
AI Supply Chain Risk Review	The risk that arrives through your vendors — including the vendors your vendors use.

Also included with your purchase

- Policy review after 12 months, included in the price
- Staff briefing session (60 minutes, remote)

Reply to your delivery email to arrange these.

PART 1

Your AI Compliance Profile

Halstead & Rowe Solicitors is an 11-50 employee UK law firm using ChatGPT, Microsoft Copilot, and Lexis+ AI to draft correspondence, summarise case documents, and conduct legal research, processing personal data from conveyancing, family, and probate files including data belonging to EU-resident clients. The firm operates under both UK GDPR and the EU AI Act, with the EU Act's Article 50 transparency obligations now in force as of 2 August 2026. There is currently no AI use policy, no data protection impact assessment for AI tools, and fee earners are using unapproved tools on their own initiative, creating immediate legal privilege, confidentiality, and regulatory exposure. The combination of sensitive client data, EU-resident data subjects, and uncontrolled AI use places the firm in active non-compliance with multiple obligations across both regimes.

Maximum Fine Exposure

Maximum financial exposure must be assessed separately under each regime and cannot be consolidated into a single figure. Under UK GDPR (as the higher UK penalty tier, Art 83(5)), the maximum fine is £17,500,000 or 4% of global annual turnover, whichever is higher. The firm has not provided turnover figures, so the turnover-based limb cannot be computed; the statutory cap of £17,500,000 is the figure that can be stated. Under the EU AI Act, the applicable penalty tier for Art 50 transparency violations (the current in-force obligation) is €15,000,000 or 3% of worldwide annual turnover; again, turnover cannot be computed, so the statutory cap is €15,000,000. For EU GDPR violations relating to EU-resident client data, the maximum is €20,000,000 or 4% of global annual turnover — statutory cap €20,000,000 without turnover figures. If Art 5 prohibited-practice violations were found after 2 December 2026, the maximum EU AI Act penalty would rise to €35,000,000 or 7% of worldwide annual turnover. In a worst-case scenario involving simultaneous UK GDPR, EU GDPR, and EU AI Act enforcement — which is legally possible given the firm's dual-regime exposure — the aggregate statutory maximums would be £17,500,000 (UK ICO) plus €20,000,000 (EU DPA for EU GDPR) plus €15,000,000 (EU AI Office for Art 50), totalling approximately £17.5m + €35m at current exchange rates, before any SRA financial penalties are added. These are ceiling figures, not predictions; actual fines depend on severity, cooperation, and remediation. The firm should treat the absence of a DPA with OpenAI, the absence of a DPIA, and the absence of an AI use policy as the three highest-priority remediation items, as each represents a standalone basis for regulatory action under both UK and EU regimes.

AI Tools Inventory

Tool	Use	Risk Level	Notes
ChatGPT (OpenAI)	Drafting client correspondence; summarising case documents	**High**	Processing special-category-adjacent data (family files may contain health, financial, or family-breakdown data) and confidential client data via a third-party consumer-grade tool. No data processing agreement confirmed as in place. Data may be used to train OpenAI models unless enterprise settings are configured — legal privilege and solicitor confidentiality obligations under SRA Code of Conduct are directly engaged. EU-resident client data transferred to US servers triggers UK GDPR Chapter V and EU GDPR Chapter V transfer obligations. Under EU AI Act Art 50 (in force 2 Aug 2026), if ChatGPT outputs are presented to clients or third

Tool	Use	Risk Level	Notes
			parties, deployer disclosure duties apply now. No approved use policy exists, so staff use constitutes an unapproved deployment with no oversight controls.
Microsoft Copilot	Drafting client correspondence; research and analysis	**Limited**	If deployed via Microsoft 365 Copilot for Business or Enterprise, data protection and privacy commitments are stronger than consumer ChatGPT — Microsoft's DPA provides GDPR-compliant contractual terms and data is not used for model training by default. Risk is reduced but not eliminated: outputs must be reviewed for accuracy (Pinsent Masons May 2026 warning is directly on point). The firm must confirm which Copilot tier is in use — consumer Copilot carries the same risks as ChatGPT. EU AI Act Art 50 deployer transparency duties apply from 2 Aug 2026 if Copilot interacts with or generates content directed at data subjects.
Lexis+ AI	Research and analysis	**Limited**	Purpose-built legal research tool with contractual confidentiality commitments standard in LexisNexis enterprise agreements — substantially lower data-leakage risk than general-purpose consumer AI. Risk is limited rather than minimal because: (1) research queries may still contain client-identifying information; (2) AI-generated legal analysis must be human-verified given hallucination risk established in Italian court rulings (March 2025–March 2026) and the Pinsent Masons false-submissions case (May 2026); (3) no internal sign-off process or output-review policy currently exists. Confirm that the firm's subscription agreement includes a GDPR/UK GDPR-compliant DPA and that queries are not retained for model training.

Applicable Regulations

UK GDPR (as retained and amended)

Governs all processing of personal data by the firm in the UK. Art 5 lawfulness, fairness and transparency principles apply to AI-assisted processing. Art 6 requires a lawful basis for each use; processing special category data in family files requires an Art 9 condition. Art 25 data protection by design and by default requires that AI tools are configured to minimise data exposure before deployment — current unapproved staff use breaches this. Art 28 requires a written data processing agreement with each AI vendor before personal data is input; absence of a DPA with OpenAI (consumer ChatGPT) is an immediate breach. Art 35 requires a Data Protection Impact Assessment before processing likely to result in high risk — inputting confidential client files into third-party AI systems almost certainly meets this threshold. Art 46 and Chapter V govern international transfers; US-based AI vendors require appropriate safeguards (SCCs or UK IDTA). Art 22 (automated decision-making): the firm states AI is not used for decisions about people, so no solely automated decisions are being made, but this must be confirmed and documented — if Copilot or ChatGPT output is adopted without human review, Art 22 is engaged.

Key date: In force. Data (Use and Access) Act Part 5 provisions commenced 5 February 2026, expanding lawful bases for solely automated decisions and introducing formal safeguards. Complaints procedure duty commenced 19 June 2026 — the firm must now operate a data protection complaints procedure with set response time limits. · Max penalty: £17,500,000 or 4% of global annual turnover, whichever is higher (UK GDPR Art 83(5) as retained). Turnover-based limb cannot be computed without the firm's figures.

Data (Use and Access) Act 2025 — Part 5

Amended UK automated-decision-making framework commenced 5 February 2026. Expands the lawful bases on which solely automated decisions affecting individuals may be made and imposes mandatory safeguards (right to human review, right to contest, transparency notices). The firm's position that AI is not used for decisions about people must be formally assessed and documented; if any AI output is adopted without meaningful human review it may constitute a solely automated decision under the expanded definition. Complaints procedure duty (commenced 19 June 2026) requires the firm to operate a documented data protection complaints procedure with defined response timelines — this is a current live obligation.

Key date: Part 5 automated-decision provisions: 5 February 2026 (in force). Complaints procedure duty: 19 June 2026 (in force). · Max penalty: Enforcement is via UK GDPR penalty regime: £17,500,000 or 4% of global annual turnover.

ICO AI Auditing Framework

The ICO's framework sets out how the ICO assesses AI deployments for UK GDPR compliance. It covers accountability and governance, data minimisation in AI inputs, transparency to data subjects about AI use, and human oversight of AI outputs. The firm has no AI governance policy, no DPIA, and no oversight procedure — all of which the framework identifies as indicators of non-compliance. The ICO's November 2024 audit outcomes on AI in recruitment and its August 2026 monitoring of frontier AI safety signal that professional services using AI without governance structures are in scope for regulatory attention. Adherence to the framework is the practical route to demonstrating UK GDPR Art 5(2) accountability.

Key date: Published and operative. ICO confirmed AI as a key enforcement focus for 2024/25. · Max penalty: Not itself a penalty-bearing instrument; non-compliance evidences UK GDPR breach, which carries the penalty above.

UK Equality Act 2010

Applies to the firm as an employer and as a service provider. AI-assisted drafting and analysis tools must not produce outputs that discriminate against clients or staff on the basis of protected characteristics (race, sex, disability, age, religion, sexual orientation, etc.). Family law files in particular involve protected characteristics. If AI tools systematically produce biased outputs — for example, characterising parties differently based on protected attributes — the firm as deployer may bear liability. No automated decision-making is claimed, but if AI-generated advice is adopted without review, indirect discrimination claims become plausible. The firm must include equality-impact considerations in any AI governance policy.

Key date: In force. No AI-specific amendment; existing provisions apply. · Max penalty: Employment tribunal: uncapped compensation for discrimination claims. County court / civil claims: damages not statutorily capped for service-provider discrimination.

EU AI Act (Regulation 2024/1689) — Article 50 Transparency Duties

Article 50 transparency obligations are IN FORCE as of 2 August 2026. Deployers of AI systems that interact with natural persons must inform those persons they are interacting with an AI system, unless it is obvious from context. Deployers of generative AI that produces content must comply with disclosure requirements. The firm acts as deployer when it uses ChatGPT, Copilot, or Lexis+ AI. If AI-generated correspondence is sent to EU-resident clients without disclosure, Art 50 is breached now. A grace period until 2 December 2026 applies specifically to machine-readable marking of synthetic content (Art 50(2)) for systems placed on the market before 2 August 2026, but the core duty to inform natural persons of AI interaction applies immediately. The EU AI Office and national regulators have enforcement powers from 2 August 2026.

Key date: Art 50 transparency duties and deployer obligations: IN FORCE 2 August 2026. Art 50(2) machine-readable marking of synthetic content: 2 December 2026. · Max penalty: Up to €15,000,000 or 3% of worldwide annual turnover for Art 50 transparency violations. Turnover-based limb cannot be computed without the firm's figures.

EU AI Act — Article 5 Prohibited Practices

Article 5 prohibitions on the most harmful AI practices are not yet in force — they take effect 2 December 2026. The firm should confirm none of the AI tools it deploys will fall within prohibited categories (subliminal manipulation, exploitation of vulnerabilities, real-time remote biometric identification in public spaces, social scoring by public authorities). On current use cases (drafting, summarising, research) no prohibited practice is engaged, but the firm must review this when the prohibitions come into force, particularly as AI use may expand.

Key date: 2 December 2026 (not yet in force as at date of this document, 8 August 2026). · Max penalty: Up to €35,000,000 or 7% of worldwide annual turnover for Art 5 violations. Turnover-based limb cannot be computed without the firm's figures.

EU AI Act — Annex III High-Risk Systems

High-risk obligations for Annex III stand-alone AI systems are deferred to 2 December 2027 following the Digital Omnibus (adopted 29 June 2026). The firm's current uses — drafting, summarising, research — are unlikely to constitute Annex III high-risk systems (which cover recruitment, credit scoring, education, essential services administration, and similar). However, if the firm were to use AI for client-outcome prediction or automated legal advice in ways that materially affect access to justice, this classification would need to be reviewed. No immediate Annex III obligation applies, but preparatory risk assessment is advisable.

Key date: Annex III high-risk obligations: 2 December 2027 (not yet in force). Annex I (product-embedded): 2 August 2028. · Max penalty: Up to €30,000,000 or 6% of worldwide annual turnover for high-risk system violations.

EU AI Act — Article 9 Risk Management and Article 13 Transparency (for Limited-Risk Systems)

For limited-risk AI systems (which ChatGPT and Copilot, as general-purpose AI deployed in a professional context, are likely to be classified), deployers must implement appropriate risk management proportionate to the risk. Art 13 requires that AI systems be sufficiently transparent to allow deployers to interpret outputs and ensure human oversight. These obligations, while less prescriptive than high-risk requirements, are operative for deployers now as part of the Art 50 / deployer obligations framework in force from 2 August 2026. The firm must document the basis on which it assessed each tool's risk category.

Key date: Deployer obligations including Art 13 transparency principles for limited-risk systems: in force 2 August 2026. · Max penalty: General non-compliance: up to €15,000,000 or 3% of worldwide annual turnover.

EU AI Act — GPAI (General-Purpose AI) Rules, Article 50 Duties on Providers

GPAI obligations for providers of general-purpose AI models (e.g., OpenAI, Microsoft) have been in force since 2 August 2025. This does not directly impose obligations on the firm as deployer for GPAI-specific compliance, but it means the firm can expect its AI vendors to have documented model cards, capability disclosures, and training data summaries. The firm should request this documentation from vendors as part of its due diligence and DPA review. The GPAI framework supports the firm's Art 13 transparency obligations by providing the information needed to explain AI outputs to clients.

Key date: GPAI provider obligations: in force 2 August 2025. · Max penalty: GPAI provider penalties are on the AI vendors, not the firm as deployer. Firm exposure is under the deployer penalty tiers above.

EU GDPR (Regulation 2016/679)

Applies to the processing of personal data of EU-resident clients regardless of where the firm is established (Art 3(2) extraterritorial scope — the firm is offering legal services to EU residents). Obligations are substantially parallel to UK GDPR: Art 5 principles, Art 6 lawful basis, Art 9 special categories, Art 25 data protection by design, Art 28 processor agreements, Art 35 DPIA, and Art 46 transfer safeguards. Where the firm processes EU-resident client data via ChatGPT (US-based), it must use Standard Contractual Clauses under EU GDPR Art 46, not the UK IDTA. This is a divergence from UK GDPR: the firm must maintain two sets of transfer mechanisms — UK IDTA for UK data flows and EU SCCs for EU-resident client data flows. The EDPB's Q1 2026 guidance on AI agents confirms data minimisation and purpose limitation apply at every step of AI processing.

Key date: In force. EDPB AI agent guidance: Q1 2026. · Max penalty: €20,000,000 or 4% of global annual turnover, whichever is higher (EU GDPR Art 83(5)). Turnover-based limb cannot be computed without the firm's figures.

SRA Code of Conduct and Solicitors Regulation Authority — AI and Confidentiality

The SRA Code of Conduct for Solicitors requires the firm to keep client information confidential and to maintain legal professional privilege. Inputting client file contents into unapproved third-party AI systems without client consent and without ensuring that data is not retained or used for training is a prima facie breach. The Pinsent Masons false-submissions case (May 2026) illustrates that courts will hold firms responsible for AI-generated errors. Regulatory obligations require the firm to have governance over all tools used in client matters, including AI tools adopted by fee earners on their own initiative. While the SRA Code is not itself a data protection instrument, SRA enforcement action and ICO enforcement action may run in parallel.

Key date: Ongoing regulatory obligation. No specific AI commencement date — applies under existing professional conduct duties. · Max penalty: SRA: unlimited fines (post-2021 tribunal powers), strike-off, suspension, training conditions. Separate from ICO penalties.

UK GDPR Gap Analysis for AI Tools

Your AI tools measured against UK GDPR: what is satisfied, what is not, and what closing each gap takes.

Requirement	Article	Current Position	Gap	Action	Priority
GAP COUNT SUMMARY	—	Critical: 4 | High: 6 | Medium: 4 | Low: 2	Total open gaps: 16	See rows below for individual actions	—
Lawful basis — ChatGPT	UK GDPR Art 6; Art 9 where special-category data in files	No documented lawful basis for processing client personal data via OpenAI's ChatGPT. No DPA in place with OpenAI.	Critical: personal data processed without a valid, recorded basis or processor contract.	Identify Art 6(1)(b) or (f) basis per use case. Execute OpenAI DPA. Record in RoPA.	Critical
Lawful basis — Microsoft Copilot	UK GDPR Art 6; Art 9	Microsoft 365 DPA likely in place but scope for Copilot AI processing of client data not confirmed.	High: Copilot-specific data processing terms and lawful basis mapping not verified or documented.	Confirm Copilot is covered by existing Microsoft DPA. Extend RoPA entry. Document Art 6 basis.	High
Lawful basis — Lexis+ AI	UK GDPR Art 6; Art 9	LexisNexis subscriber agreement may contain data processing terms but these have not been reviewed for AI features.	High: Lexis+ AI processing of pasted client data not assessed against lawful basis or processor terms.	Review LexisNexis terms for AI data use. Obtain or confirm DPA. Document lawful basis.	High
Special-category data	UK GDPR Art 9; Schedule 1 DPA 2018	Family and probate files routinely contain health, financial and family-life data. No Art 9 condition identified for AI processing.	Critical: special-category data likely entered into AI tools without an Art 9(2) condition or Schedule 1 DPA 2018 basis recorded.	Map which files contain Art 9 data. Identify Schedule 1 condition (e.g. legal claims). Prohibit AI input of such data until mapped.	Critical
Legal professional privilege and confidentiality	UK GDPR Art 6(1)(f); SRA Principle 6; Art 5(1)(b)	Fee earners paste client correspondence and case documents into ChatGPT and Lexis+ AI without firm approval or client notice.	Critical: privilege may be waived; confidentiality duty under SRA Principles breached; no client consent or notice.	Issue immediate stop-notice on unapproved AI use. Draft client-facing AI disclosure. Establish approved-tool list.	Critical
Processor contracts (Art 28)	UK GDPR Art 28	No confirmed Art 28 processor agreements in place for ChatGPT or for Lexis+ AI's AI features. Copilot status unconfirmed.	Critical: processing by all three tools without compliant Art 28 contracts is a standalone UK GDPR breach.	Execute OpenAI DPA. Verify and record Microsoft and LexisNexis processor agreements covering AI features.	Critical
Transparency — client notice	UK GDPR Art 13; Art 14	Privacy notices for conveyancing, family and probate clients do not mention AI processing. No AI disclosure in client care letters.	High: clients not informed that their personal data may be processed by third-party AI providers.	Update privacy notices and client care letter templates to disclose AI tool use, provider identity and purpose.	High

Requirement	Article	Current Position	Gap	Action	Priority
Transparency — EU-resident clients	UK GDPR Art 13/14; EU AI Act Art 13; Art 50 (in force 2 Aug 2026)	EU-resident clients (e.g. cross-border conveyancing) receive no AI disclosure. Art 50 transparency duties now enforced.	High: Art 50 deployer obligations apply from 2 Aug 2026. EU clients unaware AI is used on their matters.	Add EU-specific AI disclosure to retainer documents for EU-resident clients. Review Art 50 requirements now.	High
Data minimisation — all tools	UK GDPR Art 5(1)(c)	Fee earners paste whole documents, including unredacted client names, addresses and financial details, into AI prompts.	High: excessive personal data entered into AI tools beyond what is necessary for the drafting or research task.	Issue prompt guidance requiring redaction or anonymisation before AI input. Include in AI Acceptable Use Policy.	High
Accuracy	UK GDPR Art 5(1)(d)	AI outputs (drafts, summaries, research) reviewed inconsistently. Pinsent Masons-type risk of inaccurate AI content reaching clients.	Medium: no documented human review step to catch AI hallucinations before outputs are used in client work.	Mandate documented fee-earner review of all AI outputs before use. Log reviews in matter file.	Medium
Storage limitation — all tools	UK GDPR Art 5(1)(e)	No policy on retention of AI-generated outputs or prompts. ChatGPT conversation history may retain client data on OpenAI servers.	Medium: client data may persist in AI provider systems beyond the firm's own retention schedule.	Configure ChatGPT to disable conversation history for client matters. Confirm Copilot and Lexis+ AI data retention terms.	Medium
Security — all tools	UK GDPR Art 32; Art 5(1)(f)	No technical controls preventing use of personal AI accounts or unapproved browser extensions. No staff training on secure AI use.	High: data sent to consumer-grade AI endpoints without firm oversight represents a foreseeable security risk.	Block personal AI accounts via IT policy. Mandate use of enterprise tiers. Deliver security training within 30 days.	High
Accountability and governance	UK GDPR Art 5(2); Art 24; ICO AI Auditing Framework	No AI policy, no RoPA entries for AI tools, no Data Protection Impact Assessment, no designated AI oversight owner.	High: firm cannot demonstrate compliance. ICO AI Auditing Framework expects documented governance for AI processing.	Appoint AI Compliance Lead. Complete DPIA for each tool. Add AI entries to RoPA. Draft and adopt AI Acceptable Use Policy.	High
Data Protection Impact Assessment	UK GDPR Art 35; ICO guidance on high-risk processing	Processing of special-category data (family, health, financial) via AI tools triggers mandatory DPIA. None conducted.	Critical: mandatory DPIA not carried out before high-risk AI processing commenced.	Conduct DPIA for each AI tool covering conveyancing, family and probate use cases before resuming unapproved use.	Critical
Automated dec ision-making	UK GDPR Art 22; DUAA 2025 Part 5 (in force 5 Feb 2026)	Firm states AI is not used to make decisions about people. AI outputs currently inform but do not replace human decisions.	Low: Art 22 does not currently apply. Position must be reviewed if AI is used to assess client eligibility or risk scores.	Record that Art 22 is not triggered. Monitor tool use and reassess if decision-support use expands.	Low

Requirement	Article	Current Position	Gap	Action	Priority
Complaints procedure	DUAA 2025 s.— (duty in force 19 Jun 2026); UK GDPR Art 77	DUAA 2025 complaint-handling duty commenced 19 Jun 2026. Firm has no documented AI-related data protection complaints procedure.	Low: failure to operate a compliant complaints procedure and respond within set time limits is a breach of the DUAA duty.	Update data protection complaints procedure to cover AI processing. Publish contact point in privacy notice.	Low
International transfers — EU clients	UK GDPR Art 46; UK adequacy regulations	ChatGPT (OpenAI, US-based) processes data from EU-resident clients. Transfer mechanism not confirmed.	Medium: transfer of EU-resident client data to US AI providers requires a UK-recognised transfer mechanism.	Confirm OpenAI's transfer mechanism (e.g. UK IDTA or adequacy). Document in RoPA. Mirror for Lexis+ AI if US-hosted.	Medium

RATING SCALE: Critical = immediate breach or regulatory exposure requiring action within 14 days. High = material gap requiring action within 30 days. Medium = gap requiring action within 90 days. Low = monitoring or process update required within 6 months. REVIEW CADENCE: This gap analysis should be reviewed quarterly and whenever a new AI tool is adopted, a new use case is introduced, or a relevant regulatory change occurs. The next scheduled review date is 8 November 2026. DOCUMENT OWNER: The firm's designated AI Compliance Lead (to be appointed as a priority action). Until appointed, the COLP holds responsibility. DUAA 2025 NOTE: The Data (Use and Access) Act 2025 Part 5 automated-decision provisions came into force 5 February 2026. The DUAA complaints-handling duty came into force 19 June 2026. Both are now live obligations for Halstead & Rowe Solicitors. EU AI ACT NOTE: Article 50 transparency and deployer obligations have been enforceable since 2 August 2026. High-risk Annex III obligations (e.g. if AI were used in HR or access-to-services decisions) are deferred to 2 December 2027 following the Digital Omnibus adopted 29 June 2026. Prohibited practices under Article 5 will be enforceable from 2 December 2026. GPAI obligations for providers such as OpenAI have applied since 2 August 2025 — Halstead & Rowe as deployer must verify provider compliance. CROSS-JURISDICTION POSITION: The following obligations, once satisfied for UK GDPR, also satisfy the equivalent EU GDPR requirement for EU-resident clients: Art 6 lawful basis, Art 13/14 transparency notices, Art 28 processor contracts, Art 32 security, Art 35 DPIA. The following must be met separately: EU AI Act Art 50 deployer disclosure (no UK equivalent yet — apply EU obligation for EU-resident clients); EU AI Act Art 13 system-level transparency requirements imposed on providers (verify per tool); UK DUAA complaints-handling duty (no direct EU mirror — satisfy independently). Where the two regimes diverge, the stricter obligation applies: EU AI Act Art 50 imposes an affirmative disclosure duty to users of AI systems that has no current UK statutory equivalent — Halstead & Rowe must satisfy it for all EU-resident client interactions. MAXIMUM FINES: UK — up to £17.5 million or 4% of global annual turnover (whichever is higher) under UK GDPR; the turnover-based limb cannot be computed without the firm's figures. EU — up to €35 million or 7% of global annual turnover under the EU AI Act; up to €20 million or 4% under EU GDPR; turnover-based limbs cannot be computed without the firm's figures. SRA REGULATORY NOTE: Use of AI tools without client disclosure and without a policy may also engage SRA Principle 6 (client confidentiality) and the SRA Code of Conduct for Solicitors. Regulatory risk is therefore dual: ICO and SRA. The firm should notify its professional indemnity insurer of AI tool adoption.

AI Acceptable Use Policy

Your formal AI policy. Sign it, circulate it to every member of staff, and review it annually or whenever your AI tool usage changes.

AI Acceptable Use Policy — Halstead & Rowe Solicitors

Version 1.0 | Effective Date: 08 August 2026 | Policy Owner: Managing Partner

This policy is issued under the authority of the Managing Partner and is binding on all personnel. It must be read in conjunction with the firm's Data Protection Policy and Client Confidentiality Protocol. It is reviewed annually and whenever the firm's AI tool usage materially changes.

1. Scope

This policy governs every individual who works for or on behalf of Halstead & Rowe Solicitors, including partners, solicitors, paralegals, legal assistants, administrative staff, and any contractors or consultants who access the firm's systems or handle client matter files. It applies regardless of whether the individual is office-based, working remotely, or using a personal device to access firm systems.

The policy covers every use of an AI tool in connection with the firm's work, including drafting client correspondence, summarising case documents, conducting legal research and analysis, and any incidental use that arises in the course of a matter. It applies to all practice areas, including conveyancing, family law, and probate.

The three AI tools currently approved for use are ChatGPT (OpenAI), Microsoft Copilot, and Lexis+ AI. No other AI tool may be used for firm business until it has been approved under section 3 of this policy. The policy applies equally to UK-domiciled clients and to EU-resident clients; where the firm acts for EU-resident clients, the additional EU AI Act obligations set out in this policy apply to that work.

2. Legal Framework

This policy is designed to secure compliance with the following instruments, which apply to the firm's AI-assisted activities.

UK regime: UK GDPR (including Article 22 on automated decision-making), the Data (Use and Access) Act 2025 (Part 5 data protection provisions in force from 5 February 2026; the complaints-procedure duty in force from 19 June 2026), the ICO AI Auditing Framework, and the UK Equality Act 2010. The maximum ICO fine is £17.5 million or 4% of global annual turnover, whichever is higher; the turnover-based limb cannot be computed without the firm's figures.

EU regime: EU AI Act (Regulation (EU) 2024/1689). General-purpose AI model obligations have been in force since 2 August 2025. Article 50 transparency duties, deployer obligations, and national regulator enforcement powers came into force on 2 August 2026. New prohibitions under Article 5 and Article 50(2) synthetic-content marking requirements take effect on 2 December 2026. High-risk system obligations for Annex III systems apply from 2 December 2027 following the Digital Omnibus deferral of 29 June 2026. EU GDPR applies to the processing of personal data of EU-resident clients. The maximum EU AI Act fine is €35 million or 7% of global annual turnover.

Where the two regimes diverge, this policy states the divergence and applies the stricter obligation.

Cross-jurisdiction position: The following obligations are satisfied once for both regimes — maintaining a record of AI-assisted processing activities, conducting risk assessments before deploying new AI tools, applying data minimisation and purpose limitation when using AI, and operating a staff training programme. The following

obligations must be met separately — UK GDPR Article 22 rights exist independently of EU GDPR Article 22 and each client's rights must be honoured under the law applicable to them; EU AI Act Article 50 transparency disclosures to EU-resident clients must be made in a form compliant with EU law even where a UK-law disclosure is also made; and complaints from UK data subjects are handled under the UK regime complaints procedure whilst complaints from EU data subjects are handled under EU supervisory authority routes.

3. Approved Tools and the Process for Requesting a New Tool

The firm's approved AI tools are ChatGPT (OpenAI), Microsoft Copilot, and Lexis+ AI. These tools have been assessed against the firm's data protection and confidentiality obligations before approval. Fee earners and staff may use these tools only for the purposes set out in section 4 and subject to the restrictions in section 5.

No member of staff may use any AI tool not on the approved list for any purpose connected with the firm's work. This prohibition includes free-to-use consumer AI products, browser-integrated AI features not part of an approved product, and AI functionality within third-party platforms unless that functionality has been separately assessed and approved.

A member of staff who wishes to propose a new AI tool must submit a written request to the policy owner. The request must identify the tool, its provider, the intended use, and how personal data would flow to or through it. The policy owner will complete a Data Protection Impact Assessment (DPIA) under UK GDPR Article 35 and, where EU-resident clients may be affected, an equivalent assessment under EU GDPR Article 35 before any approval is given. No tool may be used pending that assessment. The outcome of each assessment will be recorded and retained.

4. Permitted Uses

The approved tools may be used for the following purposes only: drafting and editing client correspondence where the output is reviewed and approved by a qualified fee earner before it is sent; summarising case documents to assist fee earner review, where the summary is verified against the source document before it is relied upon; and conducting legal research and analysis, where every AI-generated reference, citation, or statement of law is independently verified by a qualified fee earner before it is used in any document, advice, or submission.

All other uses require prior written approval from the policy owner. This includes, without limitation, using AI tools to generate court documents, witness summaries, or expert instructions.

5. What Must Never Be Entered into an AI Tool

The following categories of information must never be entered into any AI tool, including the three approved tools, unless the firm has in place a Data Processing Agreement with the provider that explicitly restricts training on client data and the policy owner has confirmed in writing that entry of that category is permitted for that tool.

Personal data of clients or staff: Any information that identifies or could identify a living individual, including names, addresses, dates of birth, financial details, health information, and family circumstances found in conveyancing, family, or probate files. This applies equally to UK-based and EU-resident clients. Processing personal data through an AI tool without a lawful basis and adequate safeguards constitutes a breach of UK GDPR and EU GDPR.

Confidential client material: All information communicated by a client in the context of seeking legal advice is protected by legal professional privilege. Entering privileged communications, client instructions, or matter-specific facts into a third-party AI tool risks waiving privilege and breaching the firm's duties under the SRA Code of Conduct.

Credentials and authentication data: Passwords, access tokens, client portal credentials, and any system authentication details must never be entered into an AI tool under any circumstances.

Information subject to a non-disclosure agreement: Where the firm holds information under a contractual confidentiality obligation owed to a client, counterparty, or third party, that information must not be processed through any external AI tool.

Special category data: Health data, data revealing racial or ethnic origin, religious beliefs, sexual orientation, or other special category data within the meaning of UK GDPR Article 9 and EU GDPR Article 9 must not be entered into any AI tool.

Where a fee earner is uncertain whether a particular piece of information falls within a restricted category, they must treat it as restricted and seek guidance from the policy owner before proceeding.

6. Verification of Output and Responsibility

Every AI-generated output used in connection with a client matter must be verified by a qualified fee earner before it is used or sent externally. Verification means checking the substance of the output against authoritative sources, not merely reviewing it for typographical errors.

For legal research outputs, the fee earner must independently locate and read every case, statute, or regulatory provision cited by the AI tool before that reference is included in any advice, pleading, or correspondence. The firm notes that in May 2026 a London court criticised a law firm for false submissions based on AI-generated search results; Halstead & Rowe Solicitors is determined to prevent any equivalent failure. AI tools, including Lexis+ AI, can generate plausible but incorrect citations; the fee earner who uses the output bears personal professional responsibility for its accuracy.

For drafted correspondence, the fee earner who approves and sends the correspondence is responsible for its content as if they had drafted it personally. The use of an AI tool to produce a first draft does not reduce that responsibility.

For document summaries, the fee earner relying on the summary must satisfy themselves that it accurately reflects the source document before acting on it or incorporating it into advice.

The supervising partner on each matter retains overall responsibility for the quality and accuracy of AI-assisted work product produced by fee earners under their supervision.

7. Where a Human Decision Is Mandatory

Certain decisions must be made by a qualified human professional and may not be delegated to, or determined solely by, an AI tool. This is not merely a best-practice requirement; it reflects the firm's obligations under UK GDPR Article 22, EU GDPR Article 22, the SRA Standards and Regulations, and the firm's duties to the court.

The following decisions require a human decision-maker in every case: all legal advice given to a client; all decisions to issue, settle, or discontinue proceedings; all decisions about whether to report a matter under the Proceeds of Crime Act or the Money Laundering Regulations; all risk and conflict-of-interest assessments; all decisions about whether documents are privileged; and all decisions made in the context of family law matters affecting the welfare of children or vulnerable adults.

The Data (Use and Access) Act 2025 (Part 5, in force 5 February 2026) adjusted the framework for solely automated decisions under UK GDPR, expanding the lawful bases on which such decisions may be made and the safeguards that must accompany them. However, this firm has confirmed that it does not currently use AI to make decisions about people in an automated fashion, and no such use is authorised under this policy without a further DPIA and approval from the policy owner. The EU AI Act prohibition on certain manipulative and exploitative AI practices under Article 5 (taking effect 2 December 2026) will be reviewed before that date to confirm continued compliance.

The UK Equality Act 2010 applies to all the firm's activities. No AI-assisted process may be used in a way that results in unlawful discrimination on the basis of a protected characteristic. Where any AI tool produces output that appears to reflect bias, the fee earner must report it under section 9 of this policy and must not use that output.

8. Disclosure to Clients

The firm must inform clients when AI has played a material role in work product delivered to them. A material role means that AI-generated content forms part of correspondence, advice, or a document sent to the client, even where that content has been reviewed and edited by a fee earner.

For UK-based clients, disclosure will be made in the client care letter at the outset of the retainer, confirming that the firm uses AI tools to assist with drafting, research, and document review, and that all AI-assisted work is reviewed and approved by a qualified fee earner before delivery.

For EU-resident clients, the disclosure obligation is reinforced by EU AI Act Article 50, which has been in force since 2 August 2026. Where any of the approved AI tools functions as an AI system that interacts with natural persons or generates content in a way that falls within Article 50's scope, the firm as deployer must ensure users are informed. The disclosure in the client care letter will therefore state specifically that AI tools regulated under the EU AI Act are in use and will identify the nature of their use. The policy owner will confirm before 2 December 2026 whether any synthetic-content marking obligations under Article 50(2) apply to the firm's outputs, as those obligations take effect on that date.

Divergence between regimes: The EU AI Act Article 50 disclosure obligation is more prescriptive in form and timing than the current UK position under the ICO AI Auditing Framework. This policy applies the EU standard to all clients as the stricter obligation, ensuring a single disclosure standard across the practice.

9. Record Keeping and Retention

The firm must maintain records sufficient to demonstrate compliance with this policy and with the applicable legal frameworks. The following records must be kept.

A register of approved AI tools, maintained by the policy owner, recording the tool name, provider, date of approval, the DPIA reference, and any conditions of use. This register must be updated whenever a tool is approved, suspended, or withdrawn.

A record of AI use at matter level: where an AI tool has been used in connection with a client matter, a note must be added to the matter file identifying the tool used, the nature of the task, and the name of the fee earner who verified the output. This note forms part of the client file and is retained for the same period as the file itself, in accordance with the firm's standard file retention schedule.

DPIA records for each AI tool assessment, retained for a minimum of three years from the date of the assessment or the date the tool is withdrawn from use, whichever is later.

Training records confirming that each member of staff has received training on this policy, updated on each policy revision.

Complaint and breach records as described in section 10.

The Data (Use and Access) Act 2025 complaints-procedure duty (in force 19 June 2026) requires the firm to operate a procedure for handling data protection complaints and to respond within set time limits. Records of complaints received and responses given must be retained for a minimum of three years. The same retention standard is applied to complaints from EU-resident clients under EU GDPR and the EU AI Act to meet the stricter obligation.

10. Breach of Policy: Reporting and Disciplinary Position

Any member of staff who becomes aware of a breach of this policy, or who suspects that a breach may have occurred, must report it to the policy owner (Managing Partner) immediately and in any event within 24 hours of becoming aware. A breach includes, but is not limited to: use of an unapproved AI tool; entry of restricted information into any AI tool; failure to verify output before external use; and failure to make a required disclosure to a client.

The policy owner will assess whether the breach constitutes a personal data breach requiring notification to the ICO under UK GDPR Article 33 (72-hour notification window) and, where EU-resident clients are affected, to the relevant EU supervisory authority under EU GDPR Article 33. The policy owner will also assess whether the breach engages any obligation to notify the SRA.

Breaches of this policy are treated as disciplinary matters. Minor or first-time breaches will ordinarily result in a formal written warning and mandatory retraining. Serious breaches, including deliberate or repeated non-compliance, entry of privileged or personal data into an unapproved tool, or failure to report a known breach, may result in dismissal. The firm's standard disciplinary procedure applies. Nothing in this policy limits the firm's right to take action commensurate with the seriousness of the conduct.

All breach reports, the policy owner's assessment, any notifications made to regulators, and the outcome of any disciplinary process must be recorded and retained for a minimum of three years.

11. High-Risk AI Systems under the EU AI Act

The firm has assessed whether any of its current AI uses fall within Annex III of the EU AI Act as high-risk systems. AI tools used in recruitment, access to essential services, or administration of justice may engage Annex III. The firm's current approved uses — drafting correspondence, summarising documents, and research — do not, as presently operated, place the firm in the role of deployer of a high-risk system. However, Lexis+ AI includes analytical functions that may develop; the policy owner will reassess this position before the Annex III compliance deadline of 2 December 2027 (as deferred by the Digital Omnibus, in force 29 June 2026).

If any approved tool is reclassified or any new use brings the firm within Annex III, the full obligations of EU AI Act Articles 9 (risk management), 13 (transparency), and associated deployer duties will be implemented before that use commences.

12. Review Cycle, Policy Owner, and Signature

This policy will be reviewed annually, on or before 08 August each year. It will also be reviewed immediately upon any of the following events: the firm adopts a new AI tool; a significant change occurs in the applicable legal framework; a reportable breach occurs; or the ICO, SRA, or an EU supervisory authority issues guidance materially affecting the firm's obligations.

Policy Owner: Managing Partner, Halstead & Rowe Solicitors.

All partners and members of staff are required to confirm in writing that they have read, understood, and will comply with this policy. Signed acknowledgements are retained on each individual's personnel file.

Signed: _____ Date: 08 August 2026
Managing Partner, Halstead & Rowe Solicitors

This policy is effective from 08 August 2026 and supersedes any previous informal guidance on AI tool use. Questions should be directed to the policy owner.

Employee AI Guidelines — Practical Dos and Don'ts

The working-level guidance that sits under the policy: concrete examples of good and bad AI use in this business.

About This Document

These guidelines apply to every fee earner and member of staff at Halstead & Rowe Solicitors who uses ChatGPT, Microsoft Copilot or Lexis+ AI in their work. They sit beneath the firm's AI Acceptable Use Policy and translate its obligations into practical day-to-day guidance. They are not optional: non-compliance may expose the firm to regulatory sanction under UK GDPR, the Data (Use and Access) Act 2025, and — because we act for EU-resident clients — the EU AI Act (Regulation (EU) 2024/1689). Maximum fines under UK GDPR are £17.5 million or 4% of global annual turnover; under the EU AI Act they reach €35 million or 7% of global annual turnover. Individual solicitors also risk referral to the SRA. These guidelines take effect immediately.

Approval: Which Tools You May Use and When

Only the three tools named above — ChatGPT, Microsoft Copilot and Lexis+ AI — are approved for use on client work at Halstead & Rowe. No other AI tool, browser extension, AI-assisted search engine, or AI feature within any other application may be used on client matters without written sign-off from the supervising partner. This applies even to tools that appear professional or that a colleague has recommended.

Fee earners who have already been using other AI tools on their own initiative must stop doing so with immediate effect and disclose this to their supervising partner. That disclosure is confidential and will be used to assess any remediation needed; it is not, of itself, a disciplinary matter. The concern is not curiosity but the risk that personal data and privileged content have already passed through unapproved systems, which triggers obligations under UK GDPR Article 33 and EU GDPR Article 33 if a reportable breach has occurred.

Worked Example 1 — Drafting Client Correspondence

DO: When drafting a letter to a client in a conveyancing matter, open a ChatGPT or Copilot session and type a prompt such as: 'Draft a letter to a residential property buyer explaining that exchange of contracts is delayed because the seller's solicitors have not returned the signed contract. Tone: professional and reassuring. UK English.' Enter no name, address, file reference, or any detail that identifies the client or the property. Once you receive the draft, paste it into the file, insert the client's details from your case management system, and review it in full before sending.

DO NOT: Do not type a prompt such as 'Write a letter to John Smith of 14 Acacia Road, Birmingham B1 2XY explaining the exchange delay on his purchase of 22 Oak Lane.' Entering a client's name, address, or any combination of identifiers into ChatGPT or Copilot sends that data to a third-party processor. Unless the firm has a signed data processing agreement in place with that provider that meets UK GDPR Article 28 and EU GDPR Article 28 requirements, this is an unlawful disclosure. Even where an agreement exists, you must not send more personal data than is strictly necessary for the task: UK GDPR Article 5(1)(c) and EU GDPR Article 5(1)(c) both require data minimisation. Lexis+ AI, which is designed for legal use, has contractual privacy protections; check with the supervising partner before entering any client identifiers even there.

Worked Example 2 — Summarising Case Documents

DO: When you need to summarise a lengthy witness statement, medical report or set of financial disclosure documents in a family matter, use Lexis+ AI via the firm's licensed account, which offers stronger confidentiality protections than the consumer-facing tools. Before uploading, remove or redact names, National Insurance numbers, dates of birth, account numbers, and any other direct identifiers from a working copy. Ask the tool to summarise the redacted document, then restore context from the original file when you write your own attendance note. Keep the redacted copy only as long as needed for that task.

DO NOT: Do not upload an unredacted probate inventory, a full set of financial remedy Form E documents, or any document containing medical or biometric information directly into ChatGPT or Copilot. Such documents contain special-category data within the meaning of UK GDPR Article 9 and EU GDPR Article 9. Processing special-category data requires an explicit condition under Article 9(2); simply finding it convenient is not a condition. Uploading an unredacted document to a consumer AI platform without appropriate safeguards is likely to constitute an unlawful transfer of special-category data and a potential breach of legal professional privilege, which once lost cannot be restored.

Worked Example 3 — Research and Analysis

DO: Use Lexis+ AI to research case law, statutory provisions, and regulatory guidance. It is connected to verified legal databases and is less likely than general-purpose tools to generate fictitious citations. When using ChatGPT or Copilot for legal research — for example, to get an overview of a legal concept before drilling into primary sources — treat the output as a starting point only. Every case name, statutory reference, and legal proposition must be verified against Lexis+, Westlaw, or the primary source before it is relied upon or included in any document going to a client, court, or third party.

DO NOT: Do not copy legal research from any AI tool directly into a client advice, a court filing, or a letter to a counterparty without independent verification. In May 2026 a London court criticised a law firm for false submissions based on AI-generated search results. Italian courts have similarly developed a doctrine of professional diligence around AI hallucinations in pleadings. An AI tool can produce a plausible but entirely fictitious case citation with complete confidence in its tone. You are the qualified professional; the tool is a drafting aid. Your professional obligations under SRA Principles 2 and 5 — acting with integrity and being competent — are not delegated to the software.

Prompting Practice: Keeping Personal and Privileged Data Out

The single most effective data-protection control available to you is how you write your prompt. Before pressing send, ask yourself: if this prompt were printed and handed to a stranger, would it identify a client, reveal the substance of privileged advice, or disclose commercially sensitive information? If yes, rewrite it.

Use role and scenario prompts rather than real-matter prompts. 'A buyer in a residential conveyancing transaction has received a local authority search revealing a planning notice. Draft a paragraph explaining the implications.' conveys what you need without identifying anyone. Avoid including file numbers even in anonymised form if the number could be cross-referenced. Do not include the opposing party's name, the other solicitor's name, or the name of any expert witness. Do not paste in correspondence from another party's solicitor; it will contain personal data about their client. If you are working on a matter for an EU-resident client, bear in mind that transfers of their personal data to AI systems hosted outside the EEA may require a transfer mechanism under EU GDPR Chapter V; confirm the position with the data protection lead before using any tool for that client's documents.

Checking Output: Fabrication, Bias and Confident Errors

AI tools produce fluent, authoritative-sounding text even when the underlying content is wrong. The three failure modes you are most likely to encounter at Halstead & Rowe are: fabricated case citations (the tool invents a case name, court and year that do not exist); incorrect statements of law (the tool states a legal rule that was once correct but has since been amended); and biased framing (the tool reflects assumptions about, for example, which party in a family dispute is likely to have primary care of children).

For every piece of AI-generated research output: (1) Search for every case cited on Lexis+ or Westlaw before using it. If it does not appear, it does not exist — do not use it. (2) Check every statutory reference against the current version of the legislation on legislation.gov.uk or the EUR-Lex equivalent for EU instruments. (3) Read the output for tone and framing. If a draft letter or advice assumes facts you have not provided, or adopts a particular characterisation of the client's position, rewrite it. The UK Equality Act 2010 requires the firm to avoid facilitating discrimination; AI outputs that embed stereotyped assumptions about protected characteristics must not pass into client-facing documents. Document your verification steps in a brief file note so that, if the output is later questioned, you can demonstrate the review that took place.

Handling AI Output That Will Be Seen by a Client or Third Party

Any AI-assisted document that will be sent to a client, a court, Land Registry, HMRC, a counterparty solicitor, or any other external recipient must be reviewed and approved by the supervising fee earner before it leaves the firm. 'Reviewed' means read in full, not skimmed. 'Approved' means the reviewer takes professional responsibility for its accuracy and appropriateness — not merely that they checked the formatting.

Under EU AI Act Article 50, which entered into force on 2 August 2026, deployers of certain AI systems that interact with natural persons must ensure those persons are informed they are interacting with an AI system. Where you are using a chatbot-style interface to communicate with clients — for example, an AI-assisted client portal — that disclosure obligation applies now. If the firm sends a client a document that was drafted substantially by AI, consider whether a brief disclosure in the covering note is appropriate to maintain trust and comply with evolving transparency norms. For EU-resident clients, this is not merely best practice: Article 50 creates a binding obligation on deployers, and Halstead & Rowe is a deployer within the meaning of the Act when it uses these tools on client work. Failure to disclose where required can result in fines administered by the relevant national AI authority.

When to Stop and Escalate

Stop using AI and escalate to a supervising partner immediately in any of the following situations. First, if you realise you have already entered personal data, a client name, a file reference, or privileged content into an unapproved tool — report it at once. The firm must assess whether this constitutes a personal data breach requiring notification to the ICO within 72 hours under UK GDPR Article 33, or to the relevant EU supervisory authority under EU GDPR Article 33, if an EU-resident client's data is affected. The clock starts when the firm becomes aware, not when you report it to a partner.

Second, if an AI tool produces output that you cannot verify — for example, a citation you cannot locate, a legal proposition that contradicts your recollection, or an analysis that seems internally inconsistent — do not attempt to verify it yourself and include it anyway. Stop, note the issue, and ask a colleague or supervisor to review it with you. Third, if a client asks you directly whether AI was used in preparing their advice or documents and you are unsure what to disclose, stop and ask the supervising partner before answering. Fourth, if you encounter any AI-generated output that appears to discriminate against a client or third party on grounds of a protected characteristic under the Equality Act 2010 — such as advice that seems to treat a client's disability or race as relevant when it is not — do not send it and escalate immediately. These are the firm's red lines; there is no situation in which it is safer to proceed quietly than to flag the issue.

Cross-Jurisdiction Position

Halstead & Rowe operates under both UK GDPR and EU GDPR because it acts for EU-resident clients and holds their personal data. The firm is also subject to the EU AI Act as a deployer of AI systems whose output affects those clients.

Obligations satisfied once for both regimes: Data minimisation, purpose limitation, accuracy and storage limitation principles (UK GDPR Article 5 / EU GDPR Article 5) are substantively identical; a single internal practice satisfies both. The requirement to have a data processing agreement with AI providers (UK GDPR Article 28 / EU GDPR Article 28) is met by a single agreement if it is drafted to meet both standards — check with the data protection lead that existing agreements cover EU GDPR requirements as well as UK GDPR. The obligation to conduct a Data Protection Impact Assessment before using AI on high-risk processing (UK GDPR Article 35 / EU GDPR Article 35) is met once if the DPIA addresses risks to both UK and EU data subjects.

Obligations that must be met separately: Transfer mechanisms differ. Transfers of EU-resident client data to AI systems hosted outside the EEA require an EU Chapter V mechanism (adequacy, Standard Contractual Clauses, or equivalent). The UK's own international transfer regime applies separately to transfers of UK-resident client data outside the UK. The firm must maintain both. EU AI Act Article 50 transparency duties apply specifically to EU-resident clients and are enforceable by EU national AI authorities from 2 August 2026; there is no direct UK equivalent statute in force at this date, though the ICO's AI Auditing Framework expects transparency as a matter of good practice. Where the two regimes diverge, the firm applies the stricter obligation: in practice this means applying EU GDPR Chapter V transfer safeguards to all international AI data transfers, and applying EU AI Act Article 50 disclosure requirements to all client-facing AI use regardless of the client's residence.

High-risk AI obligations under EU AI Act Annex III are not yet in force; the Digital Omnibus of 29 June 2026 deferred that deadline to 2 December 2027. The firm should monitor whether its use of AI in case analysis falls within any Annex III category and begin preparatory work. The prohibition provisions of the EU AI Act relevant to this firm are not yet in force as of the date of this document; they take effect 2 December 2026, and the firm must review its practices again at that point.

Complaints and Record-Keeping

From 19 June 2026 the Data (Use and Access) Act 2025 requires the firm to operate a complaints procedure and respond to data protection complaints within set time limits. If a client or data subject complains that their personal data has been processed improperly through an AI tool, that complaint must be logged and directed to the data protection lead on the day it is received. The firm's response must be issued within the statutory period; staff must not hold complaints at fee-earner level without escalating.

Keep a brief record each time you use an AI tool on a client matter: the tool used, the nature of the task (not the client's name), the date, and the verification steps taken. This does not need to be elaborate — a one-line file note is sufficient — but it creates the audit trail the firm needs to respond to an ICO inquiry or an SRA review. These records should be retained in line with the firm's standard file retention policy.

ICO Framework Self-Assessment

The regulator's own framework, worked through and answered.

ICO AI Auditing Framework Self-Assessment — Halstead & Rowe Solicitors

Document: ICO Framework Self-Assessment | Client: Halstead & Rowe Solicitors | Date: 08 August 2026 | Tools in scope: ChatGPT (OpenAI), Microsoft Copilot, Lexis+ AI | Jurisdictions: UK and EU | This self-assessment works through the ICO AI Auditing Framework area by area, records Halstead & Rowe's current position against each area, assigns a RAG rating, and calls out the lowest-scoring areas for priority action. Where UK and EU obligations diverge, the stricter obligation is applied and the divergence is noted. Cross-jurisdiction position: obligations that can be discharged once for both regimes and those requiring separate action are identified in each section. Ratings: GREEN = adequate controls in place; AMBER = partial controls, remediation required; RED = no controls, immediate action required.

- [ ] **AREA 1 — ACCOUNTABILITY AND GOVERNANCE | Rating: RED | Establish a named AI Governance Lead and adopt a written AI Governance Policy before any further fee-earner use of ChatGPT, Microsoft Copilot or Lexis+ AI.**

  Appoint a partner or senior solicitor as AI Governance Lead with documented authority. Draft and circulate an AI Governance Policy covering: approved tools (currently ChatGPT, Microsoft Copilot, Lexis+ AI), prohibited uses (inputting client personal data into ChatGPT or Copilot without a signed Data Processing Agreement), mandatory human review of all AI outputs before use in client matters, and a register of AI use cases. Log all three tools in the firm's Record of Processing Activities (RoPA) under UK GDPR Art 30 and equivalent EU GDPR Art 30. Under the ICO AI Auditing Framework, accountability requires a senior individual to own AI risk; under the SRA's regulatory framework, partners bear personal responsibility for systems compliance.

  Why it matters: Without governance, every fee earner is an uncontrolled deployer: the firm is exposed to ICO enforcement (maximum fine £17.5 m or 4% global turnover under UK GDPR) and SRA regulatory action, and no other control in this assessment can function without the policy foundation.

- [ ] **AREA 1 (continued) — CROSS-JURISDICTION POSITION | Record which governance obligations are satisfied once and which require separate action for EU-resident clients.**

  Single-action obligations (satisfy once): maintain a RoPA, appoint a governance lead, conduct DPIAs. Separate-action obligations: (a) EU AI Act Art 13 transparency notices must be prepared in the language of the EU-resident client and reference EU rights; UK transparency notices satisfy UK GDPR but not EU AI Act Art 13. (b) EU AI Act Art 50 deployer disclosure duties (in force 2 August 2026) require Halstead & Rowe to inform EU-resident clients when AI has been used to generate correspondence or summaries; there is no equivalent UK statutory duty yet, though ICO guidance recommends it. Apply the stricter EU obligation to all client-facing communications regardless of client location to avoid a two-tier system.

  Why it matters: Acting for EU-resident clients on conveyancing, family and probate matters brings the firm within the territorial scope of the EU AI Act; failure to apply EU obligations to those clients risks fines of up to €35 m or 7% global turnover from EU national regulators.

☐ **AREA 2 — FAIR AND LAWFUL PROCESSING | Rating: RED | Identify and document the lawful basis for processing personal data through each AI tool and implement Data Processing Agreements (DPAs) with OpenAI, Microsoft and LexisNexis before further use.**

Conveyancing, family and probate files contain special-category data (health, financial, family status). Processing this through ChatGPT or Copilot requires a lawful basis under UK GDPR Art 6 and a condition under Art 9; legitimate interests is unlikely to be available without a completed Legitimate Interests Assessment given the sensitivity. Obtain and retain signed DPAs with each provider confirming: data is not used for model training, data is deleted after processing, and sub-processors are listed. Under the Data (Use and Access) Act 2025 (in force 5 February 2026), widened lawful bases for automated decisions apply but require documented safeguards; record these in the governance policy. For EU-resident clients, EU GDPR Art 6 and Art 9 apply in parallel; the stricter EU position (no inference of consent from continued service use) governs.

Why it matters: Processing special-category data without a documented Art 9 condition is a prima facie UK GDPR breach and an EU GDPR breach, each carrying maximum fines at the levels stated above, and constitutes a potential breach of the SRA's client confidentiality duties.

☐ **AREA 2 (continued) — LEGAL PROFESSIONAL PRIVILEGE | Rating: RED | Implement a written protocol prohibiting input of privileged communications or client-identifying information into ChatGPT or Microsoft Copilot until external-model data-handling is contractually secured.**

Legal professional privilege is not a GDPR concept but it interacts with confidentiality obligations under the SRA Code of Conduct and common law. Privileged material fed into a cloud AI tool where the provider can access prompt data risks waiver. Lexis+ AI is designed for legal use and its DPA should be reviewed to confirm privilege-protective handling; if confirmed, it may be used for case research with redacted facts. ChatGPT and Copilot must not receive client names, case references or privileged facts until the firm's DPAs confirm no human review of prompts by the provider. This protocol must be written into the AI Governance Policy and communicated to all fee earners.

Why it matters: Inadvertent waiver of privilege could destroy a client's litigation position and expose the firm to a negligence claim; the SRA could also treat disclosure of confidential information as a conduct breach.

☐ **AREA 3 — TRANSPARENCY | Rating: RED | Issue AI disclosure notices to all clients and update the firm's Privacy Notice to cover AI processing, complying with UK GDPR Arts 13–14, EU GDPR Arts 13–14, and EU AI Act Art 50 (in force 2 August 2026).**

Amend the client care letter and Privacy Notice to state: (i) which AI tools the firm uses, (ii) the categories of data processed through them, (iii) the safeguards in place, and (iv) how clients can object. For EU-resident clients, add a specific disclosure under EU AI Act Art 50 stating that AI has been used in drafting their correspondence or summarising their documents, in their preferred language. The EU AI Act Art 50 deployer obligation is in force as of 2 August 2026; non-compliance now risks fines of up to €15 m or 3% global turnover from EU national AI regulators. UK ICO guidance recommends equivalent transparency even absent a specific UK statutory duty; apply the EU standard universally. Divergence: EU Art 50 requires disclosure of AI interaction proactively; UK law does not yet mandate this by statute but ICO guidance strongly expects it — apply the EU standard.

Why it matters: Clients, including those on family and probate matters involving highly sensitive personal data, have a reasonable expectation of knowing when AI processes their information; failing to disclose breaches Arts 13–14 of both UK and EU GDPR and, for EU clients, Art 50 of the EU AI Act.

☐ **AREA 4 — SECURITY | Rating: AMBER | Conduct a Data Protection Impact Assessment (DPIA) for each AI tool and implement technical controls restricting upload of personal data to non-approved systems.**

A DPIA is mandatory under UK GDPR Art 35 and EU GDPR Art 35 where processing is likely to result in high risk; use of generative AI to process special-category legal data meets this threshold. Complete a DPIA for ChatGPT, Microsoft Copilot and Lexis+ AI separately, documenting: data flows, risks of hallucination leading to incorrect advice, confidentiality risks, and mitigations. Technical controls: configure Microsoft 365 Data Loss Prevention policies to flag or block personal data being pasted into Copilot prompts without approval; restrict ChatGPT access on firm devices to a managed enterprise account with a DPA in place; confirm Lexis+ AI is accessed only via the firm's authenticated account. Review provider security certifications (ISO 27001 or equivalent) and record findings.

Why it matters: A security breach involving client conveyancing or family data processed through an unsecured AI tool would require mandatory ICO notification within 72 hours under UK GDPR Art 33 and EU GDPR Art 33, and could result in enforcement action and reputational damage.

☐ **AREA 5 — RIGHTS | Rating: AMBER | Document how data subject rights requests (access, erasure, rectification, objection) can be fulfilled for data processed through AI tools, including the new complaints procedure duty.**

Map where AI-processed personal data is retained: if ChatGPT or Copilot retains prompt data, the firm must be able to respond to a Subject Access Request or erasure request by instructing the provider to delete it — confirm this in each DPA. Under the Data (Use and Access) Act 2025 (complaints procedure duty in force 19 June 2026), the firm must operate a documented complaints procedure for data protection complaints and respond within set time limits; create and publish this procedure now. For EU-resident clients, EU GDPR Arts 15–22 apply in parallel; where the individual exercises the right to object to automated processing under Art 22, the firm must be able to demonstrate that no solely automated decision with legal or similarly significant effect was made — the firm has stated AI is not used for decisions about people, which satisfies Art 22, but this must be documented.

Why it matters: Inability to honour a Subject Access Request or erasure request touching AI-processed data is a standalone GDPR breach; failure to operate a complaints procedure is a breach of the Data (Use and Access) Act 2025 effective 19 June 2026.

☐ **AREA 6 — EU AI ACT CLASSIFICATION AND PROHIBITED PRACTICES | Rating: AMBER | Confirm that none of the three AI tools are used in a manner that constitutes a prohibited practice under EU AI Act Art 5, and assess whether any use case falls within Annex III high-risk categories.**

Art 5 prohibited practices include subliminal manipulation, exploitation of vulnerability, social scoring, and real-time biometric identification in public spaces. Halstead & Rowe's declared uses (drafting, summarising, research) do not engage any Art 5 prohibition; record this finding in the governance register. New prohibitions take effect 2 December 2026 — review at that date. Annex III high-risk categories relevant to legal services include AI used in administration of justice and democratic processes (Annex III point 8). Halstead & Rowe uses AI to draft correspondence and summarise documents, not to determine legal outcomes; this falls below the high-risk threshold. However, high-risk compliance obligations under Annex III are deferred to 2 December 2027 (Digital Omnibus, in force 29 June 2026), giving the firm preparation time. Document the classification rationale now. GPAI rules: ChatGPT and Microsoft Copilot are General-Purpose AI models; GPAI obligations on providers (not deployers) have applied since 2 August 2025. As a deployer, Halstead & Rowe must follow provider instructions and pass through any required transparency information to end users.

Why it matters: If a use case were later reclassified as high-risk, absence of a documented classification rationale would leave the firm unable to demonstrate good-faith compliance and would accelerate regulatory timelines.

☐ **AREA 7 — UK GDPR ART 22 AND DATA (USE AND ACCESS) ACT 2025 — AUTOMATED DECISION-MAKING | Rating: GREEN (with documentation required) | Record formally that AI is not used by Halstead & Rowe to make solely automated decisions with legal or similarly significant effect on individuals.**

The firm has confirmed AI is not used in decisions about people. Document this in the governance register, specifying for each use case (drafting, summarising, research) that a qualified fee earner reviews and approves all AI outputs before they are acted upon or sent. Under UK GDPR Art 22 and the Data (Use and Access) Act 2025 (in force 5 February 2026), the widened lawful bases for automated decisions require documented safeguards; record that the human review requirement is the firm's primary safeguard. Under EU GDPR Art 22, the same position applies. No divergence between regimes on this point. Review this position if the firm introduces AI tools that score, rank or make recommendations about clients or staff.

Why it matters: If fee earners begin using AI to recommend case strategy or client risk ratings without human review, the firm would fall within Art 22 scope without controls, creating immediate compliance exposure.

- [ ] **AREA 8 — STAFF USE WITHOUT APPROVAL (SHADOW AI) | Rating: RED | Issue an immediate all-staff directive prohibiting unapproved AI tool use and introduce a mandatory AI training programme.**

  Draft and circulate a one-page directive today: fee earners must not use any AI tool not listed in the AI Governance Policy on client matters; breach is a conduct matter under the firm's disciplinary procedure. Follow within four weeks with a mandatory training session covering: what AI tools are approved, what data may be input, the hallucination risk (citing the Pinsent Masons May 2026 case where false AI-generated submissions were criticised by a London court), and how to report AI errors. Maintain a training register. Under the UK Equality Act 2010, if AI tools generate biased outputs that affect employment or service decisions, the firm bears responsibility; include this in training. Log completion in the governance register.

  Why it matters: Shadow AI use is the firm's single greatest immediate risk: a fee earner inputting a client's full probate file into a personal ChatGPT account would constitute an uncontrolled personal data transfer with no DPA, a potential privilege waiver, and a reportable breach.

- [ ] **AREA 9 — UK EQUALITY ACT 2010 AND BIAS | Rating: AMBER | Assess AI outputs used in client-facing work for potential bias and document the assessment.**

  The UK Equality Act 2010 requires that services are not provided in a discriminatory way. AI tools used to draft client correspondence for conveyancing, family or probate matters could produce outputs that are culturally biased or that treat protected characteristics differently. Implement a spot-check review: the AI Governance Lead reviews a sample of AI-drafted correspondence monthly for the first six months to identify any pattern of bias. Record findings. Where Lexis+ AI is used for research, confirm with LexisNexis that the model has been tested for legal bias in UK law contexts. This is a UK-specific obligation; there is no direct EU AI Act equivalent for non-high-risk systems at this stage, though EU GDPR Art 5(1)(a) fairness principle applies in parallel.

  Why it matters: A discriminatory AI-drafted letter to a client with a protected characteristic could constitute a service provision breach under the Equality Act 2010 and an unfairness breach under UK GDPR Art 5(1)(a), exposing the firm to civil claims and regulatory action.

- [ ] **LOWEST-SCORING AREAS — PRIORITY ACTION PLAN | Areas rated RED: Governance (Area 1), Lawful Processing and Privilege (Area 2), Transparency (Area 3), Shadow AI (Area 8). Assign owners and deadlines.**

  Week 1: Appoint AI Governance Lead; issue shadow AI directive; suspend ChatGPT and Copilot use on client matters pending DPAs. Week 2–4: Draft AI Governance Policy; initiate DPA negotiations with OpenAI and Microsoft; update client care letter and Privacy Notice; publish complaints procedure (required since 19 June 2026). Month 2: Complete DPIAs for all three tools; deliver mandatory staff training; establish monthly bias spot-check. Month 3: Review all three DPAs when executed; update RoPA; file governance register. Ongoing: Review EU AI Act Art 5 new prohibitions at 2 December 2026; begin Annex III readiness review by June 2027 ahead of 2 December 2027 deadline.

  Why it matters: The four RED-rated areas represent active, ongoing compliance breaches: every day fee earners continue using unapproved tools on client files without governance, DPAs or transparency notices, the firm accumulates regulatory and professional conduct risk that cannot be retrospectively remediated.

Compliance Roadmap

The sequence to work through. Do not start a phase until the one before it is complete — the order is deliberate.

Phase 1 — Immediate Actions (Days 1–14)

These actions must be completed before any further phase begins. They address the highest-risk exposures facing Halstead & Rowe Solicitors right now: unsanctioned use of ChatGPT, Microsoft Copilot and Lexis+ AI on live client files, and the absence of any policy governing that use. The SRA and ICO both expect firms to have controls in place before a breach, not after.

☐ **Issue an immediate interim AI use directive to all fee earners and staff.**

The managing partner issues a written notice (email with read-receipt) to every member of staff stating: (1) no client data — including names, addresses, case details or file references — may be entered into ChatGPT, Microsoft Copilot or Lexis+ AI until a formal policy is in place; (2) any AI tool not on this list is prohibited entirely; (3) breach will be treated as a disciplinary matter. Retain the distribution record.

Why it matters: Without this directive, personal data from conveyancing, family and probate files may continue to flow into third-party AI systems without a lawful basis, creating live UK GDPR and EU GDPR exposure and potentially waiving legal professional privilege.

☐ **Conduct an emergency data audit to identify what client data has already been processed through AI tools.**

Ask every fee earner to complete a short written disclosure form within five working days identifying: which AI tool was used, on which matter type, what category of data was entered (e.g. client name, financial details, medical information from family files), and whether any EU-resident client was involved. Appoint the practice manager or a senior fee earner to collate responses and flag any special-category data (health, financial vulnerability) processed on family or probate matters.

Why it matters: If personal data has already been processed unlawfully, Halstead & Rowe needs to know now in order to assess whether an ICO breach notification under UK GDPR Article 33 (72-hour window) or an EU supervisory authority notification is required.

☐ **Review and update data processor agreements for ChatGPT (OpenAI), Microsoft Copilot and Lexis+ AI.**

Locate the current terms of service and data processing agreements (DPAs) for each tool. Confirm that each provider signs as a data processor under UK GDPR Article 28 and EU GDPR Article 28, that data is not used for model training without explicit consent, and that sub-processor lists are available. Microsoft Copilot (via Microsoft 365) typically offers a compliant DPA; OpenAI's enterprise tier provides one; verify Lexis+ AI's DPA with LexisNexis directly. Do not use a tool that cannot provide a compliant DPA.

Why it matters: Absence of an Article 28-compliant DPA is itself a UK GDPR and EU GDPR breach, regardless of whether data is misused, and would be an aggravating factor in any ICO or EU supervisory authority investigation.

☐ **Identify the lawful basis for each AI use case and record it in a processing register entry.**

For each of the three declared uses — drafting client correspondence, summarising case documents, and research and analysis — record the lawful basis in Halstead & Rowe's Article 30 record of processing activities. For client correspondence and case summarisation the basis will ordinarily be UK GDPR Article 6(1)(b) (contract) and Article 6(1)(c) (legal obligation); for EU-resident clients the same articles of EU GDPR apply. Where special-category data appears (e.g. health data on family files), identify an Article 9(2) condition — most likely Article 9(2)(f) (legal claims).

Why it matters: Processing personal data through AI without a documented lawful basis exposes the firm to ICO enforcement (maximum fine £17.5 million or 4% of global turnover) and EU supervisory authority enforcement (maximum fine €35 million or 7% of global turnover).

Phase 2 — Foundational Policy and Governance (Weeks 3–8)

Phase 2 builds the internal governance structure that will underpin every subsequent compliance step. Halstead & Rowe has no AI policy in place; this phase creates one, assigns ownership, and establishes the controls the SRA, ICO and EU AI Act Article 9 risk management obligations require. No client data should be processed through AI tools until the policy in Phase 2 is signed off.

☐ **Draft and adopt an AI Acceptable Use Policy specific to Halstead & Rowe.**

The policy must cover: approved tools (ChatGPT enterprise, Microsoft Copilot, Lexis+ AI only); prohibited uses (inputting un-anonymised client data into consumer-tier ChatGPT; using unapproved tools); mandatory human review of all AI outputs before any document is sent to a client or filed; rules on client confidentiality and legal professional privilege; a requirement to disclose AI involvement to clients where material; and disciplinary consequences for breach. The policy should be signed by the managing partner and distributed to all staff with a signed acknowledgement retained on their personnel file.

Why it matters: The SRA's professional conduct rules require the firm to supervise work done on client matters; without a written policy, the firm cannot demonstrate that supervision and faces regulatory sanction if an AI error causes client harm.

☐ **Designate an AI Compliance Lead and define their responsibilities.**

Appoint a named senior fee earner or the practice manager as AI Compliance Lead. Document their responsibilities: maintaining the AI tool register, reviewing and renewing DPAs annually, receiving internal AI incident reports, liaising with the ICO or EU supervisory authority if required, and keeping abreast of regulatory changes. For a firm of 11–50 staff this does not need to be a full-time role, but the appointment must be recorded in writing.

Why it matters: The ICO's AI Auditing Framework expects demonstrable accountability; if the ICO investigates, the absence of a named responsible person is an indicator of systemic failure rather than isolated error.

☐ **Update the firm's Article 30 Record of Processing Activities to include all AI-assisted processing.**

Add a dedicated AI section to the existing ROPA documenting: each tool, the categories of data processed, the purpose, the lawful basis, the retention period, the third-country transfer position (OpenAI and Microsoft may process data in the USA — confirm adequacy decisions or standard contractual clauses apply), and the recipient (the AI provider as processor). Review the record for EU-resident clients separately and confirm the EU GDPR Article 30 entry is complete.

Why it matters: An incomplete ROPA is a standalone UK GDPR and EU GDPR breach and is typically the first document an ICO or EU supervisory authority inspector requests.

☐ **Carry out a Data Protection Impact Assessment for each AI use case.**

UK GDPR Article 35 and EU GDPR Article 35 require a DPIA for processing likely to result in high risk. AI-assisted summarisation of family or probate files almost certainly meets this threshold given the sensitivity of the data. Conduct a DPIA for each of the three use cases using the ICO's standard template. The DPIA must describe the processing, assess necessity and proportionality, identify risks (privilege waiver, data leak, inaccurate AI output used in a client matter), and record mitigation measures. Consult the ICO if a residual high risk cannot be mitigated.

Why it matters: Failure to complete a required DPIA is an independent breach of UK GDPR Article 35 and EU GDPR Article 35 and attracts ICO enforcement independent of any underlying data loss.

☐ **Address EU AI Act Article 50 transparency obligations now in force as of 2 August 2026.**

Article 50 of the EU AI Act is now in force. Where Halstead & Rowe deploys an AI system that interacts directly with EU-resident clients (e.g. an AI-drafted letter, a chatbot, or AI-generated case summary shared with a client), the firm as deployer must inform those clients that AI has been involved. Implement a standard disclosure sentence in client-facing correspondence where AI tools have contributed to the content, for example: 'This document has been prepared with the assistance of AI tools and has been reviewed and approved by a qualified solicitor.' This applies immediately to EU-resident clients and is best practice for all clients.

Why it matters: Non-compliance with Article 50 from 2 August 2026 exposes the firm to enforcement by national AI regulators, with fines for deployers potentially reaching €15 million or 3% of global annual turnover.

- [ ] **Assess whether any AI use case constitutes a high-risk system under EU AI Act Annex III.**

  Review Annex III of the EU AI Act against the firm's three use cases. AI used to draft client correspondence, summarise documents and conduct legal research does not fall within the Annex III high-risk categories (which cover recruitment, credit scoring, law enforcement, administration of justice as a decision-maker, etc.). Document this assessment and the reasoning in writing. Note: the high-risk obligations under Annex III do not apply until 2 December 2027 (as deferred by the Digital Omnibus, in force 29 June 2026), but confirming non-applicability now removes future uncertainty.

  Why it matters: If the firm later adopts a tool that does fall within Annex III without having conducted this assessment, it will have no framework in place when the December 2027 deadline arrives.

- [ ] **Confirm the position on EU AI Act prohibited practices under Article 5 (in force 2 February 2025).**

  Article 5 prohibitions have applied since 2 February 2025. Review each approved tool against the prohibited practices list: subliminal manipulation, exploitation of vulnerabilities, social scoring, real-time remote biometric identification in public spaces. None of the declared use cases (drafting, summarising, research) engages any Article 5 prohibition. Record this conclusion in the AI Compliance Lead's governance log. New prohibitions relating to synthetic intimate imagery apply from 2 December 2026 — not relevant to this firm's use cases but should be noted for future tool additions.

  Why it matters: Deploying a prohibited AI practice carries the highest EU AI Act penalty tier (€35 million or 7% of global turnover); confirming non-applicability in writing protects the firm if its tool choices are ever questioned.

- [ ] **Implement the Data (Use and Access) Act 2025 complaints procedure obligation.**

  The duty on controllers to operate a data protection complaints procedure and respond within set time limits came into force on 19 June 2026. Update Halstead & Rowe's privacy notice and client care letter to reference the complaints procedure. The procedure must allow data subjects (including clients) to complain about AI-assisted processing, and the firm must respond within the statutory time limits. Assign handling of such complaints to the AI Compliance Lead.

  Why it matters: Failure to operate a compliant complaints procedure is a breach of the Data (Use and Access) Act 2025 (in force 19 June 2026) and will be an aggravating factor in any ICO investigation.

Phase 3 — Staff Training and Privilege Safeguards (Weeks 6–12)

Fee earners at Halstead & Rowe began using AI tools on their own initiative. Training is not optional governance hygiene — it is the mechanism by which the policies in Phase 2 become operational reality. Legal professional privilege requires separate attention because it is not addressed by data protection law and cannot be recovered once waived.

- [ ] **Deliver mandatory AI use training to every fee earner and support staff member.**

  Commission or deliver a training session (two hours minimum) covering: the firm's AI Acceptable Use Policy; the risk of privilege waiver when client communications are shared with third-party AI providers; how to use each approved tool without entering un-anonymised data; how to review and verify AI outputs before use; and how to report an AI-related incident. Record attendance. Repeat annually and for all new starters.

  Why it matters: The Pinsent Masons case (May 2026) demonstrates that courts will criticise and sanction firms for unverified AI outputs; training is the firm's primary defence against fee earner error causing client or regulatory harm.

- [ ] **Establish a legal professional privilege protocol for AI-assisted work.**

  Draft a one-page privilege protocol confirming: (a) privileged communications and legal advice must not be entered into any AI tool unless the provider's DPA expressly preserves confidentiality and prohibits onward disclosure; (b) staff must treat AI tool interfaces as potentially discoverable third-party systems unless contractual protections are confirmed; (c) where in doubt, anonymise or paraphrase before entry. Attach this protocol to the AI Acceptable Use Policy and train staff on it specifically.

  Why it matters: Disclosure of privileged material to an AI provider without adequate contractual protection may constitute a waiver of privilege, exposing client communications and the firm to professional negligence claims and SRA disciplinary action.

☐ **Create an internal AI incident reporting process.**

Define what constitutes a reportable AI incident: an AI output used in a client matter that was later found to be incorrect; client data entered into an unapproved tool; a suspected data breach involving an AI system. Provide a simple reporting form (email to the AI Compliance Lead suffices for a firm of this size). Set a 24-hour internal reporting deadline so the firm can assess whether a 72-hour ICO notification under UK GDPR Article 33 is required.

Why it matters: Missing the 72-hour breach notification window under UK GDPR Article 33 is an independent regulatory breach and one of the ICO's most consistently enforced obligations.

Phase 4 — Cross-Jurisdiction Compliance Mapping (Weeks 10–16)

Halstead & Rowe acts for EU-resident clients in conveyancing, family and probate matters. Both UK GDPR and EU GDPR apply. The EU AI Act applies to the extent the firm deploys AI systems that affect EU-resident individuals. This phase maps which obligations are satisfied once and which require separate action for each regime.

☐ **Produce a written cross-jurisdiction compliance position statement.**

The AI Compliance Lead produces a one-page document recording the following position, which must be updated whenever the law or the firm's tools change. Obligations satisfied once for both regimes: Article 28/30 compliant DPAs and ROPA entries (one document covers both UK and EU data subjects if drafted to reference both regimes); DPIA process (a single DPIA template works for both, provided it references both Article 35 UK GDPR and Article 35 EU GDPR); staff training on data protection and privilege (regime-neutral content). Obligations that must be met separately: UK GDPR breach notification goes to the ICO; EU GDPR breach notification for EU-resident clients goes to the relevant EU member state supervisory authority (determined by the client's country of residence). Article 50 EU AI Act transparency disclosures must be made to EU-resident clients; there is no equivalent UK statutory requirement yet, though it is best practice for all clients. The Data (Use and Access) Act 2025 complaints procedure is a UK-specific obligation; EU-resident clients retain their EU GDPR complaint rights to their national DPA.

Why it matters: Without a clear map of which obligations are shared and which are separate, the firm risks treating a UK-only compliance step as sufficient for EU-resident clients, creating undetected EU GDPR and EU AI Act exposure.

☐ **Apply the stricter obligation where the two regimes diverge.**

Where UK and EU obligations differ, apply the stricter one to all clients. Key divergences: (1) Automated decision-making — UK GDPR Article 22 as amended by the Data (Use and Access) Act 2025 (in force 5 February 2026) provides wider lawful bases for solely automated decisions; EU GDPR Article 22 retains stricter defaults. Halstead & Rowe has confirmed AI is not used in decisions about people, so Article 22 does not currently apply in either regime — record this. (2) AI transparency — EU AI Act Article 50 (in force 2 August 2026) imposes a mandatory disclosure duty for EU-resident clients; the UK has no equivalent statutory duty. Apply the EU standard to all clients as the stricter obligation. (3) GPAI rules — General-purpose AI model obligations under the EU AI Act have applied since 2 August 2025; these fall on providers (OpenAI, Microsoft, LexisNexis), not on Halstead & Rowe as deployer. The firm's obligation is to ensure it uses only GPAI-compliant tools — verify each provider's compliance status.

Why it matters: Applying only the less demanding regime to clients who are protected by both creates live regulatory exposure in the stricter jurisdiction without any operational benefit.

☐ **Verify GPAI provider compliance for ChatGPT, Microsoft Copilot and Lexis+ AI.**

Contact each provider and request written confirmation that they comply with the EU AI Act general-purpose AI (GPAI) obligations in force since 2 August 2025, including transparency obligations to downstream deployers. For OpenAI and Microsoft, review their published EU AI Act compliance statements. For Lexis+ AI (LexisNexis), request a specific written confirmation. Retain these confirmations on the AI Compliance Lead's governance file. If a provider cannot confirm GPAI compliance, suspend use for EU-resident client matters until they can.

Why it matters: The firm as deployer has a due-diligence obligation; using a non-compliant GPAI model in EU-resident client matters may make the firm complicit in the provider's breach and undermine its own compliance position.

Phase 5 — Ongoing Monitoring and Foundational Compliance Declaration (Months 4 Onwards)

When Phases 1–4 are complete, Halstead & Rowe can honestly state that foundational compliance is in place. This phase describes the monitoring required to keep it there, the point at which that declaration can be made, and the forward-looking obligations the firm must track.

☐ **Declare foundational compliance once all prior phases are verified complete.**

The AI Compliance Lead prepares a brief signed attestation confirming completion of: interim directive issued; data audit completed; DPAs reviewed; ROPA updated; DPIAs completed; AI Acceptable Use Policy adopted; Article 50 disclosures implemented; Article 5 prohibited practices confirmed inapplicable; Annex III high-risk assessment documented; Data (Use and Access) Act complaints procedure operational; training delivered; privilege protocol adopted; incident reporting process live; cross-jurisdiction position statement produced; GPAI provider confirmations received. The managing partner countersigns. This document is the firm's first line of defence in any ICO or EU supervisory authority enquiry.

Why it matters: Without a recorded declaration, the firm cannot demonstrate to the ICO, EU supervisory authorities, the SRA, insurers or clients that it has met its obligations — even if the underlying work has been done.

☐ **Schedule quarterly reviews of AI tools, policies and regulatory developments.**

The AI Compliance Lead conducts a quarterly review covering: any new AI tools requested by fee earners (must be approved and DPA-reviewed before use); changes to the EU AI Act implementation timeline (specifically the 2 December 2026 new prohibitions and 2 December 2027 Annex III high-risk deadline); ICO AI Auditing Framework updates; SRA guidance on AI; and any changes to the firm's client base (e.g. increase in EU-resident clients). Outcomes are recorded in the governance log.

Why it matters: The EU AI Act's phased implementation means new obligations are coming into force on fixed dates; missing the 2 December 2026 or 2 December 2027 deadlines will be harder to defend if the firm has not maintained active monitoring.

☐ **Monitor the 2 December 2026 EU AI Act obligations and prepare in advance.**

From October 2026, review the firm's use of generative AI tools (ChatGPT, Copilot) against the new obligations taking effect on 2 December 2026: the Article 50(2) machine-readable marking requirement for synthetic content, and the new prohibitions on AI generating non-consensual intimate imagery (not applicable to this firm's use cases but confirm). Confirm with OpenAI and Microsoft that their tools will carry compliant markings by that date. Update client disclosure wording if required.

Why it matters: The Article 50(2) marking obligation falls on providers, but the firm's client-facing disclosures must remain accurate; failure to update them after the December 2026 changes could create a misleading impression about AI involvement.

☐ **Prepare for the Annex III high-risk deadline of 2 December 2027 and confirm continued non-applicability.**

By June 2027, the AI Compliance Lead re-runs the Annex III assessment against any AI tools the firm has adopted since Phase 2. If any tool is or becomes an Annex III high-risk system (for example, an AI system used to assess client creditworthiness or make eligibility determinations in probate matters), the firm must prepare a risk management system per Article 9, technical documentation, and human oversight measures well before 2 December 2027. If non-applicability is confirmed again, record that conclusion.

Why it matters: The Digital Omnibus deferred, but did not remove, the Annex III obligations; a firm that waits until November 2027 to assess applicability will have no realistic prospect of achieving compliance before the deadline.

☐ **Maintain readiness for ICO audit under the ICO AI Auditing Framework.**

The ICO's AI Auditing Framework sets out the accountability and governance standards the ICO applies when auditing AI deployments. Ensure the firm's governance log, ROPA, DPIAs, DPAs, training records, incident log and cross-jurisdiction position statement are held centrally and can be produced within 72 hours of an ICO request. The AI Compliance Lead should review the ICO's published audit outcomes (including the November 2024 recruitment AI audit) for any findings applicable to legal services AI use.

Why it matters: The ICO has named AI as a key enforcement priority; a firm that cannot produce coherent documentation at short notice signals systemic non-compliance and risks an escalated enforcement response.

Data Classification Matrix

Which categories of your data may go near an AI tool, and which may never. The one page staff refer to before pasting anything in.

Classification	Examples in this business	May be used with AI	Conditions if permitted	Approval required from
PUBLIC	Halstead & Rowe website content, published court judgments, SRA regulatory guidance, publicly filed Land Registry title numbers	YES — ChatGPT, Copilot, Lexis+ AI	Confirm data is genuinely in the public domain before input. No client names appended.	None — fee earner discretion
INTERNAL	Firm precedent templates, internal procedure notes, anonymised training scenarios, billing rate schedules, generic conveyancing checklists	YES — Copilot and Lexis+ AI preferred; ChatGPT permitted	All client identifiers removed before input. Use firm-approved accounts only. Do not paste into personal or unapproved instances.	Supervising fee earner
CONFIDENTIAL — CLIENT (non-special-category)	Named conveyancing transaction details, probate estate values, family law chronologies, client contact data, matter references	CONDITIONAL — Lexis+ AI only unless otherwise approved	Data-processing agreement with provider confirmed. UK GDPR Art 28 processor contract in place. Input minimised to what the task requires. No EU-resident client data via ChatGPT until SCCs verified.	Head of Department + COLP sign-off
CONFIDENTIAL — PRIVILEGED	Legal advice on family disputes, counsel's opinions, without-prejudice correspondence, litigation strategy notes, privileged attendance notes	CONDITIONAL — Lexis+ AI only; human review mandatory before output is used	Privilege must not be waived by disclosure to third-party AI provider acting outside a confirmed processor role. Confirm provider terms do not assert right to train on inputs. Document decision to use AI on the file.	COLP + Partner responsible for matter
RESTRICTED — SPECIAL CATEGORY (Art 9 UK GDPR / Art 9 EU GDPR)	Client health data in personal injury or capacity assessments, religious beliefs in family/probate matters, immigration status, trade union membership in employment-related matters	NO — not without explicit Partner and DPO authorisation	If authorised: explicit consent or Art 9(2)(f) legal claims basis documented. Strict data minimisation. Lexis+ AI only. EU-resident clients: EU GDPR Art 9 applies in parallel; stricter condition governs.	Partner + DPO (written, case-specific)
RESTRICTED — CRIMINAL OFFENCE DATA (Art 10 UK GDPR / Art 10 EU GDPR)	Criminal conviction history in family proceedings, DBS check results, fraud allegations in probate disputes, client cautions referenced in correspondence	NO	Art 10 UK GDPR prohibits processing outside official authority or specific legal basis. No AI tool currently approved for this data. Any future use requires separate DPIA and COLP sign-off.	COLP — no standing approval available
Classification	**Examples in this business**	**May be used with AI**	**Conditions if permitted**	**Approval required from**
RESTRICTED — EU-RESIDENT CLIENT DATA	Any personal data relating to clients resident in EU member states across all matter types (conveyancing,	CONDITIONAL — Lexis+ AI only where EU SCCs or adequacy	EU GDPR applies alongside UK GDPR. AI Act Art 13 transparency duties in force from 2 Aug 2026. Confirm no transfer to	COLP + DPO (per matter type)

Classification	Examples in this business	May be used with AI	Conditions if permitted	Approval required from
	family, probate)	confirmed	third-country server without Art 46 safeguard. Where UK and EU obligations diverge, the stricter obligation applies.	

DOCUMENT OWNER: COLP, Halstead & Rowe Solicitors. REVIEW CADENCE: Annually and immediately upon any change to approved AI tools, provider terms, or applicable law. EFFECTIVE DATE: 08 August 2026.

TOOLS IN SCOPE: ChatGPT (OpenAI), Microsoft Copilot, Microsoft, Lexis+ AI (LexisNexis). Only firm-approved accounts may be used. Fee earners must not create personal accounts or use unapproved instances. Use of any AI tool not listed here is prohibited pending formal approval by the COLP.

LEGAL BASIS SUMMARY — UK: UK GDPR Arts 5, 6, 9, 10, 28; Data (Use and Access) Act 2025 Part 5 provisions in force from 5 Feb 2026 (automated-decision safeguards) and 19 Jun 2026 (complaints procedure duty); ICO AI Auditing Framework; UK Equality Act 2010 (AI outputs must not produce discriminatory results affecting staff or clients). UK GDPR Art 22 on solely automated decisions does not currently apply as the firm has confirmed AI is not used for decisions about people, but this must be kept under review. EU: EU GDPR Arts 5, 6, 9, 10, 28, 46; EU AI Act 2024/1689 Art 50 transparency duties in force from 2 Aug 2026 — clients must be informed when AI has materially assisted in drafting correspondence directed at them; Art 5 prohibited practices (social scoring, manipulation) not applicable to the firm's declared uses; Annex III high-risk obligations deferred to 2 Dec 2027 by Digital Omnibus (in force 29 Jun 2026) — current uses (drafting, summarising, research) do not appear to fall within Annex III but this must be confirmed as the firm's AI use evolves; Art 9 risk management and Art 13 transparency apply now where EU-resident clients are involved; GPAI rules for general-purpose AI models (e.g. ChatGPT, Copilot) in force from 2 Aug 2025 — providers bear primary obligations but the firm as deployer must verify provider compliance before use with client data.

CROSS-JURISDICTION DIVERGENCE: Obligations satisfied once for both regimes: Art 28/processor contracts, data minimisation, purpose limitation, staff training records, DPIA process. Obligations that must be met separately: (1) EU AI Act Art 50 transparency notices to EU-resident clients — UK GDPR has no equivalent obligation; comply separately for EU clients. (2) EU GDPR Art 46 transfer mechanism for any data leaving the UK/EEA to a third-country AI server — UK adequacy decisions are separate from EU ones; check both. (3) Fines exposure is cumulative: ICO maximum £17.5m or 4% global turnover; EU AI Act maximum €35m or 7% global turnover (turnover-based limb cannot be computed without the firm's figures — apply the statutory cap as the planning figure). Where obligations diverge, the stricter obligation is applied throughout this matrix.

PRIVILEGE WARNING: Inputting privileged material into a third-party AI tool may constitute a waiver of legal professional privilege if the provider is not acting as a processor under a compliant Art 28 agreement and the communication is treated as a disclosure to a third party. Confirm provider terms before any privileged content is used. The Pinsent Masons case (London, May 2026) is a live reminder that AI-generated outputs in legal proceedings must be verified by a qualified fee earner before reliance.

SPECIAL CATEGORY AND CRIMINAL OFFENCE DATA — AI Act intersection: These categories attract the highest protection under both UK and EU GDPR. The firm's family and probate practice routinely handles health, religious belief, and criminal offence data. No standing approval exists for AI processing of these categories. Any proposed use requires a case-specific DPIA, explicit legal basis documentation, and written COLP and DPO sign-off before any input occurs.

COMPLAINTS PROCEDURE: From 19 Jun 2026 the firm is under a statutory duty (DUAA 2025) to operate a complaints procedure and respond to data protection complaints within set time limits. Any complaint relating to AI use of personal data must be logged and escalated to the COLP on the same working day it is received.

GDPR Compliance Position

Your documented data protection position for each AI tool — what a customer's procurement team asks for.

ChatGPT (OpenAI)

GDPR COMPLIANCE POSITION — ChatGPT (OpenAI)
Halstead & Rowe Solicitors | Prepared: 08 August 2026

Controller/Processor Roles and Lawful Basis
Halstead & Rowe Solicitors acts as data controller. OpenAI operates as data processor when processing personal data on the firm's behalf under the ChatGPT Enterprise or API terms. Where fee earners use consumer-tier ChatGPT accounts, OpenAI may act as an independent controller for its own purposes. The firm must confirm which tier is in use; if consumer-tier accounts are in use, the processor relationship is not established and the firm lacks the contractual protections required under UK GDPR Art 28 and EU GDPR Art 28.

Lawful basis for processing personal data through ChatGPT: Article 6(1)(b) UK/EU GDPR (performance of a contract with the data subject) for conveyancing and probate matters where the client is a party; Article 6(1)(c) (legal obligation) where processing is required by law; Article 6(1)(f) (legitimate interests) for internal case analysis where client interests do not override. Where special-category data is present (e.g. health information in family files), Article 9(2)(f) (legal claims) or 9(2)(a) (explicit consent) is required in addition. No solely automated decision-making affecting clients is declared; UK GDPR Art 22 and EU GDPR Art 22 are therefore not triggered, but this must be reviewed if AI outputs are acted on without human review.

Categories of Data and Data Subjects
Data categories in scope: names, addresses, financial details, property information (conveyancing); family relationships, health and medical information, financial circumstances (family); beneficiary details, asset schedules, will instructions (probate). Data subjects include clients, opposing parties, witnesses, beneficiaries, and third parties named in case documents. Health and relationship-status data constitute special-category data under Art 9. The firm holds files relating to EU-resident clients, bringing those individuals within the scope of EU GDPR.

Transfer Position and Mechanism
OpenAI is a US-based entity. Processing by ChatGPT involves a transfer of personal data to the United States.

UK position: Transfers must comply with UK GDPR Chapter V. The UK has not issued an adequacy regulation covering the United States under the general UK GDPR framework (the UK-US Data Bridge covers only Bridge-certified US organisations). The firm must confirm whether OpenAI's relevant entity holds current UK Data Bridge certification. If not, the transfer must rely on the ICO's International Data Transfer Agreement (IDTA) or the Addendum to the EU Standard Contractual Clauses. The firm must execute the appropriate transfer mechanism before processing client data through ChatGPT.

EU position: For EU-resident clients, EU GDPR Chapter V applies. The EU–US Data Privacy Framework (adequacy decision, July 2023) covers transfers to certified US organisations. The firm must confirm whether the relevant OpenAI entity is certified under the DPF. If not, EU SCCs (Commission Implementing Decision 2021/914) must be executed. Where both regimes apply, the stricter obligation is applied: both transfer mechanisms must be in place concurrently for files involving EU-resident clients.

Retention and Model-Training Position
OpenAI's enterprise and API terms state that inputs and outputs are not used to train OpenAI models by default and are retained for a limited period (currently up to 30 days for abuse monitoring under enterprise terms, zero-day retention available via API zero-data-retention option). Consumer-tier ChatGPT retains conversation history and may use data for model improvement unless the user opts out. The firm must: (a) confirm it is not using consumer-tier accounts for client data; (b) obtain and retain written confirmation from OpenAI of its current retention and no-training position; and (c) document this in its Records of Processing Activities (ROPA) under UK GDPR Art 30 and EU GDPR Art 30.

Data Processing Agreement
A DPA meeting the requirements of UK GDPR Art 28 and EU GDPR Art 28 must be in place. OpenAI provides a Data Processing Addendum for enterprise and API customers. The firm must: (a) execute this addendum before processing any client personal data; (b) ensure it covers sub-processor obligations (OpenAI uses Microsoft Azure infrastructure); (c) verify it includes the required provisions for the firm to conduct audits and for OpenAI to assist with data subject rights requests. If consumer-tier accounts are currently in use, no compliant DPA exists. This is a material gap requiring immediate remediation.

Overall Position — ChatGPT
Current status: NON-COMPLIANT pending remediation. Fee earners are using ChatGPT on their own initiative without an approved enterprise agreement, a DPA, or verified transfer mechanisms. Client confidentiality and legal privilege are at risk. Immediate actions required: (1) prohibit consumer-tier use for all client data with immediate effect; (2) execute an enterprise or API agreement and DPA with OpenAI; (3) establish IDTA/UK Data Bridge confirmation for UK transfers and DPF/SCC confirmation for EU transfers; (4) update ROPA; (5) issue a staff directive restricting use to approved accounts only.

Microsoft Copilot

GDPR COMPLIANCE POSITION — Microsoft Copilot
Halstead & Rowe Solicitors | Prepared: 08 August 2026

Controller/Processor Roles and Lawful Basis
Halstead & Rowe Solicitors acts as data controller. Microsoft acts as data processor under the Microsoft Products and Services Data Protection Addendum (DPA), which is incorporated by reference into the Microsoft Customer Agreement and the Microsoft Online Services Terms. This applies to Microsoft Copilot for Microsoft 365 (the commercial, tenant-bound product). If fee earners are using Copilot via a personal Microsoft account or the consumer Bing-integrated Copilot, the processor relationship does not apply and Microsoft may act as an independent controller.

Lawful basis: as stated for ChatGPT above — Art 6(1)(b), (c), or (f) depending on context; Art 9(2)(f) or (a) for special-category data. No automated decision-making affecting data subjects is declared; UK GDPR Art 22 and EU GDPR Art 22 not triggered provided human review is maintained.

Categories of Data and Data Subjects
Identical in scope to ChatGPT above: client personal and special-category data across conveyancing, family and probate files; data subjects include clients, third parties, beneficiaries and opposing parties. EU-resident clients bring EU GDPR into scope. Copilot for Microsoft 365 processes data within the firm's Microsoft 365 tenant, meaning it can access emails, documents and Teams conversations stored in that tenant. This represents a wider attack surface than a standalone tool and requires careful scope management through Microsoft Purview sensitivity labels and data loss prevention policies.

Transfer Position and Mechanism
Microsoft is a US-based entity with EU and UK data-centre regions.

UK position: Microsoft's standard enterprise terms include EU-region and UK-region data residency options for Microsoft 365 commercial customers. Where data residency is configured for the UK, personal data in the tenant at rest is stored in UK data centres. However, processing by Microsoft's AI infrastructure may involve transfers. The Microsoft DPA incorporates the ICO IDTA and the EU SCCs Addendum for UK transfers. The firm must verify its tenant data-residency configuration and confirm that Copilot processing is covered by the current Microsoft DPA and IDTA.

EU position: Microsoft participates in the EU–US Data Privacy Framework. For EU-resident client data, the firm must confirm that the relevant Microsoft contracting entity is DPF-certified or that EU SCCs are in place. The Microsoft DPA includes EU SCCs. The firm must ensure the correct Microsoft entity is named in its DPA and that the DPA is executed for the firm's tenant.

Divergence: EU GDPR imposes an obligation to document transfer impact assessments (TIAs) more explicitly than current ICO guidance requires. Where EU-resident client data is processed, the firm must maintain a TIA for Microsoft Copilot transfers. This is the stricter obligation and is applied here.

Retention and Model-Training Position
Microsoft Copilot for Microsoft 365 does not use customer tenant data to train foundation models. Microsoft's published commitments state that prompts, responses and data accessed by Copilot are not used for model training. Prompt and response data is retained within the tenant's compliance boundary subject to the firm's own retention policies. The firm must: (a) confirm it holds a Microsoft 365 commercial licence (not a consumer account); (b) configure Microsoft Purview retention policies to align with SRA file-retention requirements (minimum six years post-matter for most files); (c) review Copilot interaction logs, which are stored in Exchange Online and accessible via eDiscovery, and ensure these are within scope of the firm's data retention and deletion policy.

Data Processing Agreement
The Microsoft Products and Services DPA is automatically incorporated for commercial Microsoft 365 customers and satisfies UK GDPR Art 28 and EU GDPR Art 28. The firm must: (a) confirm it holds a commercial (not consumer or education) Microsoft 365 licence; (b) retain a copy of the applicable Microsoft DPA version in its compliance records; (c) ensure the DPA is referenced in the firm's ROPA entry for Copilot. No additional bespoke DPA negotiation is required if the standard commercial terms are in place. Gap: if any fee earner is using Bing-integrated Copilot via a personal account, no DPA covers that use. This must be prohibited by firm policy.

Overall Position — Microsoft Copilot
Conditional compliance. Where Copilot for Microsoft 365 is used under a commercial licence with data residency configured, the DPA, transfer mechanism and no-training position are structurally in place via Microsoft's standard terms. The firm's immediate actions are: (1) confirm all Copilot use is via the commercial Microsoft 365 tenant, not personal accounts; (2) verify data-residency configuration; (3) configure Purview sensitivity labels to prevent Copilot accessing documents above the permitted classification; (4) update ROPA; (5) complete a TIA for EU-resident client data flows; (6) issue a staff directive confirming approved use parameters.

Lexis+ AI

GDPR COMPLIANCE POSITION — Lexis+ AI
Halstead & Rowe Solicitors | Prepared: 08 August 2026

Controller/Processor Roles and Lawful Basis
Halstead & Rowe Solicitors acts as data controller. LexisNexis operates as data processor under the terms of the firm's subscription agreement, which includes a data processing addendum. Lexis+ AI is a closed, subscription-based legal research platform; it does not expose the firm's data to general training pipelines in the same way as consumer AI tools. The firm must confirm that its current subscription agreement incorporates a DPA meeting UK GDPR Art 28 requirements and, for EU-resident client data, EU GDPR Art 28.

Lawful basis: Art 6(1)(b) (performance of contract) for client matter research; Art 6(1)(f) (legitimate interests) for general legal analysis. Lexis+ AI is used for research and analysis rather than drafting client-facing documents, which reduces the risk of AI-generated inaccuracies reaching clients directly. However, where research outputs inform advice given to EU-resident clients, EU GDPR applies to any personal data processed in that context.

Categories of Data and Data Subjects
The primary data processed through Lexis+ AI is case-related research queries. Fee earners may inadvertently include client names, property addresses, financial figures, or family details when formulating queries. If they do, the data categories and data subjects are the same as those described for ChatGPT above. The firm must issue guidance to fee earners that queries should be anonymised or pseudonymised before submission to Lexis+ AI wherever possible, so that client personal data is not transmitted to the platform unnecessarily. This satisfies the data-minimisation obligation under UK GDPR Art 5(1)(c) and EU GDPR Art 5(1)(c).

Transfer Position and Mechanism
LexisNexis is a US-based entity (RELX Group). Lexis+ AI is delivered as a cloud service.

UK position: The firm must confirm whether LexisNexis's relevant contracting entity holds current UK Data Bridge certification or whether the firm's subscription DPA incorporates the ICO IDTA or EU SCCs Addendum. LexisNexis publishes a Privacy Centre with transfer mechanism information; the firm must obtain and retain the applicable document.

EU position: For EU-resident client data, LexisNexis must be either DPF-certified or covered by EU SCCs. The firm must confirm this from LexisNexis's published DPA or by written confirmation from its account manager. Where both regimes apply, both mechanisms must be documented. This is the stricter position and is applied here.

Divergence: The EU GDPR requires the firm to conduct a TIA where transfers rely on SCCs. The ICO encourages but does not yet mandate a TIA in the same prescriptive terms. The firm must complete a TIA for any Lexis+ AI transfers involving EU-resident client data. This obligation does not arise under UK GDPR alone but applies here because EU GDPR is in scope.

Retention and Model-Training Position
LexisNexis's published terms for Lexis+ AI state that customer query data is not used to train the underlying AI model and that query data is processed solely to return search results within the platform session. The firm must obtain written confirmation of the current retention period for query logs and ensure this is reflected in its ROPA. If LexisNexis retains query logs for any period, the firm must ensure that anonymised queries are used wherever client identifiers would otherwise be included, as described above.

Data Processing Agreement
LexisNexis provides a DPA as part of its enterprise subscription terms. The firm must: (a) confirm the DPA is executed and current; (b) verify it covers Lexis+ AI specifically (some DPAs may reference earlier product names); (c) confirm sub-processor obligations are covered (LexisNexis uses cloud infrastructure providers); (d) ensure the DPA includes provisions for the firm to exercise data subject rights on behalf of clients. If the current subscription predates Lexis+ AI's launch and the DPA has not been updated, a refreshed DPA must be requested from LexisNexis. Gap: no evidence in the firm's current records that a Lexis+ AI-specific DPA has been executed. This must be confirmed or remediated.

Overall Position — Lexis+ AI
Lexis+ AI carries lower inherent risk than the other two tools because it is a closed subscription platform used primarily for research rather than drafting. Structural protections (no model training on customer data, enterprise DPA) are available but must be confirmed as executed. Immediate actions: (1) confirm DPA covers Lexis+ AI and is current; (2) obtain transfer mechanism confirmation for both UK and EU data flows; (3) issue fee earner guidance on query anonymisation; (4) complete TIA for EU-resident client data; (5) update ROPA.

Overall Position Statement

OVERALL DATA PROTECTION POSITION — ALL AI TOOLS
Halstead & Rowe Solicitors | Prepared: 08 August 2026

Summary Assessment
As at 08 August 2026, Halstead & Rowe Solicitors does not have a documented, compliant data protection position for any of its three AI tools. Fee earners have adopted ChatGPT, Microsoft Copilot and Lexis+ AI on their own initiative without firm-level approval, without executed DPAs confirmed to be current and AI-specific, and without verified international transfer mechanisms. This creates material exposure under UK GDPR, EU GDPR, and the Data (Use and Access) Act 2025 (Part 5 provisions in force from 5 February 2026 and complaints-procedure duty in force from 19 June 2026).

Maximum regulatory exposure: UK ICO — £17.5 million or 4% of global annual turnover (the turnover-based limb cannot be computed without the firm's figures). EU supervisory authority — €35 million or 7% of global annual turnover. Both maxima apply concurrently where EU-resident clients are affected.

Cross-Jurisdiction Position
Obligations satisfied once for both regimes (where the same action meets both UK GDPR and EU GDPR): (a) executing a compliant Art 28 DPA with each processor — a single DPA drafted to the higher EU GDPR standard satisfies both; (b) maintaining a ROPA under Art 30 — a single record covering both regimes satisfies both provided it identifies which data subjects are EU-resident; (c) data minimisation and purpose limitation under Art 5 — a single policy applying the stricter standard satisfies both; (d) data subject rights procedures — a single procedure satisfying EU GDPR timescales (one month, Art 12) also satisfies UK GDPR.

Obligations that must be met separately: (a) international transfer mechanisms — the firm needs an IDTA or UK Data Bridge confirmation for UK GDPR transfers AND EU SCCs or DPF confirmation for EU GDPR transfers; these cannot be collapsed into a single instrument; (b) Transfer Impact Assessments — required under EU GDPR for SCC-based transfers; not yet mandatorily required under ICO guidance for IDTA-based transfers, but the firm must prepare one for EU flows; (c) supervisory authority notification — the ICO is the lead UK supervisory authority; for EU-resident clients, the competent EU supervisory authority is determined by the EU member state of the client's habitual residence; a single notification to the ICO does not satisfy an obligation to notify an EU DPA; (d) complaints procedure — the duty to operate a complaints procedure and respond within set time limits is now in force under the Data (Use and Access) Act 2025 (19 June 2026); this is a UK-specific obligation with no direct EU GDPR equivalent, though EU GDPR Art 77 complaint rights must also be facilitated.

Priority Remediation Actions
1. Immediately restrict ChatGPT use to an enterprise or API account with an executed DPA; prohibit consumer-tier use for all client data.
2. Confirm Microsoft Copilot is deployed via the commercial Microsoft 365 tenant; verify data residency; configure Purview controls.
3. Obtain and execute a current Lexis+ AI-specific DPA from LexisNexis.
4. For each tool: obtain written confirmation of the applicable transfer mechanism for both UK and EU data flows and file it in the compliance record.
5. Complete Transfer Impact Assessments for EU-resident client data flows for all three tools.
6. Update the firm's ROPA to include all three AI tools as processing activities.
7. Issue a firm-wide AI acceptable use policy restricting AI tool use to approved accounts and requiring query anonymisation where possible.
8. Implement the complaints procedure required under the Data (Use and Access) Act 2025.
9. Review Lexis+ AI query logs and ChatGPT/Copilot interaction logs against the firm's file-retention schedule and SRA requirements.
10. Designate a named individual (partner or compliance officer) responsible for AI data protection oversight and schedule a six-month review of this position statement.

This document represents the firm's data protection compliance position for AI tools as at 08 August 2026. It should be reviewed immediately upon execution of each DPA and transfer mechanism and no later than 08 February 2027.

Employee AI Policy Acknowledgement Form

Each member of staff signs one. Keep the signed copies — they are your evidence that the policy was communicated, which is the first thing asked for after an incident.

This form is completed by each member of staff at Halstead & Rowe Solicitors before using any approved AI tool. Signed copies are retained as evidence of policy communication and are the firm's primary record in the event of a regulatory enquiry, client complaint or incident investigation.

HALSTEAD & ROWE SOLICITORS
EMPLOYEE AI POLICY ACKNOWLEDGEMENT FORM

CONFIDENTIAL — RETAIN IN PERSONNEL FILE

SECTION 1 — EMPLOYEE DETAILS

Full name: [FULL NAME]

Job title: [JOB TITLE]

Department: [DEPARTMENT]

Date of signature: [DATE]

SECTION 2 — POLICY CONFIRMATION

I confirm that I have read, understood and will comply with the Halstead & Rowe Solicitors AI Acceptable Use Policy (version dated [POLICY VERSION DATE]) and all accompanying guidelines issued by the firm. I understand the policy governs how AI tools must be used in connection with client files, including conveyancing, family and probate matters.

SECTION 3 — APPROVED TOOLS

I am authorised to use only the AI tools listed below. Use of any other AI tool for firm or client work is prohibited without prior written approval from [POLICY OWNER NAME/ROLE].

Approved tool(s) authorised for this employee (tick all that apply):

[ ] ChatGPT (OpenAI) — for: [PERMITTED USE, e.g. drafting correspondence]
[ ] Microsoft Copilot — for: [PERMITTED USE, e.g. summarising documents]
[ ] Lexis+ AI — for: [PERMITTED USE, e.g. research and analysis]

I understand that no unprompted or unapproved tool may be used to process any client data, privileged material or personal data, and that doing so may constitute a breach of professional duty, a UK GDPR / EU GDPR violation, and a disciplinary matter.

SECTION 4 — LEGAL AND REGULATORY OBLIGATIONS

I acknowledge that my use of approved AI tools is subject to the following legal frameworks, which the firm is required to observe:

UK: UK GDPR (including Art 22 on automated decision-making); the Data (Use and Access) Act 2025 (Part 5 data protection provisions in force from 5 February 2026; complaints procedure duty in force from 19 June 2026); the ICO AI Auditing Framework; and the UK Equality Act 2010. Maximum ICO fine: £17.5 million or 4% of global turnover.

EU: EU AI Act (Regulation 2024/1689) — Art 5 prohibited practices; Art 13 transparency; Art 9 risk management; Art 50 transparency duties (in force 2 August 2026); GPAI rules (in force 2 August 2025).

High-risk obligations under Annex III apply from 2 December 2027 following the Digital Omnibus deferral of 29 June 2026. Maximum fine: €35 million or 7% of global turnover. These obligations apply because the firm acts for EU-resident clients.

Note on Art 22 / automated decisions: The firm has confirmed it does not use AI to make decisions solely about individuals. Art 22 UK GDPR therefore imposes no immediate operational duty on me at present, but I must not configure or use any tool in a way that would introduce automated decision-making without prior written approval.

Note on EU AI Act Art 50: As of 2 August 2026, I must ensure that where I use AI to generate content sent to clients or counterparties, the AI-assisted nature is disclosed where required. The marking of synthetic content under Art 50(2) comes into force on 2 December 2026; the firm will issue further guidance before that date.

SECTION 5 — CONFIDENTIALITY AND PRIVILEGE

I understand that client files held by Halstead & Rowe Solicitors attract legal professional privilege and strict confidentiality duties. I will not input privileged material, personal data or confidential client information into any AI tool unless the firm has confirmed in writing that the relevant data processing agreement and privacy safeguards are in place for that tool. I understand that inadvertent disclosure may waive privilege and breach UK GDPR / EU GDPR, risking regulatory sanction and professional disciplinary action.

SECTION 6 — INCIDENT REPORTING DUTY

I acknowledge a duty to report promptly any AI-related incident to [DESIGNATED CONTACT NAME/ROLE]. Reportable incidents include: accidental input of personal or privileged data into an unapproved tool; unexpected or inaccurate AI outputs used in client work without verification; any suspected data breach involving an AI tool; and any third-party claim or complaint relating to AI-generated content.

I will report incidents by: [REPORTING CHANNEL, e.g. email to dpo@halsteadrowe.co.uk]

I understand that failure to report an incident may itself constitute a breach of firm policy and regulatory obligations.

SECTION 7 — EMPLOYEE SIGNATURE

I confirm that all statements in this form are true and that I accept the obligations set out above.

Signature: [EMPLOYEE SIGNATURE]

Date: [DATE]

SECTION 8 — COUNTERSIGNATURE BY POLICY OWNER

I confirm that this form has been completed and signed in my presence or submitted through the firm's verified process, and that a copy of the current AI Acceptable Use Policy was provided to the employee named above.

Policy owner name: [POLICY OWNER NAME]

Role: [POLICY OWNER ROLE]

Signature: [POLICY OWNER SIGNATURE]

Date: [DATE]

SECTION 9 — FILING AND RETENTION

The signed original of this form is filed in: [LOCATION, e.g. the employee's personnel file held by HR / the firm's compliance records system].

Retention period: This form will be retained for a minimum of [6] years from the date of signature, or for such longer period as required by applicable law or regulatory guidance, whichever is the later.

Responsible for filing: [NAME/ROLE]

Full ICO AI Auditing Framework Assessment

The detailed assessment against the regulator's auditing framework — the document to produce if you are ever audited.

ICO AI Auditing Framework Assessment — Halstead & Rowe Solicitors

Document reference: H&R-AI-AUDIT-001;
Prepared by: AI Compliance Consultant
Date: 08 August 2026
Scope: ChatGPT (OpenAI), Microsoft Copilot, Lexis+ AI
Uses in scope: Drafting client correspondence, summarising case documents, research and analysis
Jurisdictions: England & Wales (UK GDPR, Data (Use and Access) Act 2025, ICO AI Auditing Framework, UK Equality Act 2010); European Union (EU AI Act 2024/1689) where Halstead & Rowe acts for EU-resident clients.

This assessment has been prepared to satisfy the ICO AI Auditing Framework and to provide an audit-ready record demonstrating Halstead & Rowe Solicitors' compliance position across both UK and EU regulatory regimes. All verified commencement dates in this document reflect primary legislative sources and supersede any press commentary.

1. Governance and Accountability

Halstead & Rowe Solicitors currently has no documented AI governance policy. Fee earners have adopted ChatGPT, Microsoft Copilot, and Lexis+ AI on their own initiative across the conveyancing, family, and probate practice areas without formal approval, risk assessment, or senior oversight. This represents a material governance gap under the ICO AI Auditing Framework, which requires controllers to demonstrate that AI use is subject to defined accountability structures, policy controls, and management oversight proportionate to the risks involved.

Under UK GDPR Article 5(2), Halstead & Rowe, as a data controller, must be able to demonstrate compliance with all data protection principles. The absence of an AI policy means the firm cannot currently discharge this accountability obligation. The Data (Use and Access) Act 2025 (commenced in its principal data protection provisions on 5 February 2026) introduced a statutory duty on controllers to operate a complaints procedure and respond to data protection complaints within prescribed time limits, with that duty having commenced on 19 June 2026. Halstead & Rowe must ensure its complaints handling procedure expressly covers AI-related complaints.

The Solicitors Regulation Authority's principles require solicitors to maintain client confidentiality and to supervise staff and systems used in client matters. Unsanctioned AI use by fee earners is therefore a regulatory risk under both the SRA framework and data protection law simultaneously.

For EU-resident clients, the EU AI Act 2024/1689 imposes deployer obligations that have been enforceable since 2 August 2026 (Article 50 transparency duties and deployer obligations). Deployers are defined as any natural or legal person that puts an AI system into use. Halstead & Rowe is a deployer in respect of all three tools when used in client-facing work. Article 9 requires deployers of AI systems to implement a risk management system. No such system exists at present.

Required action: Halstead & Rowe must immediately appoint a named AI Governance Lead (recommended: the firm's COCP or a senior partner), adopt a written AI Acceptable Use Policy, establish an approved-tools register, and implement a process by which new AI tools are assessed and authorised before use. All three existing tools must be retrospectively assessed and formally approved or prohibited.

2. Lawfulness, Fairness, and the Bias Position

Halstead & Rowe processes personal data belonging to clients — including special category data in family and probate files — when fee earners input case information into ChatGPT, Microsoft Copilot, or Lexis+ AI. Each processing activity requires a lawful basis under UK GDPR Article 6 and, where special category data is involved, a condition under Article 9(2). The firm has not documented lawful bases for AI-assisted processing, meaning it cannot currently demonstrate lawfulness under Article 5(2).

For conveyancing files, the lawful basis is most plausibly performance of a contract (Article 6(1)(b)) or legitimate interests (Article 6(1)(f)). For family files containing health, domestic circumstances, or immigration data, special category conditions apply and processing on the basis of Article 9(2)(f) (legal claims) is the most defensible route, but this must be documented. For EU-resident clients, the EU GDPR position is materially the same; the substantive lawful basis conditions are equivalent, and Halstead & Rowe must satisfy both regimes simultaneously — there is no divergence here that requires the stricter obligation to be separately identified, as both require documented lawful bases.

Fairness requires that clients are not adversely affected by AI use in ways they would not reasonably expect. Where AI is used to draft correspondence or summarise case documents, there is a risk that model outputs contain errors, reflect training-data biases, or mischaracterise facts. In family proceedings, an AI-generated summary that omits or distorts a client's circumstances could cause material harm. The Pinsent Masons case (May 2026) illustrates that English courts expect human verification of AI outputs; failure to verify could constitute a breach of professional duty and, if personal data is involved, a breach of the accuracy principle under UK GDPR Article 5(1)(d).

Bias risk: ChatGPT and Microsoft Copilot are general-purpose models whose training data may reflect societal biases. When used to draft correspondence about clients, there is a plausible risk that outputs reflect demographic assumptions. Lexis+ AI is a purpose-built legal research tool with narrower scope; bias risk in the factual research context is lower, though hallucinated case citations remain a documented risk. The ICO's November 2024 audit of AI tools in recruitment identified bias in AI outputs as a primary concern and the same principle applies here.

Under the UK Equality Act 2010, Halstead & Rowe must not discriminate against clients or staff on the basis of protected characteristics. If AI outputs systematically produce worse quality advice or correspondence for clients with particular characteristics, this could constitute indirect discrimination. The firm must put in place a verification layer — human review of all AI-generated outputs before they are sent or acted upon — that mitigates this risk. This obligation arises under UK law only; the EU AI Act does not itself replicate the Equality Act, but EU GDPR Article 22 restrictions on automated decision-making provide overlapping protection for EU-resident clients.

3. Transparency and Explainability of Each System

The ICO AI Auditing Framework requires organisations to be transparent with individuals about how AI is used to process their data and to be able to explain AI-assisted decisions or outputs in meaningful terms.

ChatGPT (OpenAI): ChatGPT is a large language model that generates text by predicting token sequences based on training data and the prompt provided. Its outputs are not rule-based and cannot be audited step-by-step. When a fee earner pastes client information into ChatGPT and uses the output in a client letter, the client has no knowledge that their personal data has been processed by an OpenAI model. This is a transparency failure under UK GDPR Article 13/14 (information to be provided at collection) and under the fairness principle. OpenAI's ChatGPT is a general-purpose AI model; under the EU AI Act, general-purpose AI model obligations (including transparency obligations for providers) came into force on 2 August 2025. Halstead & Rowe as deployer must ensure its use of ChatGPT complies with Article 50 transparency duties, which have been enforceable from 2 August 2026.

Microsoft Copilot: Copilot is integrated into the Microsoft 365 environment and, depending on configuration, may process data within a tenant-controlled environment (Copilot for Microsoft 365 with data protection commitments) or via consumer-tier access with different data handling terms. Halstead & Rowe must confirm which tier is in use. If fee earners are using personal Microsoft accounts or consumer-tier Copilot, client data may be processed

outside the firm's data processing agreement and potentially outside the UK/EU. Copilot's explainability is comparable to ChatGPT — outputs are probabilistic and not auditable at the model level. The Microsoft AI terms include a data processing addendum for enterprise customers; the firm must ensure this is in place.

Lexis+ AI: Lexis+ AI is a purpose-built legal AI tool provided by LexisNexis under a subscription agreement that includes data processing terms. Its use for legal research and case summarisation carries lower confidentiality risk than general-purpose models if the tool is configured to operate on data within LexisNexis's controlled environment without training on client data. However, when case document content is uploaded or pasted, it still constitutes personal data processing. Explainability is constrained in the same way as other LLM-based tools — the tool cannot provide a full audit trail of how a summary was generated.

All three tools: Halstead & Rowe's privacy notice does not currently disclose AI use. Clients must be informed, at the point their data is collected or as soon as practicable, that AI tools may be used in the processing of their matter. This is required under UK GDPR Articles 13 and 14, and under EU GDPR for EU-resident clients. There is no divergence between UK and EU law on this transparency obligation — both regimes require it, and the obligation is satisfied once by updating the client care letter and privacy notice to include a clear AI disclosure, provided the disclosure meets both regimes' standards. Article 50(1) of the EU AI Act additionally requires deployers to ensure users are informed they are interacting with an AI system where this is not otherwise evident; this applies where clients receive AI-generated correspondence without disclosure.

4. Security and the AI-Specific Attack Surface

Halstead & Rowe holds conveyancing, family, and probate files. These contain some of the most sensitive personal data processed by any solicitors' firm: property ownership details, mortgage information, medical records, details of domestic abuse, mental capacity assessments, and death and estate information. Introducing AI tools into the processing chain creates AI-specific security risks that are additional to conventional cyber risks.

Prompt injection: All three tools are susceptible to prompt injection, whereby a malicious actor embeds instructions in a document that, when summarised by the AI, causes the model to behave in an unintended way or to exfiltrate information. Where fee earners paste content from third-party documents (such as opposing party correspondence or downloaded land registry entries) into ChatGPT or Copilot, this attack vector is live.

Data retention and model training: OpenAI's default settings for ChatGPT (free and Plus tiers) may use conversation data for model training unless the user has disabled this. If fee earners are using personal or non-enterprise ChatGPT accounts, client data may be retained by OpenAI and used in training, which would constitute a disclosure of personal data to a third party without a lawful basis or a valid data processing agreement — a breach of UK GDPR Article 28 and EU GDPR Article 28. Halstead & Rowe must confirm account types for all users and ensure only enterprise-tier accounts with training-off settings and a signed DPA are in use.

Microsoft Copilot (enterprise tier) is designed to operate within the tenant boundary and includes commitments that data is not used to train foundation models. This is a meaningful distinction, but the firm must verify its licensing and confirm the enterprise DPA is in place. Consumer-tier Copilot does not carry the same protections.

Lexis+ AI operates under LexisNexis's enterprise agreement; the firm should confirm with LexisNexis in writing that client data uploaded to the platform is not used for model training and that data is processed within UK/EU boundaries or under an adequate transfer mechanism.

Data transfer risk: ChatGPT processing may involve transfers to the United States. Under UK GDPR, such transfers require a valid transfer mechanism — either reliance on the UK adequacy regulations, an International Data Transfer Agreement (IDTA), or UK addendum to Standard Contractual Clauses. For EU-resident clients, EU GDPR Chapter V applies and Standard Contractual Clauses (2021) are required where data is transferred to OpenAI in the US. The firm must audit transfer mechanisms for each tool and ensure they are in place before any further use involving personal data.

ICO AI Auditing Framework requirement: The firm must document its AI-specific risk assessment, including data flows, storage locations, retention periods, and attack surface analysis, as part of a Data Protection Impact

Assessment under UK GDPR Article 35. A DPIA is mandatory here given the scale and sensitivity of data involved and the novel processing activity.

5. Individual Rights, Including Automated Decision-Making

Automated decision-making under UK GDPR Article 22 and EU GDPR Article 22 applies to decisions made solely by automated means that produce legal or similarly significant effects on individuals. Halstead & Rowe has confirmed that AI is not currently used to make decisions about people. This assessment accepts that confirmation, but notes three qualifications.

First, if AI-generated summaries or correspondence are relied upon without meaningful human review, the practical effect may approach automation bias — where the fee earner treats the AI output as authoritative without genuine independent assessment. This is not a technical Article 22 breach but it is a risk the firm must manage through its AI policy.

Second, the Data (Use and Access) Act 2025 (principal data protection provisions commenced 5 February 2026) amended the UK's automated decision-making framework to introduce wider lawful bases for solely automated decisions and associated safeguards. These provisions are now in force. Where the firm's future AI use evolves into automated decision-making, the DUAA framework will apply alongside UK GDPR Article 22.

Third, for EU-resident clients, EU GDPR Article 22 applies without modification by the DUAA. This is a divergence: the DUAA reforms apply only in the UK; for EU-resident clients the original EU GDPR Article 22 framework applies in full, including the right to object to solely automated decisions and the right to obtain human review. Where the two regimes diverge on this point, the EU GDPR Article 22 position (unreformed) is stricter in that it permits fewer exceptions without explicit consent or contractual necessity, and Halstead & Rowe must apply the EU standard to all processing involving EU-resident clients. Practically, since the firm does not use AI for decisions about people, Article 22 is not currently triggered — but this must be re-assessed if AI use expands.

Data subject rights: Clients have rights of access (UK GDPR Article 15 / EU GDPR Article 15), rectification (Article 16), erasure (Article 17), and portability (Article 20) in relation to personal data processed via AI. Halstead & Rowe must be able to identify what personal data has been processed through each AI tool, retrieve it, and action subject access requests within one calendar month. Currently the firm has no mechanism for this. The duty to operate a complaints procedure and respond to data protection complaints within set time limits commenced on 19 June 2026 under the DUAA; the firm must ensure its complaints process is operational and covers AI-related complaints.

EU AI Act individual rights (in force obligations): Article 50(1) of the EU AI Act, enforceable from 2 August 2026, requires deployers to inform individuals that AI is being used where this is not obvious. Halstead & Rowe must comply with this immediately for EU-resident clients.

6. Cross-Jurisdiction Position

This section identifies which compliance obligations under UK and EU law can be satisfied by a single measure and which must be met separately.

OBLIGATIONS SATISFIED ONCE FOR BOTH REGIMES:

Documented lawful basis for personal data processing: Both UK GDPR and EU GDPR require a lawful basis under Article 6 and a condition under Article 9(2) for special category data. The substantive conditions are equivalent. A single documented lawful basis analysis covering each AI use case satisfies both regimes, provided the document explicitly addresses both.

Privacy notice and client disclosure: Both UK GDPR Articles 13/14 and EU GDPR Articles 13/14 require disclosure of AI use. A single updated privacy notice and client care letter that meets the more detailed EU GDPR requirements (which are marginally more prescriptive on third-country transfers and automated decision-making) will satisfy both. The EU AI Act Article 50 transparency duty for EU-resident clients adds a deployer-level obligation

to notify individuals when interacting with AI; incorporating this into the client care letter satisfies both the GDPR transparency obligation and the AI Act deployer obligation simultaneously.

Data Processing Agreements with AI vendors: Both UK GDPR Article 28 and EU GDPR Article 28 require a written DPA with each processor. A single DPA with OpenAI, Microsoft, and LexisNexis covering both UK and EU data subjects satisfies both regimes, provided the DPA references both frameworks.

DPIA: UK GDPR Article 35 and EU GDPR Article 35 both require a DPIA for high-risk processing. A single DPIA document covering the three tools and all personal data processed satisfies both, provided it addresses both regimes explicitly.

AI policy and governance: A single internal AI Acceptable Use Policy satisfies both regimes' accountability requirements.

OBLIGATIONS THAT MUST BE MET SEPARATELY:

Automated decision-making safeguards: The DUAA 2025 (in force 5 February 2026) reformed UK GDPR Article 22 to provide wider lawful bases for automated decisions. EU GDPR Article 22 remains in its original unamended form for EU-resident clients. If Halstead & Rowe ever uses AI for automated decisions, the UK and EU positions diverge and separate compliance measures are required. The EU position is stricter; the firm must apply EU GDPR Article 22 in full to all EU-resident clients regardless of the DUAA reforms.

International data transfers: Transfers to the US via ChatGPT or other tools require an IDTA or UK SCCs addendum for UK data subjects and EU SCCs (2021) for EU data subjects. These are separate instruments and both must be in place.

EU AI Act deployer obligations: These are EU-specific obligations with no direct UK equivalent. Article 9 risk management, Article 13 transparency to users, and Article 50 notification duties apply only in respect of EU-resident clients (and EU-market use). The UK has no equivalent statutory deployer obligations at present; compliance is governed by the ICO's principles-based framework. Both sets of obligations must be met separately.

Complaints procedure: The DUAA duty (commenced 19 June 2026) is a UK-specific statutory obligation. EU GDPR's equivalent rights of complaint to supervisory authorities are separately framed; the firm must ensure its complaints process directs EU-resident clients to their competent EU supervisory authority as well as to the ICO.

7. Findings and Remediation Actions

Finding 1 — No AI governance policy exists.
Risk: Critical. Fee earners use three AI tools without authorisation, risk assessment, or oversight. This breaches UK GDPR Article 5(2) accountability, SRA Principles, and EU AI Act Article 9 deployer obligations.
Remediation: Appoint an AI Governance Lead immediately. Draft and adopt an AI Acceptable Use Policy within 30 days. Establish an approved-tools register and a formal approval process for any new AI tool. Communicate the policy to all fee earners with mandatory acknowledgement.
Owner: Managing Partner / designated AI Governance Lead.
Deadline: 30 days from date of this report.

Finding 2 — No lawful basis documented for AI-assisted personal data processing.
Risk: High. Without a documented lawful basis, processing is unlawful under UK GDPR Article 6 and EU GDPR Article 6.
Remediation: Conduct a lawful basis analysis for each AI use case (drafting correspondence, summarising case documents, research) across each practice area (conveyancing, family, probate). Document the analysis and retain it as part of the Records of Processing Activities under Article 30.
Owner: AI Governance Lead / Data Protection Officer or nominated lead.
Deadline: 45 days.

Finding 3 — Privacy notice and client care letter do not disclose AI use.
Risk: High. Failure to inform clients that AI tools process their personal data breaches UK GDPR Articles 13/14, EU GDPR Articles 13/14, and EU AI Act Article 50(1) (in force 2 August 2026).

Remediation: Update the firm's privacy notice and client care letter to include a clear, plain-English disclosure of AI tool use, naming the categories of tool, the purposes, and the data types processed. For EU-resident clients, include the Article 50 AI Act disclosure. Issue updated documentation to all current clients and use the new version for all new matters.
Owner: AI Governance Lead and Head of Client Services.
Deadline: 21 days.

Finding 4 — No Data Processing Agreements confirmed with AI vendors.
Risk: Critical. Processing personal data via ChatGPT, Copilot, or Lexis+ AI without a compliant DPA breaches UK GDPR Article 28 and EU GDPR Article 28.
Remediation: Confirm the account tier for each tool. For ChatGPT, move all users to OpenAI's enterprise tier and execute OpenAI's enterprise DPA. For Microsoft Copilot, confirm Microsoft 365 Copilot enterprise licensing is in place and the Microsoft DPA is executed. For Lexis+ AI, obtain written confirmation from LexisNexis of data processing terms, confirm no client data is used for model training, and confirm data residency within UK/EU. Retain signed copies of all DPAs.
Owner: AI Governance Lead and IT/Operations Lead.
Deadline: 21 days. No personal data should be processed via any tool until its DPA is confirmed.

Finding 5 — No international data transfer mechanism in place.
Risk: High. ChatGPT processing may involve transfers to the United States. Without an IDTA or UK SCCs addendum (UK data subjects) and EU SCCs 2021 (EU-resident clients), these transfers are unlawful.
Remediation: For UK data subjects, execute an IDTA or a UK addendum to SCCs with OpenAI covering the ChatGPT processing. For EU-resident clients, ensure EU SCCs 2021 are incorporated into the OpenAI enterprise agreement. Confirm Microsoft and LexisNexis data residency and transfer mechanisms in the same process as Finding 4. Document transfer impact assessments.
Owner: AI Governance Lead.
Deadline: 21 days, concurrent with Finding 4.

Finding 6 — No DPIA conducted for AI processing.
Risk: High. AI-assisted processing of special category personal data (family and probate files) using novel technology requires a DPIA under UK GDPR Article 35 and EU GDPR Article 35.
Remediation: Conduct a DPIA covering all three tools and all practice areas. The DPIA must include a data flow map, risk identification, risk mitigation measures, and a residual risk assessment. Where residual risks are high and cannot be mitigated, consult the ICO prior to processing (UK GDPR Article 36) and, for EU-resident client processing, the relevant EU supervisory authority.
Owner: AI Governance Lead and Data Protection lead.
Deadline: 60 days.

Finding 7 — No human verification process for AI outputs.
Risk: High. The Pinsent Masons case (May 2026) and Italian court rulings on AI hallucinations (2025-2026) confirm that courts and regulators expect human oversight. Unverified AI outputs in client correspondence or case summaries risk professional regulatory breaches and inaccurate personal data (UK GDPR Article 5(1)(d)).
Remediation: Adopt a mandatory verification rule in the AI policy: no AI-generated output may be sent to a client, filed in a matter, or used in court without review and sign-off by the responsible fee earner. Include this as a training requirement.
Owner: Practice Group Heads.
Deadline: 30 days.

Finding 8 — No EU AI Act Article 9 risk management system for deployer obligations.
Risk: Medium (escalating to High as the firm acts for EU-resident clients and Article 50 obligations are now enforceable). Article 9 requires deployers to implement a risk management system appropriate to the AI system's risk level and use case.
Remediation: Integrate an AI risk register into the firm's risk management framework. Log each AI tool, its risk classification under the EU AI Act, applicable obligations, and mitigation measures. Review quarterly.

Owner: AI Governance Lead.
Deadline: 60 days.

Finding 9 — No complaints procedure covering AI-related data protection complaints.
Risk: Medium. The DUAA duty to operate a complaints procedure and respond within set time limits commenced 19 June 2026. The firm has no procedure confirmed.
Remediation: Adopt or update the firm's data protection complaints procedure to expressly cover AI-related complaints. Ensure EU-resident clients are directed to their competent EU supervisory authority. Publish a contact route on the firm's website.
Owner: Data Protection Lead / Compliance Manager.
Deadline: 14 days.

8. Overall Maturity Rating

Overall maturity rating: INITIAL (Level 1 of 5).

Basis for rating: The ICO AI Auditing Framework assesses maturity across five domains — governance, lawfulness and fairness, transparency, security, and individual rights. At Level 1 (Initial), AI use is ad hoc, undocumented, and ungoverned. Halstead & Rowe presents all the hallmarks of this level: three AI tools in active use with no policy, no DPAs confirmed, no client disclosure, no DPIA, no lawful basis analysis, and no human verification protocol.

The firm is not at Level 2 (Repeatable) because there are no defined processes, even informal ones, that are applied consistently. The firm is not at Level 3 (Defined) because there is no documented AI framework of any kind. Levels 4 and 5 (Managed and Optimising) require quantitative measurement and continuous improvement, which are entirely absent.

Mitigating factors: Halstead & Rowe's AI use is in scope of the lower-risk categories of the EU AI Act — the tools are not Annex III high-risk systems as currently deployed (legal AI research tools and correspondence drafting are not listed in Annex III, and the high-risk Annex III obligations do not take effect until 2 December 2027 in any event following the Digital Omnibus deferral of 29 June 2026). The firm has confirmed it does not use AI for decisions about people, which removes the Article 22 compliance obligation from the immediate critical path. Lexis+ AI is purpose-built for legal use, which reduces, though does not eliminate, the risk of hallucinated outputs in the research context.

Aggravating factors: The processing of special category personal data in family and probate files, the presence of EU-resident clients triggering both UK and EU obligations, the absence of any DPAs with AI vendors, and the confirmed absence of any policy or governance structure place the firm at material regulatory risk. The ICO's maximum fine for a serious breach is £17.5 million or 4% of global annual turnover (whichever is higher); the turnover-based limb cannot be computed without the firm's financial figures. Under the EU AI Act, fines for breach of deployer transparency obligations can reach €15 million or 3% of worldwide annual turnover. The Solicitors Regulation Authority operates its own sanctioning regime in parallel.

Path to Level 3 (target within 90 days): Full implementation of all nine findings above, completion of the DPIA, execution of DPAs with all three vendors, publication of the updated privacy notice, and adoption of the AI Acceptable Use Policy will move the firm to Level 3. Level 4 should be targeted within 12 months through introduction of periodic AI audits, staff training records, and a documented review cycle. This assessment should be repeated annually or within 30 days of any material change to AI tool use.

Employment AI Procedures

Using AI in recruitment, monitoring or management decisions — the highest-risk use in most businesses, and the most regulated.

1. Purpose and Scope

This document sets out Halstead & Rowe Solicitors' binding procedures for the use of artificial intelligence tools in any context touching employment, recruitment, staff monitoring, or management decisions. It applies to all partners, fee earners, paralegals, and support staff across the firm's UK operations and, where the firm acts for or employs EU-resident individuals, across the EU regulatory perimeter.

The firm's three declared AI tools — ChatGPT (OpenAI), Microsoft Copilot, and Lexis+ AI — are the only AI tools approved for use at Halstead & Rowe. No other AI tool may be used in any employment-related context. This restriction responds directly to the firm's identified concern that fee earners have already begun using AI tools on their own initiative without an approved policy in place.

This document must be read alongside the firm's broader UK and EU Combined Compliance Framework. Where this document is silent, that Framework governs.

2. Employment Uses of AI at Halstead & Rowe — Declared Position

As at 8 August 2026, Halstead & Rowe has not formally adopted AI tools for recruitment, candidate screening, staff performance monitoring, disciplinary processes, or automated management decisions. The firm has confirmed that AI is not used to make decisions about people. This position is accepted and recorded here.

However, because fee earners are known to have begun using approved tools — particularly ChatGPT and Microsoft Copilot — without direction, the risk that those tools are being used informally in employment-adjacent tasks (for example, drafting job advertisements, summarising CVs, or preparing performance-review notes) is real and must be managed. This document therefore applies both to any formally adopted employment use and to any informal or unsanctioned use that may already be occurring.

For completeness: Lexis+ AI is approved for legal research and case analysis only. Its use in any employment or HR process is not approved and is prohibited unless the firm formally extends its scope under a revised policy.

3. Discrimination Risk and Indirect Discrimination

The use of AI tools in any employment-related task — including drafting job advertisements, summarising application materials, or generating interview questions — creates a risk of direct and indirect discrimination. Indirect discrimination arises where an AI tool applies a criterion or practice that appears neutral but places candidates or staff with a protected characteristic at a particular disadvantage, contrary to the UK Equality Act 2010 (sections 19 and 39). Protected characteristics include age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, and sexual orientation.

Large language models such as ChatGPT and Microsoft Copilot are trained on data that may encode historical workforce patterns. If those patterns reflect past under-representation of particular groups in legal roles, the model may replicate that bias in, for example, language choices in job advertisements, ranking criteria embedded in a prompt, or summary language used when reviewing CVs. This is an indirect discrimination risk even where no discriminatory intent exists.

Halstead & Rowe must apply the following testing controls. First, any AI-generated job advertisement or role description must be reviewed by a fee earner or manager with delegated HR responsibility before publication, using the firm's equality checklist. Second, where AI tools are used to draft interview questions, those questions

must be reviewed for neutrality and checked against the Equality Act 2010 protected characteristics before use. Third, if the firm ever formally adopts AI for CV screening or shortlisting, a bias audit must be conducted before deployment, using a representative test dataset, and the results documented. The ICO AI Auditing Framework (published by the Information Commissioner's Office) sets out the methodology the firm must follow for that audit, including testing across demographic sub-groups.

Under EU law, Article 13 of the EU AI Act 2024/1689 (in force for deployer obligations from 2 August 2026) requires that AI systems used by deployers be sufficiently transparent for users to interpret outputs. Where AI-generated content is used in any employment decision affecting an EU-resident employee or applicant, the responsible manager must be able to explain what the AI produced and why the firm relied on it — this is the minimum standard of human interpretability required before any employment action is taken.

4. Reasonable Adjustments and Accessibility

The UK Equality Act 2010 (section 20) places a duty on Halstead & Rowe to make reasonable adjustments where a provision, criterion, or practice — including any AI-assisted process — places a disabled person at a substantial disadvantage compared with persons who are not disabled.

If AI tools are used at any stage of a recruitment or performance process, the firm must ensure that the process as a whole remains accessible. Concretely: AI-generated application forms or interview invitations must be available in accessible formats on request. If an AI tool is used to summarise or score a candidate's application, a candidate who has disclosed a disability must be given the opportunity to provide supplementary information that the tool may not have captured or weighted appropriately — for example, gaps in employment history arising from a disability-related absence.

No AI-generated output may be the sole basis for deciding that a reasonable adjustment request is unnecessary or disproportionate. That decision requires human judgement by a manager with delegated authority, informed by occupational health advice where appropriate.

For EU-resident staff or applicants, the same standard applies by virtue of the EU AI Act's requirement (Article 9, risk management obligations — applicable to high-risk systems from 2 December 2027, but adopted here as a matter of good practice now) that AI systems be designed and used in a way that avoids adverse impacts on protected groups. The firm adopts this standard voluntarily for all employment uses regardless of the formal commencement timetable.

5. What Candidates and Staff Are Told, and When

Transparency is a dual obligation under UK and EU law.

Under the UK GDPR (Article 13 and Article 14, as retained in UK law and as supplemented by the Data (Use and Access) Act 2025), individuals whose personal data are processed must be told the purposes and legal basis for that processing at the point of collection. Where AI tools process personal data — including CVs, performance reviews, or correspondence about a staff member — this must be disclosed. The firm's privacy notice for employees and candidates must be updated to state that ChatGPT, Microsoft Copilot, and Lexis+ AI may be used to process personal data in the course of HR administration, and to explain the legal basis (legitimate interests for internal HR administration, with a legitimate interests assessment on file).

Under EU AI Act Article 50 (in force from 2 August 2026), deployers of AI systems that interact directly with natural persons — including, for example, a Copilot-drafted message sent to a candidate — must inform the recipient that they are interacting with or receiving content generated by an AI system. This obligation applies now. Any AI-drafted recruitment communication sent by the firm must carry a brief, plain-language disclosure: for example, "This message was drafted with AI assistance and reviewed by [name]." This obligation applies whether the recipient is UK- or EU-based.

The obligation under UK law to inform individuals about automated decision-making (UK GDPR Article 22) applies where a decision based solely on automated processing produces legal or similarly significant effects. The firm has confirmed it does not use AI for decisions about people in this sense. That position must be maintained and reviewed each time a new AI use is proposed. If it changes, Article 22 safeguards (the right to human review, to express a point of view, and to contest the decision) must be implemented before the new use commences.

Under the Data (Use and Access) Act 2025 (Part 5, in force 5 February 2026), wider lawful bases for solely automated decisions are now available in UK law, but each carries mandatory safeguards. The firm does not currently rely on those bases and must not do so without a formal policy amendment and updated privacy notices.

The firm must also operate a complaints procedure for data protection complaints and respond within the statutory time limits imposed by the Data (Use and Access) Act 2025, duty in force from 19 June 2026. HR-related data complaints received from staff or candidates must be logged and responded to within that procedure.

6. Human Review of Decisions Affecting a Person

Halstead & Rowe's confirmed position is that AI does not make decisions about people. This section records what human review must look like if AI tools are used in any preparatory step that feeds into such a decision.

Where ChatGPT or Microsoft Copilot is used to draft a rejection letter, a disciplinary note, a performance summary, or any other document that will be used in a decision affecting a member of staff or a candidate, a named manager must review and approve the final document before it is sent or placed on file. The manager's review must be substantive — the manager must read the document, satisfy themselves it is accurate and fair, and record that they have done so. Counter-signing an AI draft without reading it does not constitute human review for these purposes and may expose the firm to an Equality Act 2010 claim if the draft contains discriminatory content.

For EU-resident individuals, Article 13 of the EU AI Act 2024/1689 (deployer transparency obligations, in force 2 August 2026) reinforces this: where an AI system's output is used in a context with legal or similarly significant effects on a person, the deployer — here, Halstead & Rowe — must ensure the output is interpretable and that a human has verified it before it is acted upon. This is consistent with the doctrine established by Italian courts between March 2025 and March 2026 on algorithmic hallucinations, which has established that professional diligence requires human oversight to counter automation bias. The same professional standard is expected of UK solicitors following the Pinsent Masons criticism in May 2026.

No disciplinary warning, performance improvement plan, redundancy selection outcome, or recruitment rejection may be issued without a named senior manager or partner sign-off, documented on the relevant file, regardless of whether AI was used in preparing the underlying materials.

7. Records: What Is Kept and for How Long

The firm must maintain records sufficient to defend a challenge under the Equality Act 2010, the UK GDPR, the EU AI Act, and the Solicitors Regulation Authority's Code of Conduct. The following records must be kept in the firm's HR file system.

First, for each recruitment exercise: the job advertisement as published (including any AI-generated version and the final approved version); the names of any AI tools used; the name of the reviewing manager; the equality checklist completed at review; and, if a bias audit was conducted, the audit report. Retention period: six years from the date the role was filled or the exercise was abandoned, to cover the limitation period for employment claims.

Second, for each instance where AI tools process personal data about a candidate or staff member: a log entry recording the tool used, the category of data processed, the purpose, the legal basis, and the name of the person who approved the processing. Retention period: the duration of the individual's employment or candidacy, plus six years.

Third, for each AI-assisted document used in a decision about a person (performance review, disciplinary note, rejection letter): the original AI draft (where recoverable), the final approved version, and the name of the manager

who approved it. Retention period: six years from the date of the decision.

Fourth, data protection complaints received under the Data (Use and Access) Act 2025 complaints procedure: all correspondence, the date received, the response date, and the outcome. Retention period: three years from closure of the complaint.

Under EU AI Act Article 9 (risk management — adopted by the firm as good practice ahead of the December 2027 deadline for Annex III high-risk systems), records of risk assessments carried out in relation to AI use in employment must also be retained for ten years from the date of the assessment, to the extent that the firm's employment uses come within scope of those requirements when they become mandatory.

All records must be stored in the firm's secure case management or HR system and must not be held solely in a personal email account or on an AI provider's servers.

8. Cross-Jurisdiction Position: Employment AI

Certain obligations in this document are satisfied once and apply to both UK and EU regulatory perimeters. Others must be met separately.

Satisfied once for both: The human review requirement (section 6) satisfies both UK GDPR Article 22 safeguards and EU AI Act Article 13 deployer obligations. Maintaining records of AI use (section 7) satisfies both ICO AI Auditing Framework record-keeping expectations and EU AI Act Article 9 risk management documentation requirements. The bias-testing and equality review requirement (section 3) satisfies both the UK Equality Act 2010 and the EU AI Act's requirement that deployers avoid adverse impacts on protected groups.

Must be met separately: Transparency disclosures in candidate and staff communications must comply with UK GDPR Article 13/14 (UK-resident individuals) and EU AI Act Article 50 (EU-resident individuals). The EU obligation under Article 50 to disclose AI interaction is narrower in its trigger but more prescriptive in form than the UK GDPR notice requirement; where the two diverge, the firm applies the stricter obligation — that is, the Article 50 disclosure is given to all recipients of AI-generated communications regardless of residence. Data protection complaints under the Data (Use and Access) Act 2025 (complaints procedure, in force 19 June 2026) apply to UK data subjects only; EU data subjects' complaints are handled under the EU GDPR complaints and supervisory authority referral mechanism separately. Automated decision-making safeguards under UK GDPR Article 22 and the Data (Use and Access) Act 2025 (Part 5, in force 5 February 2026) are UK-specific; equivalent EU obligations arise under EU GDPR Article 22 and, for high-risk AI, under EU AI Act Annex III (mandatory from 2 December 2027). Where the firm's AI uses do not currently constitute solely automated decision-making, both regimes are satisfied simultaneously by the firm's existing human-review policy.

Divergence note: The EU AI Act imposes fines of up to €35 million or 7% of global annual turnover for prohibited practices. For transparency violations under Article 50, fines of up to €15 million or 3% of global annual turnover apply. The UK ICO maximum under UK GDPR is £17.5 million or 4% of global annual turnover. The turnover-based limb cannot be computed without the firm's financial figures. In all cases the firm should treat the higher statutory maximum as the operative risk figure when assessing the severity of non-compliance.

9. Prohibited Uses and Approval Process

The following uses of any AI tool in an employment context are prohibited at Halstead & Rowe without explicit written approval from the managing partner: automated or AI-assisted shortlisting or scoring of candidates without human review; use of any AI tool not on the firm's approved list (ChatGPT, Microsoft Copilot, Lexis+ AI) for any HR or employment task; inputting a named individual's personal data into any AI tool for any purpose other than those listed in the firm's data processing register; and using AI to generate or inform a disciplinary or grievance outcome document without substantive manager review.

Any fee earner or member of staff who wishes to use an AI tool in a new employment-related context must submit a written request to the managing partner before doing so. The request must identify the tool, the data involved, the

purpose, and the proposed human oversight mechanism. The managing partner must respond within five working days. Approved uses are added to the firm's AI use register and this policy is updated accordingly.

This approval requirement is the firm's direct response to the identified risk that staff have already begun using AI tools without a policy in place. Retrospective approval is not available; past unsanctioned use must be disclosed to the managing partner by 30 September 2026 so that a data protection impact assessment can be carried out where required.

10. Review and Ownership

This document is owned by the managing partner of Halstead & Rowe Solicitors. It must be reviewed in full no later than 1 December 2026 to account for the commencement of new EU AI Act prohibitions and Article 50(2) synthetic content marking obligations on 2 December 2026. It must also be reviewed following any material change to the firm's AI tools, employment practices, or the applicable regulatory framework.

All staff must confirm in writing that they have read and understood this document within 21 days of its issue. Confirmed receipt must be recorded on each individual's personnel file. This document takes effect on 8 August 2026.

Automated Decision-Making Notices and Opt-Out Procedures

The notices you give when a decision is made by a machine, and the route out that the law requires you to offer.

1. Scope and Purpose

This document sets out the automated decision-making notices that Halstead & Rowe Solicitors ('the Firm') is required to give to data subjects, together with the opt-out and human-review procedures that UK GDPR and the Data (Use and Access) Act 2025 ('DUAA') require. It also records the firm's position under EU AI Act 2024/1689 Article 50 transparency duties, which came into force on 2 August 2026 and apply because the Firm acts for EU-resident clients.

This document forms part of the Firm's AI compliance pack dated 8 August 2026. It covers the three AI tools in current use — ChatGPT (OpenAI), Microsoft Copilot, and Lexis+ AI — deployed for drafting client correspondence, summarising case documents, and legal research across conveyancing, family, and probate matters.

2. Which Decisions at Halstead & Rowe Are Automated or Significantly Automated

The Firm has confirmed that it does not currently use AI to make decisions about people in the sense of producing legal effects or similarly significant effects without human involvement. Fee earners use ChatGPT, Microsoft Copilot, and Lexis+ AI to generate drafts, produce summaries, and conduct research, but a qualified fee earner reviews every output before it is relied upon or communicated. On the evidence presently available, this pattern of use does not constitute 'solely automated decision-making' within the meaning of UK GDPR Article 22 or the expanded automated-decision provisions of the DUAA, because a human applies professional judgement before the AI output has any effect on a client or third party.

Nevertheless, the Firm recognises two categories where automation is sufficiently significant to warrant notice and procedure. First, AI-assisted document triage: where Lexis+ AI or Copilot ranks, filters, or flags case documents or legal authorities before a fee earner reviews them, the selection and de-selection of material may influence the scope of information a client receives. Second, AI-assisted correspondence drafting: where ChatGPT or Copilot produces a near-final letter that a fee earner approves with minimal alteration, the substantive content reaching the client originates substantially from an AI system. These are treated as 'significantly automated' processes for the purpose of this document, and notices are issued accordingly. Fully automated decisions producing legal effects without human review are prohibited at the Firm and must not be introduced without a further policy amendment and data protection impact assessment.

3. Legal Basis: UK Regime

UK GDPR Article 22 gives data subjects the right not to be subject to a decision based solely on automated processing that produces a legal or similarly significant effect. The DUAA Part 5 provisions, in force from 5 February 2026, widen the lawful bases on which solely automated decisions may be taken and introduce accompanying safeguards, including the duty to inform data subjects and to offer a meaningful route to human review. The DUAA duty on controllers to operate a complaints procedure and respond to data protection complaints within set time limits came into force on 19 June 2026. The Firm must comply with both provisions now.

The ICO AI Auditing Framework reinforces that even where processing does not meet the Article 22 threshold, transparency about AI involvement is an element of the accountability principle under UK GDPR Article 5(1)(a). The UK Equality Act 2010 is relevant because AI outputs may embed or replicate bias; any human reviewer must be instructed to consider whether a draft or recommendation disadvantages a client on grounds of a protected characteristic before it is adopted.

Maximum penalties under the UK regime are £17.5 million or 4% of global annual turnover, whichever is higher. The turnover-based limb cannot be computed without the Firm's figures.

4. Legal Basis: EU Regime

The Firm acts for EU-resident clients, bringing it within the territorial scope of EU AI Act 2024/1689. Article 50 transparency duties are in force from 2 August 2026. Article 50(1) requires deployers of AI systems that interact with natural persons to inform those persons that they are interacting with an AI system. Article 13 (transparency and provision of information) and Article 9 (risk management) apply to high-risk systems under Annex III; however, following the Digital Omnibus adopted on 29 June 2026, the compliance deadline for Annex III high-risk systems has been deferred to 2 December 2027. The Firm should keep Annex III applicability under review as its AI use evolves, but the immediate obligation is Article 50.

Article 5 prohibited practices are not engaged by the Firm's current use cases. GPAI rules (obligations for providers of general-purpose AI models) came into force on 2 August 2025; these bind OpenAI and Microsoft as providers, not the Firm as deployer, though the Firm should verify that each provider has published the required transparency information. EU GDPR (Regulation 2016/679) continues to apply to personal data of EU-resident clients, including its Article 22 right against solely automated decisions. Maximum penalties under the EU AI Act are €35 million or 7% of global annual turnover; that turnover-based limb cannot be computed without the Firm's figures.

5. Cross-Jurisdiction Position

Several obligations are satisfied by a single action covering both regimes. A single client notice that discloses AI involvement in processing, names the tools used, and offers a route to human review satisfies the transparency requirement under both UK GDPR Article 13/14 and EU AI Act Article 50(1). A single record of human-review outcomes satisfies the accountability principle under both UK and EU GDPR. A single data protection impact assessment covering AI tools satisfies the UK ICO's expectation and provides the evidentiary base for EU risk management under Article 9.

Obligations that must be met separately are as follows. The EU AI Act Article 50 duty to inform users they are interacting with an AI system applies specifically to EU-resident clients and must be tracked separately for those clients; UK-only clients are covered by UK GDPR transparency obligations, which do not include an equivalent prescriptive disclosure in those terms but are treated as equally requiring it under the accountability principle, so the Firm applies the EU standard to all clients as the stricter obligation. Where the two regimes diverge on automated decision-making safeguards, the Firm applies the stricter obligation: where UK DUAA permits a wider lawful basis for automated decisions with safeguards, and EU GDPR Article 22 requires explicit consent or contractual necessity plus additional measures, the Firm applies the EU GDPR standard to all processing involving EU-resident clients. Complaints-procedure timelines under the DUAA (in force 19 June 2026) are a UK-specific obligation with no exact EU equivalent; the Firm maintains a single complaints procedure that meets the DUAA timelines and is offered to all clients.

6. Ready-to-Use Notices

NOTICE A — AI-ASSISTED CORRESPONDENCE (for use at the foot of any letter or email substantially drafted using ChatGPT or Microsoft Copilot)

'This communication was prepared with the assistance of an AI drafting tool. The content has been reviewed and approved by the fee earner named above before sending. If you would prefer that any response or further communication from us is prepared without the use of AI tools, please inform us using the contact details below and we will arrange this.'

NOTICE B — AI-ASSISTED DOCUMENT SUMMARY (for use when providing a client with a summary of documents produced using Lexis+ AI or Copilot)

'The summary provided to you was produced with the assistance of an AI tool and has been reviewed by the fee earner named in this matter. The original documents remain available to you on request. If you have any concern about the accuracy or completeness of this summary, or if you wish the summary to be prepared without AI assistance, please contact your fee earner directly.'

NOTICE C — AI SYSTEM INTERACTION DISCLOSURE (EU clients — Article 50 EU AI Act, in force 2 August 2026; also applied to all clients as the stricter standard)

'Halstead & Rowe Solicitors uses AI systems, including ChatGPT (OpenAI), Microsoft Copilot, and Lexis+ AI, in the preparation of correspondence, document summaries, and legal research. These tools process information about your matter. A qualified solicitor or legal executive reviews all AI-generated material before it is used. You have the right to request that a specific piece of work is carried out without AI assistance. To exercise this right, please contact your fee earner or the Firm's Data Protection Lead at [DPL name and email].'

All three notices are approved for immediate use. Fee earners must not alter their wording without sign-off from the Data Protection Lead.

7. How the Opt-Out or Human-Review Request Is Made and Routed

A client or data subject wishing to opt out of AI-assisted processing, or to request human review of a specific output, may do so by any of the following routes: (a) writing to the fee earner with conduct of the matter; (b) writing to the Firm's Data Protection Lead at the address or email address stated in the client care letter; or (c) calling the main office number and asking for the Data Protection Lead. The request does not need to use any particular form of words. Any communication from a client expressing concern about AI use, querying how a document was produced, or asking for personal involvement of a human must be treated as a human-review request and routed accordingly.

On receipt, the fee earner or support staff member who receives the request must log it in the matter file and notify the Data Protection Lead by email on the same working day, copying in the supervising partner for the matter. The Data Protection Lead records the request in the Firm's central AI Requests Register (see Section 9 below). No AI-generated output that is the subject of an opt-out request may be sent to or relied upon by the client until the human review has been completed and the client has been informed.

8. Deadline for Responding and Who Responds

The Firm will acknowledge every human-review request within two working days of receipt. Acknowledgement must confirm that the request has been received, identify the fee earner and supervising partner responsible for the review, and give a target date for completion.

The substantive human review — meaning the preparation of the relevant output (letter, summary, or research note) without AI involvement, or a fresh human review and rewrite of the AI output — must be completed and provided to the client within ten working days of the date of acknowledgement, unless the complexity of the matter makes this impracticable, in which case the fee earner must write to the client within that period explaining the revised timetable and the reason for it. This deadline also satisfies the DUAA complaints-response obligation in force from 19 June 2026.

The fee earner with conduct of the matter carries out the human review. The supervising partner is responsible for quality-assuring the outcome before it is sent. The Data Protection Lead is notified of completion. Where the request relates to a complaint about AI accuracy or data processing, the Data Protection Lead takes the lead on the response, and the ten-working-day clock applies.

9. How the Outcome of a Human Review Is Recorded

The Firm maintains a central AI Requests Register, held by the Data Protection Lead. Each entry must contain: (1) the date the request was received and by whom; (2) the client name (or matter reference where confidentiality requires) and matter type; (3) the AI tool whose output is under review; (4) the nature of the output — correspondence, summary, or research; (5) the fee earner and supervising partner assigned; (6) the date of acknowledgement to the client; (7) the date the human review was completed; (8) a brief description of the outcome — whether the original AI-assisted output was adopted without change, amended, or replaced entirely; and (9) confirmation that the outcome was communicated to the client.

A copy of the final human-reviewed output must be saved to the matter file in the Firm's practice management system with a file note recording that it was the product of a human review requested by the client. This record satisfies the accountability requirement under UK GDPR Article 5(2) and supports the Firm's ability to demonstrate compliance to the ICO or, in relation to EU-resident clients, to a relevant national supervisory authority. Records must be retained in line with the Firm's document retention schedule, with a minimum period of six years for conveyancing and probate matters and seven years for family matters, unless a longer period is required by the retainer or applicable professional rules.

10. Where the Notice Appears and Proof It Was Given

Notice A must appear at the foot of every letter or email substantially drafted with ChatGPT or Copilot. 'Substantially' means the AI produced a draft that was sent with fewer than one-third of its words altered by the fee earner. Fee earners must apply this test honestly; uncertainty should resolve in favour of including the notice. The notice forms part of the body of the document, not a separate attachment, so that it is transmitted with and inseparable from the communication. Proof of delivery is the sent-item record in the Firm's email system or the posting record in the case of hard copy.

Notice B must be included on the covering page of any document summary delivered to a client where Lexis+ AI or Copilot produced the summary. It must appear in the same font and size as the body of the covering page. Where the summary is delivered by email, Notice B must appear in the email body, not only in the attachment.

Notice C must appear in the Firm's client care letter for every new retainer opened from 8 August 2026 onwards, and must be sent as a standalone notice to all existing clients within 30 days of this document being adopted. Proof of issue to existing clients must be retained — either a copy of the email with send confirmation or a record of the letter on the matter file. From 8 August 2026, the client care letter template is amended to include Notice C in a clearly headed section entitled 'Use of Artificial Intelligence'. Clients must be asked to acknowledge receipt; where acknowledgement is not received within 14 days, the fee earner must follow up once by email or telephone and record the outcome.

All three notices and the delivery evidence are reviewed by the Data Protection Lead on a quarterly basis to confirm continued compliance as the Firm's AI tool use and the regulatory environment develop.

Data Subject Rights Procedures for AI-Processed Data

How you answer an access, correction or deletion request when the data has passed through an AI system.

1. Document Scope and Legal Basis

This procedure governs how Halstead & Rowe Solicitors ('the firm') handles data subject rights requests where personal data has been processed through or inputted into an AI tool — specifically ChatGPT (OpenAI), Microsoft Copilot, or Lexis+ AI. It applies to data held on conveyancing, family, and probate files, and to data relating to EU-resident clients as well as UK-resident clients.

The firm processes personal data through AI tools and therefore engages obligations under UK GDPR (as retained and amended under the UK GDPR and the Data Protection Act 2018), the Data (Use and Access) Act 2025 (most Part 5 provisions in force from 5 February 2026, complaints-procedure duty in force from 19 June 2026), and — where data subjects are EU residents or where output is directed to EU territory — EU GDPR (Regulation 2016/679) and the EU AI Act (Regulation 2024/1689). Where obligations under UK and EU law diverge, the stricter obligation is stated and applied. Article 50 transparency obligations under the EU AI Act came into force on 2 August 2026 and apply now.

This document may be provided to the ICO, EU supervisory authorities, the firm's professional indemnity insurers, or to a data subject's legal representative.

2. Rights Covered, Statutory Deadlines, and Internal Owners

The firm recognises the following rights for data processed through AI tools, with the deadlines and owners set out below. All deadlines run from the day the firm receives a valid, sufficiently identified request.

Right of Access (Subject Access Request — SAR). Under UK GDPR Article 15 and EU GDPR Article 15, the firm must respond within one calendar month, extendable by two further months where requests are complex or numerous (the firm must notify the data subject of the extension within the first month). Internal owner: the Compliance Partner, supported by the fee earner who used the AI tool on the matter in question.

Right to Rectification. Under UK GDPR Article 16 and EU GDPR Article 16, inaccurate personal data must be corrected within one calendar month (extendable as above). Where AI-summarised content contains a factual error about the data subject, this right applies to the source record and to any downstream document derived from the AI output. Internal owner: the supervising fee earner, escalated to the Compliance Partner for AI-derived inaccuracies.

Right to Erasure ('Right to be Forgotten'). Under UK GDPR Article 17 and EU GDPR Article 17, erasure must be actioned within one calendar month where a valid ground exists. The AI-specific complications for this right are addressed separately in Section 6. Internal owner: Compliance Partner in all AI-related erasure requests, given the vendor-retention risks.

Right to Restriction. Under UK GDPR Article 18 and EU GDPR Article 18, processing must be restricted within one calendar month pending resolution of an accuracy dispute or an objection. During restriction, personal data may be stored but not actively processed through any AI tool. Internal owner: the Compliance Partner, who must notify each relevant system administrator.

Right to Object. Under UK GDPR Article 21 and EU GDPR Article 21, the firm must stop processing upon receipt of a valid objection unless it can demonstrate compelling legitimate grounds. In the context of AI tools, this includes the right to object to profiling. Where the firm relies on legal obligation or legal claims as the basis for continued processing, the Compliance Partner records this in writing within the response period. Internal owner: Compliance Partner.

Right Not to Be Subject to Solely Automated Decision-Making. Under UK GDPR Article 22 and EU GDPR Article 22, individuals have the right not to be subject to a decision based solely on automated processing that produces a legal or similarly significant effect. The Data (Use and Access) Act 2025 (in force 5 February 2026) introduces wider lawful bases for such decisions and the safeguards that accompany them under UK law. The firm's current declared position is that AI is not used for decisions about people; if this changes, this section must be re-reviewed before deployment. For the avoidance of doubt, the firm does not disapply Article 22 on the basis of its current practice — it records the position and reviews it whenever a new AI use case is adopted. Internal owner: Compliance Partner.

Complaints Procedure (DUAA duty). From 19 June 2026, the Data (Use and Access) Act 2025 requires the firm to operate a complaints procedure and respond to data protection complaints within set time limits. Any complaint arising from an AI-processed data request is logged under that procedure and acknowledged within five working days, with a substantive response within one calendar month.

3. Locating Personal Data Held Inside or by an AI Vendor

When the firm receives a SAR or erasure request concerning a data subject whose data may have been inputted into ChatGPT, Microsoft Copilot, or Lexis+ AI, the Compliance Partner must conduct a structured data-mapping exercise specific to AI-held data before the response is issued.

For each tool, the following steps apply. First, the fee earner who used the tool is asked to identify the relevant matter, the approximate dates of AI use, and the nature of the personal data inputted (for example, client names and addresses in a conveyancing instruction, or medical records in a family matter). Second, the Compliance Partner reviews the firm's records — matter management system, email, and any AI session logs — to reconstruct what was submitted.

Third, the firm checks the data-processing terms and privacy documentation for each vendor. Microsoft Copilot, where deployed under a Microsoft 365 commercial licence, does not use customer data to train its underlying models by default, and tenant administrators can confirm this in the Microsoft admin centre. The Compliance Partner must verify the firm's current licence tier and configuration. OpenAI's ChatGPT Enterprise (or API) terms provide that inputs are not used for training; however, if any fee earner has been using a personal or free ChatGPT account without firm approval — a risk explicitly flagged in the firm's declared concerns — the standard consumer terms may apply and retention or training use cannot be excluded. Lexis+ AI is a legal-specific product whose data terms should be reviewed against the firm's current subscription agreement.

The firm cannot guarantee that it can extract or enumerate personal data held in vendor inference logs. Where the vendor's terms confirm no retention beyond the session, this is stated in the SAR response. Where retention cannot be ruled out, the firm discloses this to the data subject, explains the steps taken to seek deletion from the vendor (see Section 6), and records the limitation in the request log.

For EU-resident data subjects, the firm notes that EU GDPR Article 28 requires a data-processing agreement with each vendor acting as a processor. The Compliance Partner must confirm that such agreements are in place for all three tools before responding to a SAR from an EU resident. Where a DPA is absent, this is a separate compliance failure that must be escalated immediately.

4. Explaining an Automated Decision in Terms a Person Understands

The firm's declared position is that AI tools are used for drafting correspondence, summarising case documents, and research — not for making decisions about people. Accordingly, UK GDPR Article 22 and EU GDPR Article 22 do not presently apply to any live use case. This position is recorded and reviewed each time a new AI use case is considered.

However, if a data subject asks the firm to explain how AI was used in processing their data — even where the AI did not produce a decision — the firm provides a plain-English explanation as a matter of good practice and to satisfy transparency obligations under UK GDPR Article 13/14 and EU AI Act Article 50 (in force 2 August 2026).

The explanation must cover: which tool was used; what type of data was inputted; what the AI produced (for example, a summary of medical evidence in a family file, or a draft letter in a conveyancing matter); and what human review took place before the output was used or sent.

Where, in future, the firm uses AI in a way that does produce a decision with legal or similarly significant effect on a data subject, the following applies. Under UK GDPR Article 22(3) and EU GDPR Article 22(3), the firm must provide meaningful information about the logic involved, the significance, and the envisaged consequences. This explanation must be written in plain English without technical jargon about model architecture. The explanation must specify: the inputs the system used (the categories of personal data); the general logic applied (for example, document classification, risk scoring); the output and how it was used; and who reviewed it. The Compliance Partner drafts this explanation with input from the fee earner and, where necessary, the relevant technology provider.

Under EU AI Act Article 13 (transparency and provision of information), deployers of AI systems must ensure that natural persons can understand the AI's capabilities and limitations. This obligation applies to the firm as a deployer as of 2 August 2026.

5. Right to Object to, and to Obtain Human Review of, an Automated Decision

As noted, the firm does not currently use AI to make decisions about people. This section records the firm's obligations if that position changes, and also addresses the right to object to AI-assisted processing more broadly.

Any data subject may at any time exercise their right to object under UK GDPR Article 21 or EU GDPR Article 21 to their personal data being processed through an AI tool. On receipt of such an objection, the Compliance Partner assesses whether the firm has a legal obligation, a contractual necessity, or a compelling legitimate interest that overrides the objection. In a legal services context, the firm may be required by law to retain and process certain data (for example, under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017), in which case the objection cannot be upheld in full; this must be explained to the data subject in writing within the response period.

Where the firm does use AI in a way that meets the Article 22 threshold, the data subject has the right to: (a) obtain human intervention in the decision; (b) express their point of view; and (c) contest the decision. The human review must be substantive, not a rubber-stamp. The fee earner or Compliance Partner conducting the review must document that they considered the original data independently of the AI output and reached their own conclusion. The Data (Use and Access) Act 2025 (in force 5 February 2026) widens the lawful bases under which solely automated decisions may be taken under UK law and modifies the accompanying safeguards; the Compliance Partner must confirm the applicable safeguard is in place before any such processing begins.

Divergence between UK and EU law: EU AI Act Article 14 (human oversight) imposes obligations on deployers of high-risk AI systems to enable oversight by natural persons. High-risk system obligations under Annex III are not yet in force (deferred to 2 December 2027 by the Digital Omnibus, in force 29 June 2026). The firm should nonetheless design any future AI-assisted decision process to permit human override, as this is both good practice and will be a hard legal requirement from December 2027.

6. Erasure Where a Vendor May Have Retained or Trained on the Input

A right to erasure request presents particular complexity where personal data has been inputted into a third-party AI tool. The firm's response procedure is as follows.

Step 1: Assess whether a valid erasure ground exists under UK GDPR Article 17(1) or EU GDPR Article 17(1) — for example, the data is no longer necessary for the purpose for which it was collected, or the data subject withdraws consent and there is no other lawful basis. If a retention obligation applies (for example, the firm's duty to retain conveyancing files for at least six years, or SRA record-keeping obligations), the erasure must be refused on that ground and the data subject informed in accordance with Section 7.

Step 2: Where erasure is due, the Compliance Partner submits a deletion request to each relevant vendor. For Microsoft Copilot under a commercial licence, the Microsoft 365 compliance centre provides data subject request tooling. For Lexis+ AI, the firm's account manager is the contact point and the firm's DPA should specify the deletion mechanism and timescale. For ChatGPT, if used under an Enterprise or API agreement, OpenAI provides a privacy request portal. The Compliance Partner logs the date of each vendor request, the vendor's response, and any confirmation of deletion received.

Step 3: If any fee earner has been using an unapproved personal ChatGPT account and personal data from a client file has been inputted, this constitutes a likely personal data breach under UK GDPR Article 33 and EU GDPR Article 33. The Compliance Partner must assess whether the breach threshold (risk to individuals' rights and freedoms) is met and, if so, notify the ICO within 72 hours and, where high risk, notify the affected data subject. The firm cannot compel deletion from a consumer AI account where it has no contractual relationship with the vendor; this must be disclosed to the data subject and to the regulator.

Step 4: Where deletion from a vendor system cannot be confirmed — because the vendor's terms do not provide for it, or because the vendor used the input for model training before a deletion request was made — the firm records this in the request log, informs the data subject of the limitation, and documents the steps taken. This honest account satisfies the firm's accountability obligation under UK GDPR Article 5(2) and EU GDPR Article 5(2). The firm cannot warrant deletion it cannot verify, and must not do so.

7. Refusal Grounds and How a Refusal Is Recorded

The firm may refuse a data subject rights request, in whole or in part, on the grounds set out in UK GDPR and EU GDPR. The most relevant grounds in the context of AI-processed legal data are as follows.

Legal professional privilege: Personal data held on a client file and processed through AI tools may be subject to legal professional privilege. The firm may withhold information that would reveal privileged communications. This is a content-based exemption, not a refusal of the right itself; the firm must still confirm that data exists and provide non-privileged information.

Retention obligation: Where a statutory or regulatory retention period has not expired (for example, SRA rules, the Limitation Act 1980 for limitation purposes, HMRC requirements for probate matters), an erasure or restriction request may be refused to the extent the data must be retained. The data subject is told which obligation applies and for how long it runs.

Manifestly unfounded or excessive requests: Under UK GDPR Article 12(5) and EU GDPR Article 12(5), the firm may refuse or charge a reasonable fee for requests that are manifestly unfounded or excessive. This ground must be applied narrowly and with documented justification; it is not a general mechanism to avoid responding to AI-related complexity.

Third-party data: A SAR response that would involve disclosing personal data about another individual (for example, the opposing party in a family matter) may be redacted or refused to the extent necessary to protect that third party's rights.

Every refusal, whether full or partial, must be: (a) communicated to the data subject in writing within the applicable deadline; (b) drafted in plain English explaining which ground applies and why; (c) accompanied by information about the data subject's right to complain to the ICO (UK) or the relevant supervisory authority (EU), and their right to a judicial remedy; and (d) logged in the request log (see Section 8) with the ground, the date of the decision, and the name of the Compliance Partner who authorised the refusal.

8. Request Log Template

The firm must maintain a written log of every data subject rights request involving AI-processed data. The log is a record of processing activity under UK GDPR Article 5(2) accountability obligations and EU GDPR Article 5(2). It is reviewed by the Compliance Partner quarterly and retained for a minimum of three years. The following fields must be completed for every entry.

Request reference number (sequential, for example DSR-2026-001). Date request received. Data subject name and contact details (or unique identifier if anonymisation is applied to the log). Nature of right(s) exercised (access / rectification / erasure / restriction / objection / automated decision review). Brief description of personal data and matter type (for example, 'client address and financial information — conveyancing file'). AI tool(s) involved (ChatGPT / Microsoft Copilot / Lexis+ AI — specify which). Fee earner who used the AI tool. Date data-mapping exercise completed. Vendor deletion request submitted (yes / no / not applicable) — date and method. Vendor deletion confirmed (yes / no / pending / unable to confirm) — date and evidence reference. Response issued to data subject — date and summary of response. Outcome (request fulfilled / partially fulfilled / refused). If refused: ground relied upon and authorising partner. Extension invoked (yes / no) — if yes, date data subject notified. Any associated breach report — ICO or EU supervisory authority reference number. Compliance Partner sign-off and date.

The log must be stored securely, access-restricted to the Compliance Partner and senior management, and must not itself be processed through any AI tool without a separate lawful basis and risk assessment.

9. Cross-Jurisdiction Position

The following obligations are satisfied once and apply to both UK and EU data subjects: appointing an identified internal owner for each right; maintaining the request log; conducting the vendor data-mapping exercise; applying legal privilege as a refusal ground; issuing written refusals with complaint-route information; and operating the complaints procedure required by the Data (Use and Access) Act 2025 (which meets the procedural standard expected by EU supervisory authorities under EU GDPR Article 77).

The following obligations must be met separately for UK and EU data subjects. Data-processing agreements with AI vendors: EU GDPR Article 28 requires a formal DPA for each vendor processing EU resident data; UK GDPR carries the same requirement but under a separate statutory instrument. Both must be in place; they cannot be satisfied by a single agreement unless it is explicitly dual-compliant. Supervisory authority notification on breach: UK breaches are notified to the ICO; EU resident data breaches are notified to the lead EU supervisory authority for the relevant member state. Both 72-hour windows run independently. EU AI Act Article 50 transparency obligations (in force 2 August 2026): these apply to interactions with EU-resident data subjects and require the firm, as a deployer, to inform users when AI is involved in generating output directed at them. UK law does not yet have an equivalent statutory provision; the stricter EU obligation therefore applies to all EU-resident client communications where AI-generated content is used.

Divergence to note: The EU AI Act Article 22 transparency fine ceiling for non-compliance is up to €15 million or 3% of worldwide annual turnover. The maximum ICO fine under UK GDPR is £17.5 million or 4% of global turnover — the firm cannot compute the turnover-based limb without its own figures, but notes the EU percentage ceiling is lower. The stricter absolute figure is the UK ceiling at £17.5 million; the stricter percentage is 4% under UK law. Both ceilings are material for a firm of this size and both regulators can investigate independently.

Sector-Specific Obligations Review

The rules that apply because of the sector you are in, on top of the general AI and data regime.

1. Regulators with Jurisdiction over Halstead & Rowe Solicitors

Halstead & Rowe Solicitors is authorised and regulated by the Solicitors Regulation Authority (SRA) as its primary professional regulator. The SRA sets the standards of conduct, competence and ethics that govern the firm and every individual solicitor within it. The Legal Services Board (LSB) sits above the SRA as the oversight regulator for the legal services sector in England and Wales and may issue regulatory directions that cascade to the firm through the SRA.

The Information Commissioner's Office (ICO) has concurrent jurisdiction wherever the firm processes personal data, including through ChatGPT, Microsoft Copilot and Lexis+ AI. Because the firm acts for EU-resident clients, the data protection supervisory authorities of the relevant EU member states also have jurisdiction over processing that relates to those clients under the EU GDPR. The two data protection regimes run in parallel and the firm must satisfy both.

The Legal Ombudsman handles client complaints but is not a conduct regulator and does not directly supervise AI use. No FCA, MHRA or Ofcom jurisdiction applies to the firm's declared activities.

2. Sector Rules that Bear on AI Use

The SRA Standards and Regulations 2019 are the primary sector instrument. The SRA Principles require the firm to act with honesty and integrity (Principle 1), in the best interests of each client (Principle 7), and to maintain the trust the public places in solicitors and in the provision of legal services (Principle 2). These Principles are not disapplied because work is assisted by AI; they apply to every output the firm produces regardless of the tool used to produce it.

SRA Code of Conduct for Firms, paragraph 4.2 requires the firm to have effective governance structures and arrangements in place. The absence of any AI policy at Halstead & Rowe is a current breach risk: the SRA has made clear in its published AI guidance (updated 2024) that firms are expected to have identified who is responsible for AI governance, what tools are permitted, and how outputs are reviewed before use. Fee earners using ChatGPT, Microsoft Copilot and Lexis+ AI on their own initiative without an approved policy is a live compliance gap against this paragraph.

SRA Code of Conduct for Solicitors, paragraph 3.4 prohibits a solicitor from making, or causing or allowing to be made, any statement which they know or believe to be false or misleading. Where AI-generated content contains hallucinations or inaccuracies and a fee earner incorporates that content into client correspondence or court documents without verification, each such submission is a potential breach. The Pinsent Masons criticism by a London court in May 2026 for false submissions based on AI-generated search results illustrates the standard against which Halstead & Rowe will be measured.

SRA Transparency Rules impose obligations on how the firm communicates the nature of its services. Where AI materially drafts correspondence sent to clients under the firm's name, the question of whether that constitutes a misleading impression of who or what has performed the work is directly engaged.

The SRA Accounts Rules 2019 are not directly engaged by the AI tools declared, but any AI-assisted processing of financial data from client ledgers would engage them.

3. Where Sector Rules Are Stricter than the General Regime

The general AI and data protection regimes set minimum floors; SRA regulation raises those floors in several material respects specific to Halstead & Rowe.

Legal professional privilege (LPP) and client confidentiality go beyond the confidentiality obligations in UK GDPR and EU GDPR. Under common law and the SRA Code of Conduct for Firms (paragraph 6.3), the firm must keep the affairs of clients confidential. When a fee earner pastes client matter content into ChatGPT, that content leaves the firm's controlled environment and is processed by OpenAI on terms that may permit use for model training unless the firm has configured an enterprise account with appropriate data processing terms. This is a potential waiver of LPP — a risk that has no equivalent in the general GDPR regime, which is concerned with lawfulness of processing rather than privilege. Loss of privilege cannot be remedied after the fact; it is permanent and damages the client. The sector rule is therefore strictly additional to and more demanding than the general data protection requirement.

The SRA's competence framework (statement of solicitor competence) requires fee earners to understand and supervise the tools they use. A fee earner who relies on a Lexis+ AI research summary without verifying cited authorities against primary sources is not demonstrating the level of legal competence the SRA demands, even if the AI provider's terms disclaim accuracy. General AI governance frameworks do not impose personal professional liability of this kind.

Professional indemnity insurance under the SRA Minimum Terms and Conditions of Professional Indemnity Insurance 2013 (MTC) requires the firm's qualifying insurer to indemnify against claims arising from civil liability in private legal practice. Insurers are increasingly scrutinising AI use in underwriting. Undisclosed or unsanctioned use of AI tools that contributes to a negligent outcome may give an insurer grounds to contest coverage under the MTC's basis-of-contract and disclosure conditions. The firm's failure to have a policy governing AI use is therefore a direct insurance risk, not only a regulatory one.

4. Professional and Indemnity Obligations Engaged by AI Use

Every piece of client correspondence drafted using ChatGPT or Microsoft Copilot is issued under the firm's professional authority. The firm remains wholly responsible for its accuracy, tone and legal effect. If AI-drafted correspondence misadvises a client on a conveyancing step, a family law position or a probate entitlement, that is a negligence claim against the firm and potentially a disciplinary matter before the SRA.

The SRA's published position is that AI is a tool, not a person, and does not share in professional responsibility. Responsibility rests with the supervising solicitor. Halstead & Rowe must therefore implement a supervision protocol under which every AI-assisted output in a client matter is reviewed and approved by a qualified fee earner before despatch or filing. This is not discretionary; it is required by SRA Principle 7 (best interests of client) and the competence obligations.

Under the SRA Minimum Terms and Conditions, the firm's insurer must be notified of circumstances likely to give rise to a claim. If an AI error has caused or may have caused a client loss — for example, an incorrect title search summary in a conveyancing matter — the firm must notify its insurer promptly. Delay in notification is itself a breach of the MTC.

For EU-resident clients, the firm's obligations under the applicable EU member state's legal professional rules may also be engaged. Solicitors acting in cross-border matters may be subject to the Council of Bars and Law Societies of Europe (CCBE) Code of Conduct for European Lawyers, which imposes its own client confidentiality and competence standards. The firm should confirm the specific member state rules for each EU client relationship.

5. Reporting and Approval Duties Owed to the SRA

The SRA Code of Conduct for Firms (paragraph 7.7) requires the firm to report to the SRA promptly if it has reasonable grounds to believe there has been a serious breach of the SRA's regulatory arrangements. An undisclosed, systemic use of unapproved AI tools that results in a material failure — such as a confidentiality breach affecting client files, or a negligent AI-assisted advice — is capable of being a serious breach that triggers this mandatory reporting duty.

The SRA has no pre-approval process for individual AI tools equivalent to, for example, FCA product approval. There is therefore no prior authorisation duty before deploying ChatGPT, Microsoft Copilot or Lexis+ AI. However, the firm is required under the SRA Code of Conduct for Firms (paragraph 2.1) to keep its training and competence arrangements under review. Introducing AI tools into client work without updating competence frameworks, training records or supervision arrangements is a failure of that ongoing duty.

If a client makes a complaint about AI use that is not resolved internally, it may reach the Legal Ombudsman. A pattern of upheld complaints connected to AI errors could prompt the SRA to commence a thematic review of the firm's practices. The firm should maintain records of AI use in each matter file sufficient to demonstrate, if required, what tool was used, who reviewed the output, and what changes were made before the output was finalised. These records are also relevant to any ICO audit or SRA file review.

6. EU AI Act Obligations in Force as at 8 August 2026

As at the date of this document, the following EU AI Act provisions are in force and directly relevant to Halstead & Rowe's use of AI tools for EU-resident clients.

Article 50 transparency duties came into force on 2 August 2026. Where the firm uses ChatGPT or Microsoft Copilot to draft correspondence that is substantially AI-generated and that correspondence is sent to EU-resident clients, the deployer (Halstead & Rowe) must ensure those clients are informed that the content was generated by AI, unless the context makes it sufficiently obvious. This obligation applies now, not prospectively. Failure to comply can attract fines of up to €15 million or 3% of worldwide annual turnover, whichever is higher. The firm's turnover-based exposure cannot be calculated without its financial figures, but the fixed cap applies regardless.

General-purpose AI (GPAI) model obligations under the EU AI Act have applied since 2 August 2025. ChatGPT and Microsoft Copilot are built on GPAI models. The obligations at the provider level (OpenAI, Microsoft) include transparency and copyright compliance duties; the firm as deployer is not the primary duty-bearer for GPAI obligations, but must satisfy itself, through its data processing agreements, that the providers it uses are compliant.

Article 5 prohibited practices apply. None of the firm's declared uses — drafting, summarising, research — constitute prohibited AI practices under Article 5 as currently in force. The firm does not use AI for social scoring, subliminal manipulation, or real-time biometric identification in public spaces.

Annex III high-risk obligations do not apply until 2 December 2027 following the Digital Omnibus deferral adopted on 29 June 2026. The firm should monitor whether any future tool deployment (for example, AI-assisted client risk assessment) falls within Annex III categories. For now, no Annex III compliance action is required.

Article 9 risk management and Article 13 transparency requirements for high-risk systems are not yet in force for the firm's current tools but should be incorporated into the firm's AI governance framework as forward planning before December 2027.

7. Cross-Jurisdiction Position: What Is Satisfied Once and What Must Be Met Separately

Certain obligations are substantively identical under UK GDPR and EU GDPR and a single compliant measure satisfies both. A data processing agreement (DPA) with OpenAI (ChatGPT), Microsoft (Copilot) and LexisNexis (Lexis+ AI) that meets the Article 28 requirements under UK GDPR will also meet the equivalent EU GDPR Article 28 requirements, provided the DPA references both regimes. A single record of processing activities (Article 30, both regimes) covering AI-assisted processing is sufficient if it identifies both UK and EU subject data separately. A staff training programme on data minimisation and purpose limitation satisfies the underlying principle in both regimes.

The following must be met separately. The Article 50 EU AI Act transparency duty for EU-resident clients is an EU-only obligation with no direct UK equivalent currently in force. The firm must implement a disclosure mechanism for EU-resident clients that is not required for UK-only clients under current UK law. The ICO AI Auditing Framework is a UK-only instrument; compliance with it does not satisfy the EU AI Act's transparency or risk management articles. Conversely, steps taken to comply with EU AI Act Article 50 do not automatically satisfy the ICO's audit expectations, which are framed around the five UK AI principles.

On automated decision-making: UK GDPR Article 22 and the Data (Use and Access) Act 2025 (most Part 5 provisions in force from 5 February 2026, with the complaints procedure duty in force from 19 June 2026) govern solely automated decisions about individuals in the UK. EU GDPR Article 22 governs the same for EU-resident clients. The firm has declared that it does not use AI in decisions about people, so neither Article 22 regime is currently triggered. This position must be reassessed if any AI tool is used to generate recommendations that directly affect a client's legal position without human review.

Where the two regimes diverge, the stricter obligation applies. On confidentiality of communications with AI providers, no EU or UK law specifically addresses LPP waiver through AI tool use, but the SRA sector rule is stricter than either data protection regime on this point and governs.

AI Risk Register

The ongoing record of AI risks, their owners and their mitigations. A live document — review it on the cadence stated at the foot.

Risk ID	Risk	Tool / Process	Likelihood	Impact	Inherent Rating	Mitigation	Owner	Residual Rating	Review Date
AIR-01	Personal data from conveyancing, family or probate files entered into AI tools and processed by vendor on external servers, breaching UK GDPR / EU GDPR.	ChatGPT, Microsoft Copilot, Lexis+ AI	High	Critical	Critical	Enforce data input rules: no names, addresses, NI numbers or file references. Use anonymisation / pseudonymisation before any AI input. Confirm DPAs with each vendor.	Data Protection Lead	Medium	01 Feb 2027
AIR-02	Client legal privilege waived by disclosing privileged content to a third-party AI vendor, undermining SRA duties and litigation privilege.	ChatGPT, Lexis+ AI	High	Critical	Critical	Prohibit input of privileged communications. Train all fee earners. Include privilege warning in AI Acceptable Use Policy. Log compliance spot-checks quarterly.	Head of Risk & Compliance	Medium	01 Feb 2027
Risk ID	**Risk**	**Tool / Process**	**Likelihood**	**Impact**	**Inherent Rating**	**Mitigation**	**Owner**	**Residual Rating**	**Review Date**
AIR-03	AI-generated draft correspondence or legal summary contains factual or legal errors	ChatGPT, Microsoft Copilot, Lexis+ AI	High	Critical	Critical	Mandatory fee-earner review and sign-off before any AI output is sent or	Supervising Solicitor	Medium	01 Feb 2027

Risk ID	Risk	Tool / Process	Likelihood	Impact	Inherent Rating	Mitigation	Owner	Residual Rating	Review Date
	relied upon without human review, causing client loss or negligence claim.					filed. Apply lessons from Pinsent Masons (May 2026) hallucination ruling. Record review in file note.			
AIR-04	Fee earners using unapproved AI tools (shadow AI) outside any policy, creating uncontrolled data leakage and privilege risk.	Any unapproved tool	High	High	Critical	Publish AI Acceptable Use Policy immediately. Maintain approved-tool list. Block non-approved AI URLs at network level where possible. Disciplinary consequence for breach.	Managing Partner	Medium	01 Aug 2027
AIR-05	AI tool processes personal data of EU-resident clients without satisfying EU GDPR Art 13/14 transparency notices or Art 28 processor agreements.	ChatGPT, Microsoft Copilot, Lexis+ AI	High	High	Critical	Update client privacy notices for EU residents. Execute Art 28 DPAs with all three vendors. Apply stricter EU standard where UK and EU obligations diverge.	Data Protection Lead	Medium	01 Feb 2027
Risk ID	**Risk**	**Tool / Process**	**Likelihood**	**Impact**	**Inherent Rating**	**Mitigation**	**Owner**	**Residual Rating**	**Review Date**
AIR-06	Failure to comply	ChatGPT, Microsoft	High	High	Critical	Add AI-disclosure	Head of Risk & Co	Medium	02 Dec 2026

Risk ID	Risk	Tool / Process	Likelihood	Impact	Inherent Rating	Mitigation	Owner	Residual Rating	Review Date
	with EU AI Act Art 50 transparency duties (in force 2 Aug 2026): clients not informed when AI drafts correspondence or summaries are AI-generated.	Copilot, Lexis+ AI				statement to all client correspondence produced with AI assistance. Display notice on client portal. Record disclosure method per matter.	mpliance		
AIR-07	Bias in AI outputs affecting family or probate clients with protected characteristics, breaching UK Equality Act 2010 s.4 and EU non-discrimination principles.	ChatGPT, Lexis+ AI	Medium	High	High	AI is not used in decisions about people (client-declared). Residual risk: biased research summaries. Fee earner must critically review outputs involving protected-characteristic issues.	Supervising Solicitor	Low	01 Aug 2027
Risk ID	**Risk**	**Tool / Process**	**Likelihood**	**Impact**	**Inherent Rating**	**Mitigation**	**Owner**	**Residual Rating**	**Review Date**
AIR-08	Regulatory change: EU AI Act Annex III high-risk obligations (effective 2 Dec 2027) may capture AI-assisted legal research	Lexis+ AI, ChatGPT	Medium	High	High	Monitor EU AI Office guidance on Annex III scope for legal services. Conduct classification review by Jun 2027. Prepare	Head of Risk & Compliance	Medium	01 Jun 2027

Risk ID	Risk	Tool / Process	Likelihood	Impact	Inherent Rating	Mitigation	Owner	Residual Rating	Review Date
	or case assessment tools if classification changes.					Art 9 risk-management system and Art 13 documentation if required.			
AIR-09	Vendor failure or service outage (OpenAI, Microsoft, LexisNexis) disrupting feeearner productivity and client service obligations.	ChatGPT, Microsoft Copilot, Lexis+ AI	Medium	Medium	Medium	Maintain non-AI fallback workflows for all three use-cases. Review vendor SLAs and uptime guarantees. Include vendor resilience in annual supplier review.	IT / Operations Manager	Low	01 Aug 2027
AIR-10	Vendor data breach or insolvency exposes client personal data held in AI platform logs or training pipelines, triggering ICO and supervisory authority notification duties.	ChatGPT, Microsoft Copilot, Lexis+ AI	Medium	Critical	High	Confirm contractual data-deletion and breach-notification clauses in each DPA. Test 72-hour ICO notification readiness (UK GDPR Art 33). Mirror process for EU supervisory authority where EU residents affected.	Data Protection Lead	Medium	01 Feb 2027

Risk ID	Risk	Tool / Process	Likelihood	Impact	Inherent Rating	Mitigation	Owner	Residual Rating	Review Date
AIR-11	UK DUAA Part 5 automated-decision sa	All tools	Low	Medium	Medium	Complete formal assessment confirming	Data Protection Lead	Low	01 Feb 2027

Risk ID	Risk	Tool / Process	Likelihood	Impact	Inherent Rating	Mitigation	Owner	Residual Rating	Review Date
	feguards (in force 5 Feb 2026) not assessed: firm has declared no AI decisions about people but position must be formally confirmed and documented.					no solely automated decisions under UK DUAA / UK GDPR Art 22. Record conclusion in data protection documentation and revisit if tool use expands.			
AIR-12	No complaints procedure for data protection complaints meeting the UK DUAA duty (in force 19 Jun 2026) to operate a procedure and respond within set time limits.	All tools / all personal data processing	Medium	Medium	Medium	Implement written AI / data protection complaints procedure with response time limits. Publish procedure to clients. Log all complaints and responses.	Data Protection Lead	Low	01 Dec 2026
Risk ID	**Risk**	**Tool / Process**	**Likelihood**	**Impact**	**Inherent Rating**	**Mitigation**	**Owner**	**Residual Rating**	**Review Date**
AIR-13	GPAI model rules (EU AI Act, in force 2 Aug 2025): Halstead & Rowe is a deployer, not a provider, of GPAI tools. Deployer	ChatGPT, Microsoft Copilot	Medium	Medium	Medium	Confirm deployer status with each vendor. Obtain vendor's EU AI Act compliance documentation. Retain copies. No systemic risk desig	Head of Risk & Compliance	Low	01 Feb 2027

Risk ID	Risk	Tool / Process	Likelihood	Impact	Inherent Rating	Mitigation	Owner	Residual Rating	Review Date
	obligations must be understood and met.					nation expected for firm's use scale.			
AIR-14	Regulatory change: UK statutory AI rules for powerful models may be introduced if voluntary safeguards fail (AI Minister statement, Aug 2026). Position should be monitored.	All tools	Low	Medium	Low	Monitor DSIT and ICO announcements. Subscribe to ICO AI Auditing Framework updates. Review policy annually or on any commencement of new UK AI legislation.	Managing Partner	Low	01 Aug 2027

DOCUMENT TITLE: AI Risk Register | Halstead & Rowe Solicitors | Version 1.0 | Date: 08 August 2026 | Next scheduled full review: 01 February 2027

RATING SCALE — apply consistently across all rows:
Likelihood: Low = unlikely in the next 12 months given current controls; Medium = plausible in the next 12 months; High = likely or already occurring.
Impact: Low = minor operational disruption, no regulatory exposure; Medium = reportable incident, reputational harm or client complaint likely; High = significant regulatory, legal or financial consequence; Critical = ICO / supervisory authority enforcement, professional regulatory action, negligence claim or privilege loss.
Inherent Rating (before mitigations): Low × Low = Low; Medium × Medium = Medium; High × High or any Critical impact = High or Critical. Residual Rating applies the same scale after mitigations are implemented.

CROSS-JURISDICTION POSITION:
Obligations satisfied once for both UK and EU: (a) Data Processing Agreements with vendors satisfy both UK GDPR Art 28 and EU GDPR Art 28 if a single agreement addresses both regimes explicitly. (b) A single anonymisation / data-minimisation protocol satisfies both regimes. (c) A single staff training programme covering both UK and EU obligations satisfies both provided EU-specific requirements (Art 50 AI Act disclosures) are included. (d) The vendor resilience and business-continuity review (AIR-09) applies across both regimes.
Obligations that must be met separately: (1) Privacy notices: EU-resident clients require notices compliant with EU GDPR Art 13/14; UK clients require UK GDPR-compliant notices. These are distinct documents or distinct sections. (2) Breach notification: UK GDPR Art 33 requires ICO notification within 72 hours; EU GDPR Art 33 requires notification to the lead supervisory authority for EU residents within 72 hours — both procedures must be operable independently. (3) EU AI Act Art 50 transparency disclosures are an EU-law obligation with no current equivalent UK statutory duty; the disclosure step must be implemented specifically for EU-resident clients and any EU-facing service delivery. (4) Complaints procedure: the UK DUAA duty (in force 19 Jun 2026) is a UK-specific obligation; EU GDPR has its own data-subject rights complaints pathway — both must be maintained.
Divergence and stricter obligation: Where EU AI Act Art 50 imposes disclosure duties not yet replicated in UK law, the EU obligation is applied to all client-facing AI use at Halstead & Rowe as the stricter standard, including for UK-resident clients, so

that a single disclosure practice satisfies both regimes and reduces compliance risk.

APPLICABILITY NOTE — EU AI Act Annex III high-risk systems: As at 08 August 2026 the Digital Omnibus (adopted 29 June 2026) has deferred Annex III high-risk obligations to 2 December 2027. Current AI use at Halstead & Rowe (drafting, summarising, research) does not self-evidently fall within Annex III categories, but the firm must conduct a formal classification review before 1 June 2027 (see AIR-08) because the scope of Annex III for legal services tools remains subject to EU AI Office guidance not yet finalised.

APPLICABILITY NOTE — EU AI Act Art 5 prohibited practices: New prohibitions take effect 2 December 2026. None of ChatGPT, Microsoft Copilot or Lexis+ AI as used for drafting, summarising and research constitute prohibited practices on current declared use. The firm does not use AI for social scoring, real-time biometric identification or manipulation. This position must be reconfirmed at the December 2026 review if tool use expands.

APPLICABILITY NOTE — Art 22 UK GDPR / automated decisions: The firm has declared that AI is not used in decisions about people. AIR-11 records this as a formal finding. If any tool is later configured to produce outputs that directly determine client-facing outcomes without human review, this register must be updated and a full Art 22 / UK DUAA Part 5 assessment conducted before deployment.

MAXIMUM FINES FOR CONTEXT (not an estimate of the firm's exposure): UK: up to £17,500,000 or 4% of global annual turnover, whichever is higher — turnover-based limb cannot be calculated without the firm's financial figures. EU GDPR: up to €20,000,000 or 4% of global annual turnover. EU AI Act: up to €35,000,000 or 7% of global annual turnover for the most serious breaches; up to €15,000,000 or 3% for Art 50 transparency breaches.

REVIEW CADENCE: This register must be reviewed in full by 01 February 2027. It must also be reviewed within 30 days of: any new AI tool being adopted; any change to the firm's AI use cases; any ICO or supervisory authority enforcement action in the legal sector; or any commencement of new AI legislation in the UK or EU. Individual risks with earlier review dates (AIR-06, AIR-12) must be updated on those dates without waiting for the full review cycle.

AI Incident Response Procedure

What happens in the first hour after an AI-related incident, and who does it. The regulator clock starts before anyone has decided who is in charge.

1. Document Identity and Scope

Document: AI Incident Response Procedure
Issued to: Halstead & Rowe Solicitors
Date: 08 August 2026
Version: 1.0

This procedure governs every incident arising from the use of ChatGPT (OpenAI), Microsoft Copilot, or Lexis+ AI within Halstead & Rowe Solicitors. It applies to all fee earners, support staff, and any locum or contractor working on the firm's files. It operates alongside, and does not replace, the firm's existing data breach procedure under UK GDPR and the SRA Codes of Conduct. Where this procedure and another firm document conflict, the stricter obligation prevails.

Because the firm processes personal data via AI and acts for EU-resident clients, both UK GDPR and EU GDPR obligations apply. The EU AI Act (Regulation (EU) 2024/1689) also applies to the extent that the firm deploys AI systems whose output affects EU-resident data subjects. The Data (Use and Access) Act 2025 (DUAA), with its Part 5 data protection provisions in force from 5 February 2026 and its complaints-procedure duty in force from 19 June 2026, applies to all UK processing. The ICO AI Auditing Framework and the UK Equality Act 2010 inform the post-incident review obligations.

2. What Counts as an AI Incident

An AI incident is any event in which the use of ChatGPT, Microsoft Copilot, or Lexis+ AI causes, or creates a material risk of causing, harm to a client, a third party, the firm, or any regulatory obligation. The harm may be to confidentiality, data protection, professional privilege, accuracy of advice, or the firm's regulatory standing.

Examples specific to Halstead & Rowe include: a fee earner pastes a client's full name, address, and conveyancing transaction details into ChatGPT without confirming whether data-sharing with OpenAI's training pipeline has been disabled; Microsoft Copilot generates a draft client letter that incorporates information from a different client's file stored in the same Microsoft 365 tenancy; Lexis+ AI returns a case citation that does not exist and the fee earner includes it in a court submission without verification; a member of staff uses a personal, unapproved AI tool on a family law matter and a document containing special-category data (health or financial information) is processed outside the firm's agreed data processors; an AI-generated summary of a probate file overstates or omits an asset, leading to a misleading statement to HMRC or a beneficiary; or an EU-resident client is not informed that correspondence sent to them was substantially drafted by a generative AI system, potentially engaging Article 50 transparency duties of the EU AI Act which came into force on 2 August 2026.

The trigger is reasonable suspicion, not certainty. Staff must not wait for confirmation of harm before raising an incident.

3. Severity Levels and the Response Each Triggers

Every incident is classified at first report as one of three severity levels. Classification may be upgraded but not downgraded without the approval of the Designated Compliance Officer (defined in Section 5).

Level 1 — Critical. Personal data of clients or third parties has been, or is highly likely to have been, disclosed to an AI system in a manner that was not authorised by the firm's data processing agreements; or privileged information has left the firm's control; or an AI output has been relied upon in a filed court document, a HMRC

submission, or a Land Registry application and is materially incorrect; or the incident affects EU-resident clients and may engage EU AI Act Article 50 obligations or EU GDPR notification requirements. Level 1 triggers immediate containment (Section 4), mandatory regulator-notification assessment within the first hour, and activation of the full incident team.

Level 2 — Significant. An unapproved AI tool has been used on a client matter but there is no confirmed data exfiltration; or an AI-generated document was sent to a client but the error was caught and corrected before reliance; or a transparency obligation to a client may have been missed but no regulatory deadline has yet elapsed. Level 2 triggers containment, evidence preservation, and a written incident report within 24 hours. Regulator notification is assessed within 24 hours.

Level 3 — Low. An AI tool was used without following the firm's sign-off process but no client data was processed and no output was relied upon. Level 3 triggers a documented review and a process reminder to the relevant staff member. No regulatory notification is expected, but the incident is still recorded in the AI Incident Register.

4. First-Hour Actions: Contain, Preserve Evidence, Stop the Tool

The first hour after an incident is reported is the period of highest regulatory and legal risk. The regulator clock under UK GDPR Article 33 and EU GDPR Article 33 runs from when the firm becomes aware, not from when it completes its investigation. The following actions are mandatory and must be completed in sequence, with each step time-stamped.

Step 1 — Contain (minutes 0–10). The staff member who identifies the incident stops using the AI tool immediately and does not delete, overwrite, or share any file, prompt, output, or conversation log. If the incident involves ChatGPT, the staff member does not close or clear the chat session. If it involves Microsoft Copilot, they do not close the document or application. If it involves Lexis+ AI, they preserve the search and output screen. The staff member telephones the Designated Compliance Officer (DCO) immediately; email alone is not sufficient for Level 1 or Level 2.

Step 2 — Preserve evidence (minutes 10–25). The DCO or their deputy takes screenshots or exports of all relevant AI prompts and outputs, preserving metadata. Copies are saved to the firm's secure incident folder, not the matter file. The original matter file is placed on read-only access pending review. Any email or document generated by AI that has already been sent is flagged and its recipient noted.

Step 3 — Stop the tool (minutes 25–40). The DCO determines whether the relevant AI tool should be suspended across the firm or only for the specific user and matter. For Level 1 incidents, firm-wide suspension is the default. Access credentials or Microsoft 365 permissions are revoked or restricted by the firm's IT administrator. The DCO contacts the vendor using the escalation route in Section 8.

Step 4 — Assess and classify (minutes 40–60). The DCO completes a written first-hour assessment recording: the tool involved, the data or output affected, whether personal data was processed, whether any EU-resident clients are affected, and the provisional severity level. This assessment is the foundation for the regulator notification decision in Section 6.

5. Named Roles and Their Deputies

The following roles are fixed. Deputies must be briefed on this procedure and have access to all relevant credentials before any incident occurs.

Designated Compliance Officer (DCO): [Insert name of COLP or senior partner with compliance responsibility]. Deputy DCO: [Insert name of nominated deputy]. The DCO leads the incident response, makes the regulator notification decision, and authorises all external communications. The DCO is the single point of contact for the ICO, the SRA, and any EU supervisory authority.

Data Protection Lead (DPL): [Insert name]. Deputy DPL: [Insert name]. The DPL supports the DCO on all UK GDPR and EU GDPR questions, drafts notifications to regulators and affected individuals, and maintains the AI

Incident Register.

IT Administrator: [Insert name or role if outsourced]. Responsible for revoking or restricting tool access, preserving system logs, and liaising with Microsoft, OpenAI, and LexisNexis on technical matters.

SRA Reporting Partner: [Insert name of COLP if different from DCO]. Responsible for assessing whether the incident requires notification to the SRA under the firm's regulatory obligations and for any notification to the Legal Ombudsman where client detriment has occurred.

Out-of-hours contact: All named individuals must ensure the DCO and DPL hold each other's personal mobile numbers. Incidents do not pause for weekends or bank holidays.

6. The Regulator Notification Decision and Its Statutory Deadline

UK GDPR and Deadline. Under UK GDPR Article 33, the firm must notify the ICO of a personal data breach without undue delay and, where feasible, within 72 hours of becoming aware, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. The 72-hour clock starts at the moment any member of staff becomes aware of the incident, not when the DCO is notified. If the firm cannot notify within 72 hours, it must notify as soon as possible and provide reasons for the delay. Under UK GDPR Article 34 and DUAA Part 5 safeguards in force from 5 February 2026, affected individuals must be notified without undue delay if the breach is likely to result in a high risk to their rights and freedoms. The DUAA's complaints-procedure duty (in force 19 June 2026) means the firm must also be able to log and respond to any complaint from a data subject arising from the incident within the statutory time limits.

EU GDPR and Deadline. Where the incident affects EU-resident clients and the firm acts as controller in respect of their data, EU GDPR Article 33 imposes the same 72-hour notification obligation to the lead supervisory authority in the relevant EU Member State. Where clients are resident in multiple EU Member States, the DCO must identify the competent authority. EU GDPR Article 34 mirrors the high-risk individual notification threshold. The EU regime does not provide a longer deadline; both clocks run from the same moment of awareness. The firm must keep written records of every breach regardless of whether it notifies, pursuant to Article 33(5) of both regimes.

Divergence and Stricter Obligation. The substantive 72-hour deadline is identical under both regimes. Where they diverge is in the supervisory authority to be notified: the ICO for UK processing, and the relevant EU Member State authority for EU-resident clients' data. Both notifications may be required for the same incident. The firm must not assume that notifying the ICO satisfies its EU obligations.

EU AI Act — Article 50 Transparency. With Article 50 transparency duties in force from 2 August 2026, if the incident reveals that EU-resident clients received AI-generated correspondence without the required disclosure, the DCO must assess whether a transparency failure has occurred and document the remediation steps. There is no separate short-form notification deadline under Article 50 itself, but the failure must be corrected promptly and recorded.

SRA Notification. The SRA Codes of Conduct require the firm to report serious breaches of regulatory requirements and matters that put client interests at risk. A Level 1 incident will ordinarily require the COLP to assess SRA notification; this assessment must be completed within 24 hours of the incident being classified Level 1.

Maximum Exposure. The maximum ICO fine is £17.5 million or 4% of global annual turnover, whichever is higher (the turnover-based limb cannot be computed without the firm's figures). The maximum EU AI Act fine for a transparency breach under Article 50 is €15 million or 3% of worldwide annual turnover. For other infringements the maximum is €35 million or 7% of global annual turnover. The turnover-based limb cannot be computed without the firm's figures.

7. Notifying Affected Individuals and the Threshold for Doing So

The obligation to notify affected individuals arises under UK GDPR Article 34 and EU GDPR Article 34 when a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons. For Halstead & Rowe, the practical threshold is met in any of the following circumstances: client personal data (including special-category data in family law or health-related probate matters) has been submitted to an AI tool in a manner not covered by an adequate data processing agreement; AI-generated advice or correspondence has caused, or is likely to cause, financial loss or legal prejudice to a client; or client data has been cross-contaminated between matters through an AI tool.

The notification to the individual must be in plain language, describe the nature of the breach, give the name and contact details of the DCO, describe the likely consequences, and set out the measures taken or proposed. It must not be delayed pending the completion of the internal investigation if the high-risk threshold is already met.

Where the firm acts for EU-resident clients, the notification obligation under EU GDPR Article 34 runs in parallel. The content requirements are substantively identical. Where a client is both UK and EU-resident (for example, a dual national), both regimes apply and the stricter presentation standard governs.

Notification may be deferred only if it would prejudice a law enforcement investigation or if the firm has implemented measures that eliminate the high risk. The DCO must document the reasoning for any deferral in the AI Incident Register. Client notification is never deferred solely because the firm is still assessing its own liability.

8. Vendor Escalation Route

Each of the three AI tools in scope has a specific escalation route, and the IT Administrator must hold current contact details for each.

ChatGPT (OpenAI). OpenAI's data processing agreement (DPA) governs the firm's use of ChatGPT for business purposes. In the event of a suspected data incident, the firm must submit a security incident report via the OpenAI business support portal and request confirmation of whether any data submitted in the affected session was retained or used for model training. The DCO should request a written response within 24 hours. OpenAI's DPA and sub-processor list must be reviewed as part of the post-incident review to confirm whether the incident falls within a notifiable breach under the firm's contract.

Microsoft Copilot. Microsoft's data processing terms under the Microsoft Product Terms and Data Protection Addendum govern Copilot use within Microsoft 365. The firm's IT Administrator should raise a Priority A support ticket via the Microsoft 365 Admin Centre, flagging it as a potential data breach. Microsoft's contractual obligation is to notify the firm without undue delay if it becomes aware of a personal data breach affecting the firm's data. The DCO should request confirmation of audit log availability and any data access or exfiltration by Microsoft systems.

Lexis+ AI (LexisNexis). The firm's subscription agreement with LexisNexis will contain a DPA. The DCO or DPL contacts the LexisNexis account manager and data protection contact directly, requesting written confirmation of data handling for the session in question and whether any matter-specific data was retained outside the firm's tenancy.

In all cases, vendor responses are preserved in the AI Incident Register. The firm does not rely on verbal assurances; all confirmations must be in writing.

9. Post-Incident Review and the Register

A post-incident review is conducted for every incident, regardless of severity level. For Level 1 and Level 2 incidents the review is completed within 14 calendar days. For Level 3 incidents it is completed within 30 calendar days.

The review is conducted by the DCO and DPL and must address: the root cause of the incident; whether existing policies or training were inadequate; whether the AI tool involved requires updated configuration, additional

contractual protections, or withdrawal from use; whether the incident reveals a systemic pattern (for example, fee earners consistently bypassing approval processes, which was identified as a concern at onboarding); and any remedial action taken or planned. Where the incident involves EU-resident clients or EU AI Act Article 50 transparency obligations, the review must also confirm that the required transparency measures are now in place for future interactions with those clients.

The ICO AI Auditing Framework and the firm's obligations under the UK Equality Act 2010 inform the review where the incident touches on outputs that could have discriminatory effect on clients with protected characteristics. At present the firm has confirmed that AI is not used in decisions about people, so the Equality Act dimension will typically be limited to reviewing whether AI outputs embedded in client advice inadvertently reflected bias. This must nonetheless be checked in every review.

All incidents, including Level 3 incidents that did not trigger regulatory notification, are recorded in the AI Incident Register. The Register is a permanent, dated record containing: the date and time of the incident; the AI tool involved; the matter type (conveyancing, family, or probate) and client identifier (not full name in the register itself); the severity classification; the first-hour actions taken with timestamps; the regulator notification decision and outcome; any individual notifications sent; vendor escalation steps and responses; and the post-incident review findings and remedial actions. The Register is reviewed by the DCO quarterly and is produced to the ICO, SRA, or any EU supervisory authority on request. It constitutes the firm's record of compliance with UK GDPR Article 33(5) and EU GDPR Article 33(5) and satisfies the DUAA's accountability requirements. The Register is stored securely and access is limited to the DCO, DPL, and SRA Reporting Partner.

10. Cross-Jurisdiction Position: What Is Satisfied Once and What Must Be Met Separately

Satisfied once for both regimes. The 72-hour personal data breach notification deadline (UK GDPR Article 33 and EU GDPR Article 33) is substantively identical; a single internal assessment and decision process satisfies both, though the notifications themselves go to different authorities. The individual notification threshold and content requirements (UK GDPR Article 34 and EU GDPR Article 34) are substantively identical; a single notification letter, appropriately addressed, satisfies both where the client is the same individual. The obligation to maintain a written record of all breaches (Article 33(5) of both regimes) is satisfied by a single AI Incident Register maintained to the higher standard. The post-incident review process satisfies both regimes' accountability principles.

Must be met separately. Regulatory notification must be sent separately: to the ICO for UK processing and to the competent EU Member State supervisory authority for EU-resident clients' data. These are separate submissions to separate bodies. The EU AI Act Article 50 transparency obligation (in force 2 August 2026) has no direct UK equivalent in statute at present; the UK's principles-based framework does not impose an equivalent statutory disclosure requirement for AI-generated content, so this obligation must be tracked and met independently for EU-resident clients. High-risk AI obligations under EU AI Act Annex III are deferred to 2 December 2027 following the Digital Omnibus adopted on 29 June 2026; no equivalent obligation exists under UK law at present, so no action is currently required on this point, but the firm must monitor the UK position as the government has indicated it may introduce statutory rules for powerful AI models. The DUAA's complaints-procedure duty (in force 19 June 2026) applies to UK processing only; EU-resident complainants' rights are governed by EU GDPR and the applicable Member State's supervisory authority procedures.

EU AI Act Risk Tier Classification

Each AI tool placed in its risk tier under the Act, with the reasoning written down. The tier decides every obligation that follows.

Tool	Use Case (Halstead & Rowe)	Role	Risk Tier	Basis for Classification	Obligations Triggered (in force)	Obligations Triggered (not yet in force)
ChatGPT (OpenAI)	Drafting client correspondence; summarising case documents	Deployer. OpenAI is the provider. Halstead & Rowe deploys ChatGPT for professional purposes.	LIMITED RISK (current). Possible GPAI scrutiny.	ChatGPT is a general-purpose AI (GPAI) system, not listed in Annex I or Annex III. It does not make decisions about people. Deployer transparency duties under Art 50 apply from 2 August 2026.	Art 50 transparency: inform clients and staff when AI-drafted content is involved. GPAI provider obligations (OpenAI) active from 2 August 2025. Deployer must not obscure AI involvement.	Art 5 prohibited practices enforceable 2 December 2026 — confirm ChatGPT use does not employ subliminal manipulation. Annex III high-risk obligations not applicable here; deadline 2 December 2027 in any event.
ChatGPT (OpenAI)	Drafting client correspondence; summarising case documents	Deployer	BOUNDARY NOTE	Use involves personal data from conveyancing, family and probate files, including EU-resident clients. This raises the risk profile but does not alone elevate the tier. Remains Limited Risk absent Annex III characteristics.	Cautious position adopted: treat as upper boundary of Limited Risk. Document this classification annually or upon any material change in use.	If ChatGPT is used to profile individuals or support consequential decisions about them, re-classify immediately against Annex III criteria.
Microsoft Copilot	Drafting client correspondence; summarising case documents; research and analysis	Deployer. Microsoft is the provider. Halstead & Rowe deploys Copilot within its Microsoft 365 environment.	LIMITED RISK (current). Possible GPAI scrutiny.	Copilot is a GPAI-based assistant integrated into productivity tools. Not Annex I or Annex III listed. Does not make decisions about people per client declaration. Art 50 deployer transparency duties apply from 2 August 2026.	Art 50: disclose AI involvement to clients and staff where Copilot drafts or summarises material. Verify Microsoft's GPAI compliance (in force 2 August 2025). Review Microsoft's data processing terms for UK GDPR and EU GDPR alignment.	Art 5 prohibited practices: enforceable 2 December 2026 — no issue identified on current use. Annex III obligations not applicable; deadline 2 December 2027 if classification changes.

Tool	Use Case (Halstead & Rowe)	Role	Risk Tier	Basis for Classification	Obligations Triggered (in force)	Obligations Triggered (not yet in force)
Microsoft Copilot	Drafting client correspondence; summarising case documents; research and analysis	Deployer	BOUNDARY NOTE	Copilot operates inside Microsoft 365 tenancy, processing firm and client data. Integration depth creates a higher confidentiality risk than a standalone tool. Tier remains Limited Risk but warrants enhanced contractual and technical controls.	Cautious position adopted: treat as upper boundary of Limited Risk. Confirm Microsoft's contractual commitments on data residency, confidentiality, and no model training on client data before any further rollout.	Re-assess if Copilot is extended to case management, client-facing outputs, or legal advice generation, as those uses may approach Annex III criteria.
Lexis+ AI	Research and analysis; summarising case documents	Deployer. LexisNexis is the provider. Halstead & Rowe deploys Lexis+ AI for legal research.	LIMITED RISK (current). Annex III proximity noted.	Lexis+ AI is a domain-specific GPAI tool for legal research. Not Annex I listed. Annex III does not explicitly list legal research AI. It does not make decisions about people. Art 50 transparency duties apply from 2 August 2026.	Art 50: where Lexis+ AI output is incorporated into advice or correspondence, disclose AI involvement. Verify LexisNexis GPAI provider obligations. Apply human review to all AI-generated citations — Pinsent Masons (May 2026) confirms judicial risk of unverified AI outputs.	Art 5: no prohibited practice identified on current use. Annex III high-risk obligations: if Lexis+ AI is later used to support decisions in administration of justice contexts (Annex III point 8), re-classify by 2 December 2027 deadline.
Lexis+ AI	Research and analysis; summarising case documents	Deployer	BOUNDARY NOTE	Legal research AI sits adjacent to Annex III point 8 (administration of justice and democratic processes). Current use is research-support only, not decision-support. Cautious position: classify as Limited Risk but monitor Annex III point 8 guidance from AI Office.	Cautious position adopted: document that Lexis+ AI outputs are reviewed and verified by a qualified fee earner before use in any client matter. Maintain audit log of research tasks performed.	If the firm uses Lexis+ AI to generate legal opinions, predict case outcomes, or support tribunal submissions without full human review, re-classify as high-risk under Annex III point 8 immediately.

DOCUMENT: EU AI Act Risk Tier Classification | CLIENT: Halstead & Rowe Solicitors | DATE: 08 August 2026

RATING SCALE

The EU AI Act (Regulation (EU) 2024/1689) establishes four tiers: (1) Prohibited — banned outright under Art 5; (2) High-Risk —

Annex I (products) and Annex III (stand-alone systems in sensitive domains); (3) Limited Risk — transparency obligations under Art 50 apply; (4) Minimal Risk — no mandatory obligations. All three tools deployed by Halstead & Rowe are classified as Limited Risk. None is Prohibited. None currently meets Annex III high-risk criteria on the declared uses. None falls within Annex I product categories.

CURRENT OBLIGATIONS IN FORCE (as at 08 August 2026)
Art 50 transparency duties commenced 2 August 2026. From that date Halstead & Rowe, as deployer, must ensure clients and counterparties are informed when AI systems are used to generate or substantially alter written communications. This applies immediately to all three tools. GPAI provider obligations (covering OpenAI, Microsoft, and LexisNexis) have been in force since 2 August 2025; Halstead & Rowe should obtain written confirmation from each provider of their compliance status.

OBLIGATIONS NOT YET IN FORCE
Art 5 prohibited practices: extended enforcement from 2 December 2026. The prohibited practices do not appear to be engaged on current declared uses, but the firm must confirm this before that date. Annex III high-risk obligations for stand-alone systems: deferred to 2 December 2027 by the Digital Omnibus (in force 29 June 2026). Annex I high-risk obligations: deferred to 2 August 2028. Art 50(2) machine-readable marking of synthetic content: 2 December 2026 (grace period for systems already on market before 2 August 2026).

ART 9 RISK MANAGEMENT (not yet mandatory for Limited Risk tools)
Although Art 9 formal risk management systems are required only for high-risk AI, Halstead & Rowe should begin documenting a proportionate risk log for each tool now. This will reduce reclassification burden if any tool's use expands, and demonstrates regulatory good faith to the ICO and EU AI Office.

ART 13 TRANSPARENCY (not yet mandatory for Limited Risk tools)
Art 13 detailed technical transparency applies to high-risk systems. It is not triggered on current classification. However, the firm should maintain internal records of which tool was used for which task, to support any future audit.

GPAI RULES (Chapter V, EU AI Act)
ChatGPT, Microsoft Copilot, and Lexis+ AI are all based on general-purpose AI models. Provider-level GPAI obligations (copyright policy, summary of training data, cooperation with AI Office) fall on OpenAI, Microsoft, and LexisNexis respectively — not on Halstead & Rowe as deployer. The firm's obligation is to deploy these tools within the terms of their provider agreements and to avoid uses that would constitute prohibited practices.

FINE EXPOSURE (EU)
For Limited Risk non-compliance (primarily Art 50 transparency failures): up to €15 million or 3% of global annual turnover, whichever is higher. For prohibited practice violations (Art 5): up to €35 million or 7% of global annual turnover. Turnover-based limb cannot be computed without the firm's figures; the statutory maximum is stated. These are EU-side figures; UK-side fines are addressed in companion documents.

UNAPPROVED STAFF USE
Fee earners at Halstead & Rowe have been using AI tools on their own initiative without a policy in place. This creates deployer liability under Art 50 because undisclosed AI use by staff is attributable to the firm as deployer. A formal AI Acceptable Use Policy must be adopted as an immediate priority, predating any further staff use of the three tools.

CLIENT CONFIDENTIALITY AND LEGAL PRIVILEGE
Classification under the EU AI Act does not reduce obligations under UK GDPR, EU GDPR, or the SRA Code of Conduct. Personal data processed via AI tools — including conveyancing, family, and probate file content — must not be input into tools that train on user data without explicit contractual prohibition from the provider. This must be verified in each provider's data processing agreement before continued use.

REVIEW CADENCE
This classification must be reviewed: (a) annually as a minimum; (b) immediately upon any material change in how a tool is used; (c) before 2 December 2026 to confirm Art 5 compliance; (d) before 2 December 2027 to assess whether any tool has migrated to Annex III high-risk. Owner: the designated AI Compliance Lead (to be appointed).

CROSS-JURISDICTION NOTE

This document addresses EU AI Act classification only. The companion UK framework document covers UK GDPR Art 22, the Data (Use and Access) Act, the ICO AI Auditing Framework, and the UK Equality Act 2010. Where the EU AI Act and UK obligations diverge — in particular on transparency disclosure and automated decision-making safeguards — the stricter obligation applies. Art 50 transparency duties (EU) are currently stricter than any equivalent UK statutory duty and therefore govern disclosure practice for both UK and EU-resident clients.

Annex III High-Risk Gap Analysis

Measured against the high-risk obligations: what is in place, what is missing, and what closing each gap requires.

Obligation	Requirement	Current Position	Gap	Action Required	Owner	Priority
PRELIMINARY: Annex III Applicability Assessment	Determine whether AI tools used by Halstead & Rowe fall within any Annex III high-risk category.	No formal classification exercise conducted. ChatGPT, Copilot and Lexis+ AI used ad hoc by fee earners.	No classification decision documented.	Complete a written classification exercise against all eight Annex III domains. Document conclusions.	COLP / Managing Partner	CRITICAL
PRELIMINARY: Deployer vs Provider Distinction	Deployers (those who put an AI system into use) carry distinct obligations from providers (developers). Halstead & Rowe is a deployer of ChatGPT, Copilot and Lexis+ AI.	No policy distinguishes deployer duties. Fee earners treat tools as personal productivity aids.	Deployer obligations entirely unaddressed.	Adopt a written deployer policy. Confirm provider terms for each tool and retain copies.	COLP	CRITICAL
Annex III — 1. Biometric identification and categorisation	AI used for real-time or post-remote biometric ID of natural persons is high-risk.	None of the three tools is used for biometric identification at Halstead & Rowe.	Not applicable. No gap.	No action required. Record this exclusion in the classification log.	COLP	N/A
Annex III — 2. Critical infrastructure management	AI managing or operating road, water, gas, electricity or digital infrastructure is high-risk.	Halstead & Rowe is a solicitors' firm. It does not operate critical infrastructure.	Not applicable. No gap.	Record exclusion in classification log.	COLP	N/A
Annex III — 3. Education and vocational training	AI determining access to, or assessing performance in, education or training is high-risk.	No AI tool is used for trainee assessment or admission decisions at the firm.	Not applicable. No gap.	Record exclusion in classification log.	COLP	N/A
Annex III — 4. Employment, worker management and access to self-employment	AI used in recruitment, promotion, task allocation or monitoring workers is high-risk.	Copilot and ChatGPT are not currently deployed for HR decisions. Use is limited to legal work.	Low risk of scope creep if fee earners begin using tools for HR tasks without approval.	Governance policy must explicitly prohibit unapproved AI use in recruitment or performance management.	Managing Partner / HR lead	HIGH

Obligation	Requirement	Current Position	Gap	Action Required	Owner	Priority
Annex III — 5. Access to essential private and public services (credit, benefits, emergency)	AI used to evaluate creditworthiness or assess entitlement to essential services is high-risk.	Halstead & Rowe does not make credit or benefit decisions. Conveyancing, family and probate work does not engage this category.	Not applicable on current use. No gap.	Record exclusion. Monitor if practice areas expand.	COLP	N/A
Annex III — 6. Law enforcement	AI used for individual risk assessment, polygraph-equivalent tools or crime analytics by law enforcement is high-risk.	Halstead & Rowe is not a law enforcement body and does not supply tools to one.	Not applicable. No gap.	Record exclusion in classification log.	COLP	N/A
Annex III — 7. Migration, asylum and border control	AI used in immigration risk assessment, document authenticity or asylum applications is high-risk.	The firm acts for EU-resident clients in conveyancing, family and probate matters. None of the three tools is used for immigration or asylum determinations.	Not applicable on current use. No gap.	Record exclusion. If immigration work commences, reassess.	COLP	N/A
Annex III — 8. Administration of justice and democratic processes	AI assisting courts, tribunals or alternative dispute resolution in applying law to facts, or influencing elections, is high-risk.	Lexis+ AI and ChatGPT are used to summarise case documents and draft correspondence. This may constitute AI assisting in the administration of justice.	Potential high-risk classification. No assessment or documentation exists.	Conduct written risk assessment. Engage Lexis+ AI provider for classification documentation. Seek SRA guidance.	COLP / Head of Legal	CRITICAL
EU AI Act Art 9 — Risk Management System (deployer)	Deployers must implement a risk management system throughout the AI system lifecycle (Art 9, EU AI Act 2024/1689). Applicable from 2 December 2027 for Annex III systems (Digital Omnibus, 29 June 2026).	No risk management system exists for any AI tool in use.	Complete gap. Deadline is 2 December 2027 but preparatory work is required now.	Design and document a risk management framework covering identification, evaluation, and mitigation of risks for each tool.	COLP / DPO	HIGH

Obligation	Requirement	Current Position	Gap	Action Required	Owner	Priority
EU AI Act Art 13 — Transparency and provision of information (deployer)	Deployers must ensure AI systems are sufficiently transparent for users to interpret output and use it appropriately. Applicable from 2 December 2027 for Annex III.	Fee earners receive no structured guidance on the limitations or error rates of ChatGPT, Copilot or Lexis+ AI.	No transparency or limitations documentation provided to staff.	Issue tool-specific guidance notes on known limitations, hallucination risk and verification requirements. Review provider documentation.	Head of Legal / COLP	HIGH
EU AI Act Art 50 — Transparency to natural persons (deployer, in force 2 August 2026)	Art 50 is now in force (2 August 2026). Deployers using AI that interacts with natural persons must disclose AI involvement. Applies to client-facing AI output.	Client correspondence drafted with AI assistance is sent without any disclosure of AI involvement.	Active breach risk. No disclosure mechanism in place for EU-resident clients.	Implement AI disclosure wording in client correspondence and engagement letters for EU-resident clients immediately.	COLP / Client Relations	CRITICAL
EU AI Act Art 50 — Synthetic content marking (in force 2 December 2026)	From 2 December 2026, machine-readable marking of AI-generated content will be required (Art 50(2)). Four-month grace period for pre-August 2026 tools ends 2 December 2026.	No watermarking or tagging of AI-generated content is in place.	Gap will become a breach on 2 December 2026.	Confirm with OpenAI, Microsoft and LexisNexis whether their tools support ma chine-readable content marking. Plan implementation before 2 December 2026.	IT Manager / COLP	HIGH
EU AI Act Art 5 — Prohibited practices (in force 2 December 2026)	Certain AI practices are prohibited from 2 December 2026, including subliminal manipulation, exploitation of vulnerabilities, and non-consensual intimate image generation.	None of the three tools is used for prohibited purposes on current evidence.	Risk of inadvertent breach if unapproved tools are adopted by fee earners without governance controls.	AI governance policy must list prohibited use cases. Staff training to cover Art 5 prohibitions before 2 December 2026.	COLP	HIGH
EU AI Act GPAI Rules — General Purpose AI obligations (in force 2 August 2025)	GPAI model rules apply to providers of GPAI models. Halstead & Rowe is a deployer, not a provider. Deployers are not directly subject to GPAI obligations.	Not directly applicable as a deployer. However, firm relies on GPAI models (ChatGPT, Copilot).	Indirect risk: if providers are non-compliant, deployer's own compliance may be affected.	Review provider GPAI compliance documentation and retain evidence. Include in due diligence for tool approvals.	COLP / IT Manager	MEDIUM

Obligation	Requirement	Current Position	Gap	Action Required	Owner	Priority
UK GDPR / DUAA — Automated decision-making (Art 22 UK GDPR; DUAA Part 5, in force 5 February 2026)	Art 22 UK GDPR restricts solely automated decisions with significant effects. DUAA Part 5 introduces wider lawful bases and safeguards for such decisions. The firm has stated AI is not used in decisions about people.	Confirmed: AI not used for decisions about individuals. No Art 22 exposure on current use.	No gap on stated use. Risk if use changes without governance controls.	Governance policy must prohibit use of AI tools for decisions about individuals without COLP sign-off.	COLP / DPO	MEDIUM
UK GDPR — Personal data processed via AI tools	Processing personal data via AI tools requires a lawful basis, data minimisation, and appropriate processor agreements (UK GDPR Arts 5, 6, 28).	Conveyancing, family and probate files containing personal data are being uploaded to ChatGPT and Copilot by fee earners. No data processing agreements confirmed for all tools.	Significant gap. Client personal data may be processed without adequate contractual or legal basis.	Confirm DPA / processor agreements with OpenAI, Microsoft and LexisNexis. Assess data residency. Restrict upload of personal data until controls are in place.	DPO / COLP	CRITICAL
UK DUAA — Complaints procedure (in force 19 June 2026)	Controllers must operate a complaints procedure and respond to data protection complaints within set time limits (DUAA, in force 19 June 2026).	No AI-specific complaints procedure exists. General client complaints procedure may not cover AI-related data issues.	Gap against the 19 June 2026 obligation, which is already in force.	Update complaints procedure to cover AI-related data protection complaints. Publish response timelines.	COLP / DPO	HIGH
ICO AI Auditing Framework — Risk and governance	The ICO AI Auditing Framework requires documented accountability, risk assessment and human oversight for AI processing personal data.	No AI governance documentation, risk register or oversight log exists at the firm.	Complete gap against the ICO framework.	Create an AI risk register, assign accountability, and document human review processes for AI-assisted work.	DPO / Managing Partner	HIGH
Obligation	**Requirement**	**Current Position**	**Gap**	**Action Required**	**Owner**	**Priority**
UK Equality Act 2010 — Non-discrimination in AI outputs	AI tools must not produce outputs that discriminate on protected characteristics. Fee earners relying	No policy on reviewing AI outputs for discriminatory content. No training	Gap: discriminatory AI output risk unmanaged.	Include equality bias review in AI output verification protocol. Add to staff training.	Head of Legal / HR lead	HIGH

Obligation	Requirement	Current Position	Gap	Action Required	Owner	Priority
	on AI drafts in family or probate matters carry liability for biased outputs.	provided.				
SRA Regulatory Obligations — Client confidentiality and legal privilege	SRA Principles and Codes require solicitors to protect client confidentiality. Uploading privileged file content to third-party AI tools may waive privilege or breach confidentiality.	Fee earners are uploading case documents to ChatGPT and Copilot without any policy restriction or privilege assessment.	Active breach risk of SRA obligations and legal professional privilege.	Issue immediate instruction prohibiting upload of privileged or confidential content to AI tools pending full policy implementation.	Managing Partner / COLP	CRITICAL
Governance — AI Acceptable Use Policy	A formal AI Acceptable Use Policy is required to bring unsanctioned tool use under control and satisfy ICO, SRA and EU AI Act deployer obligations.	No policy exists. Fee earners are using AI tools entirely on their own initiative.	Complete gap. Root cause of most other gaps identified in this analysis.	Draft, approve and publish an AI Acceptable Use Policy covering approved tools, permitted uses, data restrictions and disciplinary consequences.	COLP / Managing Partner	CRITICAL
Governance — Staff Training	Staff must be trained on AI risks, permitted uses, verification duties and regulatory obligations before using AI tools on client matters.	No training has been provided. Use is ad hoc and uncontrolled.	Complete gap.	Deliver mandatory AI compliance training to all fee earners before AI tool use resumes on client files.	Head of Legal / COLP	CRITICAL
Cross-Jurisdiction — Obligations satisfied once for both regimes	Certain controls satisfy both UK and EU obligations simultaneously: AI Acceptable Use Policy, staff training, DPA / processor agreements, human oversight procedures, and equality bias review.	None of these controls are in place.	All cross-jurisdiction baseline controls are absent.	Implement controls listed. Document that each satisfies both UK GDPR and EU AI Act requirements where applicable.	COLP / DPO	CRITICAL
Obligation	**Requirement**	**Current Position**	**Gap**	**Action Required**	**Owner**	**Priority**
Cross-Jurisdiction — Obligations that must be met separately	EU Art 50 disclosure to EU-resident clients must be addressed separately from UK	No jurisdiction-specific compliance measures in place for either	Dual-regime gap. EU obligations are generally stricter (higher	Apply EU standard as the floor for all shared obligations.	COLP / DPO	HIGH

Obligation	Requirement	Current Position	Gap	Action Required	Owner	Priority
	GDPR notices. EU AI Act risk management documentation must satisfy Art 9 (EU) and the ICO AI Auditing Framework (UK) independently. Where they diverge, the stricter obligation applies.	regime.	fines: €35m / 7% turnover vs £17.5m / 4% turnover).	Maintain separate EU-facing client disclosure and Art 9 risk management documentation.		

DOCUMENT: Annex III High-Risk Gap Analysis | CLIENT: Halstead & Rowe Solicitors | DATE: 08 August 2026 | FRAMEWORK: UK + EU Combined Compliance Framework

GAP SUMMARY COUNT BY PRIORITY:
- CRITICAL (immediate action, existing or imminent breach): 8 gaps
- HIGH (action required before relevant deadline or within 90 days): 8 gaps
- MEDIUM (monitor and address within 6 months): 2 gaps
- N/A (Annex III domain assessed and confirmed not applicable): 6 domains

PRIORITY RATING SCALE:
CRITICAL — obligation already in force; evidence of non-compliance exists or breach risk is immediate. Address within 30 days.
HIGH — obligation in force or coming into force within 12 months; controls absent. Address within 90 days.
MEDIUM — obligation in force but current exposure is low; monitor and address within 6 months.
N/A — obligation assessed and confirmed not applicable to this business on current facts; record exclusion in classification log and review if practice areas change.

ANNEX III CLASSIFICATION NOTE (DOMAIN 8 — ADMINISTRATION OF JUSTICE):
This is the most significant classification question for Halstead & Rowe. Annex III, point 8 of EU AI Act 2024/1689 designates as high-risk any AI system intended to assist a judicial authority in researching and interpreting facts and law, or in applying the law to a concrete set of facts. Lexis+ AI is marketed explicitly for legal research and analysis. ChatGPT is used to summarise case documents. Both uses may fall within the scope of this category when applied to live client matters. The high-risk obligations for Annex III systems apply from 2 December 2027 (Digital Omnibus, in force 29 June 2026), but preparatory risk management and documentation work must begin now. The COLP must commission a written classification opinion and engage LexisNexis regarding its own classification documentation before that deadline.

DEPLOYER OBLIGATIONS DISTINGUISHED FROM PROVIDER OBLIGATIONS:
Halstead & Rowe is a deployer, not a provider, of all three tools. As a deployer of a high-risk Annex III system (if classified), the firm's obligations under EU AI Act 2024/1689 include: (a) use the AI system in accordance with the provider's instructions (Art 26(1)); (b) assign human oversight to competent individuals (Art 26(2)); (c) monitor operation and report serious incidents to the provider and national authority (Art 26(5)); (d) conduct a fundamental rights impact assessment before deployment where required (Art 27); (e) implement the Art 9 risk management system as applied to deployer context; (f) comply with Art 50 transparency duties to natural persons, now in force from 2 August 2026. Providers (OpenAI, Microsoft, LexisNexis) carry the obligations for conformity assessment, CE/UKCA marking, technical documentation and registration in the EU AI database — these are not the firm's responsibility, but the firm must verify that its chosen providers meet them before or by 2 December 2027.

VERIFIED DATES APPLIED IN THIS DOCUMENT:
- Art 50 transparency duties: in force 2 August 2026.
- Art 50(2) synthetic content marking: in force 2 December 2026.
- Art 5 new prohibitions: in force 2 December 2026.
- Annex III high-risk obligations: in force 2 December 2027 (post Digital Omnibus deferral, 29 June 2026).
- Annex I high-risk obligations: in force 2 August 2028.

- GPAI model rules: in force 2 August 2025.
- DUAA Part 5 automated decision provisions: in force 5 February 2026.
- DUAA complaints procedure duty: in force 19 June 2026.

FINE EXPOSURE NOTE:
UK maximum: £17.5 million or 4% of global annual turnover (whichever is higher). The turnover-based limb cannot be computed without Halstead & Rowe's financial figures.
EU maximum: €35 million or 7% of global annual turnover (whichever is higher). The turnover-based limb cannot be computed without the firm's financial figures.
Where UK and EU obligations diverge, this analysis applies the stricter EU standard as the compliance floor.

REVIEW CADENCE:
This gap analysis must be reviewed: (i) within 30 days of adoption of the AI Acceptable Use Policy; (ii) no later than 1 November 2026 to address the 2 December 2026 Art 5 and Art 50(2) deadlines; (iii) no later than 1 September 2027 ahead of the 2 December 2027 Annex III deadline; (iv) whenever a new AI tool is proposed for use, a new practice area is opened, or a regulatory enforcement action is announced affecting the legal sector.

Article 50 Transparency Assessment and Disclosures

Where you must tell people they are dealing with AI, and the exact wording to use.

Document Identity

Document title: Article 50 Transparency Assessment and Disclosures
Prepared for: Halstead & Rowe Solicitors
Date: 08 August 2026
Regimes covered: UK GDPR; Data (Use and Access) Act 2025 (Part 5 provisions in force 5 February 2026; complaints-procedure duty in force 19 June 2026); ICO AI Auditing Framework; EU AI Act 2024/1689 — Article 50 transparency duties in force 2 August 2026; GPAI rules in force 2 August 2025.

This document identifies every customer-facing AI touchpoint operated by Halstead & Rowe Solicitors, states the disclosure obligation that attaches to each, supplies ready-to-use disclosure wording, addresses the marking of AI-generated content, and sets out placement, timing and accessibility requirements. It covers both UK and EU obligations explicitly and, where they diverge, applies the stricter obligation.

Applicable Legal Framework

Under the EU AI Act, Article 50(1) (in force 2 August 2026) requires deployers of AI systems that interact directly with natural persons — including systems that generate or manipulate text, images or other content — to disclose that fact to those persons in a clear and timely manner before the interaction begins or, at the latest, at the first interaction. Article 50(3) imposes additional obligations on deployers of generative AI systems that produce synthetic content: such content must be marked in a machine-readable format and, where technically feasible, detectable as artificially generated. Article 50(2) obligations relating to machine-readable marking of synthetic content do not apply until 2 December 2026; however, the human-readable disclosure duty under Article 50(1) is in force now. Article 13 requires that AI systems placed on the market be transparent enough for deployers to understand how to use them. Article 9 requires deployers to implement risk-management measures commensurate with the risks of the system. GPAI obligations under the Act have applied since 2 August 2025.

Under UK law, the ICO AI Auditing Framework requires organisations to implement transparency measures that are meaningful, contextual and delivered at the point of interaction. UK GDPR Articles 13 and 14 require data subjects to be informed of automated processing of their personal data. The Data (Use and Access) Act 2025, Part 5, provides updated safeguards for solely automated decisions; as Halstead & Rowe has confirmed it does not use AI for decisions about people, the Article 22 / DUAA solely-automated-decision regime does not apply.

Where the two regimes diverge, this document applies the stricter obligation. The EU AI Act Article 50(1) requires disclosure before or at the first moment of interaction; UK ICO guidance requires disclosure at the point of interaction. These are materially equivalent. The EU regime imposes explicit machine-readable marking of synthetic content from 2 December 2026; the UK has no equivalent statutory obligation at this date. The EU obligation is therefore stricter on that point and governs the firm's practice for EU-resident clients; Halstead & Rowe should adopt it universally as best practice.

Cross-Jurisdiction Position

The following obligations are satisfied once and satisfy both regimes simultaneously: (a) human-readable disclosure that AI is being used in a client-facing interaction; (b) records of AI tools in use and their purposes; (c) staff training on disclosure obligations; (d) a written AI use policy identifying approved tools.

The following obligations must be met separately or have jurisdiction-specific content: (a) machine-readable marking of AI-generated content — required for EU-resident clients from 2 December 2026 under EU AI Act Art

50(2)/(3); no equivalent UK statutory duty exists at this date, but the firm should apply it universally; (b) complaints-procedure responses within statutory time limits — the DUAA duty (in force 19 June 2026) applies to UK data subjects; EU GDPR one-month response period applies to EU data subjects; where both apply, the shorter deadline governs; (c) any notification to an EU national AI supervisory authority must follow that Member State's procedures; ICO is the relevant UK authority. Halstead & Rowe acts for EU-resident clients in conveyancing, family and probate matters, so both regimes are engaged in practice.

Customer-Facing AI Touchpoints

Halstead & Rowe Solicitors has declared three AI tools in active use: ChatGPT (OpenAI), Microsoft Copilot, and Lexis+ AI. The firm uses these for drafting client correspondence, summarising case documents, and research and analysis. The following touchpoints have been identified as customer-facing or as producing output that is delivered to clients.

Touchpoint 1: Client correspondence drafted or substantially assisted by ChatGPT or Microsoft Copilot. This includes letters of advice, completion statements, care-arrangement letters in family matters, and grant-of-probate covering letters. The client receives a document that has been generated or materially shaped by a generative AI system.

Touchpoint 2: Case summaries or document summaries produced using any of the three tools and shared with the client. This includes summaries of title registers, medical reports in family proceedings, or estate-asset schedules in probate matters.

Touchpoint 3: Research and analysis outputs produced using Lexis+ AI or ChatGPT that are incorporated into or attached to client-facing advice documents, opinions or reports.

Touchpoint 4: Any AI-assisted email sent directly to a client. Where fee earners use Microsoft Copilot within Outlook to draft or substantially redraft client emails, the resulting message is a client-facing AI-generated communication.

No AI chatbot or automated client portal has been declared. If such a system is introduced, this document must be updated before deployment and a prior-to-interaction disclosure added.

Disclosure Obligations by Touchpoint

Touchpoint 1 — Drafted correspondence: EU AI Act Art 50(1) requires Halstead & Rowe, as deployer, to inform the client that the letter was produced with the assistance of a generative AI system before or at the moment the correspondence is received. ICO AI Auditing Framework requires the same in substance. The disclosure must be prominent, not confined to a footer, and must name or describe the AI involvement clearly.

Touchpoint 2 — AI-generated summaries: The same Article 50(1) duty applies. A summary is content produced or substantially shaped by AI and delivered to the client. The disclosure must accompany the summary, not appear only in a general terms-of-business clause.

Touchpoint 3 — Research and analysis incorporated into advice: Where AI-generated analysis is incorporated into a document provided to the client, disclosure is required. The ICO AI Auditing Framework explicitly requires contextual disclosure rather than generic privacy-policy references. If the AI output is used only as an internal research aid and the fee earner rewrites the advice entirely in their own professional judgement, the output is no longer AI-generated content delivered to the client; disclosure at client level is not triggered, but internal records must reflect the tool used.

Touchpoint 4 — AI-assisted client emails: Where Microsoft Copilot drafts or substantially rewrites an email sent to a client, the email is AI-generated correspondence and the Article 50(1) duty is triggered. A brief inline disclosure must be included within the email body itself, not solely in a signature block.

Ready-to-Use Disclosure Wording

The following wording is approved for immediate use. Fee earners must select the appropriate version and insert it at the specified location. No amendment is permitted without sign-off from the designated AI Compliance Lead.

Wording A — For letters and formal correspondence (to be placed as the first paragraph or immediately beneath the salutation, before the substantive content):

"Please note: this letter was drafted with the assistance of an artificial intelligence tool. The content has been reviewed and approved by the fee earner named above, who accepts professional responsibility for it. If you have any questions about our use of AI, please contact us."

Wording B — For AI-generated case or document summaries (to be placed as a heading or introductory note on the first page of the summary):

"AI-Assisted Summary — Halstead & Rowe Solicitors has prepared this summary using an artificial intelligence tool. The summary has been checked by the supervising fee earner. It is provided to assist your understanding and should be read alongside the original documents."

Wording C — For research or analysis documents containing AI-generated content (to be placed on the cover page or as the opening paragraph of the document):

"This document contains analysis produced with the assistance of an AI research tool. All conclusions and recommendations have been reviewed and adopted by the responsible fee earner, who remains professionally accountable for the advice given."

Wording D — For AI-assisted client emails (to be placed as the first line of the email body, above the greeting or immediately after it, not in the signature):

"Note: This email was drafted with the assistance of an AI writing tool and has been reviewed by the sender before sending."

Wording E — For EU-resident clients receiving AI-generated content from 2 December 2026 onwards (machine-readable marking supplement): In addition to the human-readable wording above, all documents delivered to EU-resident clients must include a machine-readable metadata tag identifying the content as AI-generated, in compliance with EU AI Act Art 50(2)/(3). The IT lead must implement a document metadata protocol by 1 December 2026. Until that date, human-readable disclosure under Wording A, B or C is sufficient.

Marking of AI-Generated or Manipulated Content

The EU AI Act Art 50(3), in force 2 August 2026, requires deployers of generative AI systems to ensure that outputs are marked in a machine-readable format where technically feasible, so that content can be detected as artificially generated. The Art 50(2) obligation relating specifically to synthetic content marking has a grace period to 2 December 2026 for systems already on the market before 2 August 2026. ChatGPT, Microsoft Copilot and Lexis+ AI were all in use before that date, so the grace period applies to machine-readable marking. Human-readable disclosure is required now.

For UK-resident clients, there is no equivalent statutory machine-readable marking obligation at this date. The ICO AI Auditing Framework recommends clear labelling of AI-generated material but does not impose a machine-readable format requirement.

Practical action: Halstead & Rowe must ensure that all letters, summaries and reports delivered to EU-resident clients and generated with AI assistance carry a machine-readable metadata tag by 2 December 2026. In the interim, human-readable Wording A, B or C above satisfies the disclosure obligation. The firm should extend machine-readable marking to all clients as a single universal practice to avoid a two-track system and to demonstrate compliance to both the ICO and EU supervisory authorities. Microsoft Word and PDF formats both support custom metadata fields that can be used for this purpose; the IT lead must configure a standard metadata field labelled "AI-Assisted: Yes" to be applied to all AI-drafted documents before they leave the firm.

Placement and Timing

Both the EU AI Act Art 50(1) and the ICO AI Auditing Framework require that disclosure arrives at or before the moment the client first encounters the AI-generated content. Placement in a footer, in standard terms and conditions, or in a privacy notice appended to the engagement letter is not sufficient on its own. Those locations are permissible as supplementary references but do not discharge the obligation.

For Touchpoint 1 and Touchpoint 3 (letters and advice documents), Wording A or C must appear as the first paragraph of the document or immediately below the salutation. It must not be buried on a final page.

For Touchpoint 2 (summaries), Wording B must appear as a header or introductory note on the first page, before any substantive content.

For Touchpoint 4 (emails), Wording D must appear as the first line of the email body. It must not appear only in the footer or signature block, which many clients read last or not at all.

For any future client-facing AI chatbot or automated telephone interaction, disclosure must be given before the substantive interaction begins — for example, as the opening message before any question is posed or answered. This requirement is stated here for forward planning purposes; no such system is currently deployed.

Fee earners must not defer disclosure to a follow-up communication. If an AI-drafted letter is sent and disclosure is omitted, a corrective disclosure must be sent immediately and the incident recorded in the AI incident log.

Accessibility of Disclosures

The ICO AI Auditing Framework and the EU AI Act Art 13 both require that transparency information be accessible to the intended audience. For Halstead & Rowe, clients include individuals who may have low digital literacy, be under stress (family and probate matters in particular), have visual impairments, or use English as a second language given the firm's EU-resident client base.

The following accessibility standards apply to all disclosure wording used by the firm. Language must be plain English, written at no higher than a GCSE reading level; avoid legal Latin and technical AI terminology. Font size in printed correspondence must be no smaller than 11pt; digital documents must use a minimum 12pt equivalent. For clients who have notified the firm of a visual impairment or who use screen readers, documents must be provided in an accessible format (tagged PDF or Word with heading styles) and the disclosure wording must be included in the document's accessibility metadata as well as in the visible text.

For EU-resident clients whose correspondence language is not English, the disclosure wording must be provided in the language of the correspondence. Approved translations of Wording A through D must be obtained and stored in the precedents library before any AI-generated document is sent in a language other than English. Using AI to produce those translations is permissible provided a qualified translator reviews them.

The firm's website and client care letter must include a standing reference explaining that AI tools are used in service delivery and directing clients to request further information. This standing reference is not a substitute for document-level disclosure but ensures clients who wish to query AI use have a clear route to do so before they receive any document.

Client Confidentiality, Legal Privilege and Data Protection Interface

Disclosure under Art 50 does not resolve confidentiality and legal privilege risks; it runs alongside them. When fee earners input client data into ChatGPT, Microsoft Copilot or Lexis+ AI, personal data about clients — including special-category data arising in family proceedings and financial data in conveyancing and probate — is processed by a third-party system. UK GDPR and EU GDPR both require a lawful basis for that processing and a data processing agreement with each provider. The AI transparency disclosures set out in this document must be accompanied by an updated privacy notice explaining what data is shared with AI providers and on what legal basis.

The firm must not include data that is subject to legal professional privilege in any prompt submitted to a third-party AI system unless it has confirmed that the provider's terms do not permit use of that data for model training and that the data is processed within an environment that preserves confidentiality. Microsoft Copilot for Microsoft 365 (enterprise licence) and Lexis+ AI both provide contractual confidentiality commitments that the firm should verify are current. ChatGPT used through a consumer account does not provide equivalent protections; fee earners must use only the ChatGPT Enterprise or API version under a data processing agreement, or cease using it for client matters immediately.

This document does not stand alone on data protection; it must be read with the firm's Data Protection Impact Assessment and AI Acceptable Use Policy.

Governance and Implementation Steps

The following steps are required to give effect to this document. Each has a named responsibility and a deadline.

Immediate (by 22 August 2026): The AI Compliance Lead must circulate Wording A through D to all fee earners with written instruction that use of the wording is mandatory for all AI-assisted client documents from the date of receipt. A simple checklist must be added to the matter-opening and document-finalisation workflow.

By 1 September 2026: The firm's client care letter and engagement terms must be updated to include a standing AI-use disclosure. The privacy notice must be updated to describe AI tool use and third-party processing.

By 1 October 2026: All fee earners must complete a 90-minute AI transparency and data protection training session. Attendance records must be kept for ICO inspection.

By 1 December 2026: The IT lead must implement the document metadata protocol for machine-readable AI marking, ready for the EU AI Act Art 50(2) obligation effective 2 December 2026.

Ongoing: Any new AI tool must be assessed against this framework before deployment. Client-facing use of an unapproved tool is a reportable incident. The AI incident log must record any omitted disclosure, the corrective action taken, and the date resolved.

Maximum penalties for non-compliance: Under the EU AI Act, failure to comply with Art 50 transparency obligations carries fines of up to €15 million or 3% of worldwide annual turnover, whichever is higher (note: the briefing cites €15m/3%; the overall Act maximum of €35m/7% applies to the most serious prohibited-practice violations under Art 5, which are not engaged here). Under UK GDPR, the ICO maximum for transparency failures is £17.5 million or 4% of global annual turnover; the turnover-based limb cannot be calculated without the firm's figures. Both figures are cited so the firm understands the regulatory stakes; the firm's insurers and partners should be made aware of these exposure levels.

Cross-Jurisdiction Compliance Position

Where the regimes agree, where they diverge, and which obligations you satisfy once rather than twice.

Document Identity

Document: Cross-Jurisdiction Compliance Position
Client: Halstead & Rowe Solicitors
Prepared by: AI Compliance Consultancy
Date: 08 August 2026
Scope: UK GDPR, Data (Use and Access) Act 2025, ICO AI Auditing Framework, UK Equality Act 2010, EU AI Act 2024/1689, EU GDPR
AI Tools in Scope: ChatGPT (OpenAI), Microsoft Copilot, Lexis+ AI

1. Jurisdictional Basis

Halstead & Rowe Solicitors is established in the UK and is therefore subject to UK GDPR, the Data (Use and Access) Act 2025 (DUAA), and the ICO's AI Auditing Framework as a matter of primary obligation. The firm also acts for EU-resident clients on conveyancing, family and probate matters. Because the firm's AI tools process personal data belonging to those EU-resident clients — data that originates from persons located in the EU — the firm falls within the territorial scope of EU GDPR (Article 3(2)(a)) and the EU AI Act 2024/1689 as a deployer offering services to individuals in the EU (Article 2(1)(c) EU AI Act). Both regimes therefore apply in full and are addressed explicitly throughout this document.

The maximum regulatory exposure under UK GDPR is £17.5 million or 4% of global annual turnover, whichever is higher. The firm has not disclosed its turnover; the turnover-based limb cannot therefore be calculated here and must be assessed internally. Under the EU AI Act, the maximum fine for a deployer breaching transparency or other deployer obligations is €15 million or 3% of global annual turnover; for prohibited-practice violations the ceiling is €35 million or 7% of global annual turnover. Again, the turnover-based limb requires the firm's own figures. These figures represent the combined worst-case exposure and should be communicated to the firm's professional indemnity insurer.

2. Obligations Satisfied Once for Both Regimes

Several foundational obligations are substantively identical across UK and EU law and can be discharged by a single measure that meets the stricter of the two standards.

Lawful basis for processing personal data via AI. Both UK GDPR and EU GDPR require a lawful basis under Article 6 before personal data from client files may be submitted to ChatGPT, Microsoft Copilot, or Lexis+ AI. For client data, legitimate interests (Article 6(1)(f)) is the most likely basis, but it must be documented in a legitimate interests assessment that takes into account the special sensitivity of legal-matter data. One assessment, drafted to the higher standard required by EU GDPR supervisory guidance, satisfies both regimes simultaneously.

Data-processing agreements with AI vendors. Both regimes require a controller-processor agreement (UK GDPR Article 28; EU GDPR Article 28) before a processor may handle personal data on the firm's behalf. The firm must execute data-processing agreements with OpenAI, Microsoft, and LexisNexis. A single agreement drafted to include all Article 28 mandatory clauses satisfies both regimes, provided the international-transfer safeguards addressed in Section 3 are also in place.

Purpose limitation and data minimisation. The principle that personal data must not be used for purposes incompatible with the original collection purpose (UK GDPR Article 5(1)(b); EU GDPR Article 5(1)(b)) and must be limited to what is necessary (Article 5(1)(c)) applies identically. Halstead & Rowe's internal AI use policy must

prohibit fee earners from pasting entire client files into AI tools and must specify that only the minimum data needed for the drafting or summarisation task may be submitted. One policy provision satisfies both regimes.

Record of processing activities. Both regimes require a Record of Processing Activities (RoPA) under Article 30. Adding AI-assisted processing activities — drafting correspondence, summarising case documents, legal research — to the firm's existing RoPA discharges the obligation in both regimes.

Human oversight and verification of AI outputs. The ICO AI Auditing Framework and the EU AI Act Article 13 (transparency and human oversight) both require that AI outputs are reviewed by a qualified person before being relied upon or sent to clients. The Pinsent Masons case (May 2026), in which a court criticised a firm for false submissions based on AI-generated results, makes clear that this is also a professional conduct requirement under the Solicitors Regulation Authority (SRA) standards. One documented oversight protocol — requiring a fee earner to verify every AI-generated draft or summary — satisfies both regimes and the SRA simultaneously.

Transparency to clients about AI use. EU AI Act Article 50 (in force 2 August 2026) requires deployers to inform natural persons when they are interacting with, or receiving content substantially generated by, an AI system. UK GDPR Articles 13 and 14 require disclosure of automated processing in privacy notices. A single updated client privacy notice and engagement-letter clause, drafted to include the Article 50 disclosure in plain language, satisfies both the UK transparency obligation and the EU AI Act deployer obligation.

3. Obligations That Must Be Met Separately

International data transfers require separate analysis for each regime. UK GDPR governs transfers of personal data from the UK to third countries under the UK's own adequacy regulations and International Data Transfer Agreements (IDTAs). EU GDPR governs transfers of EU-resident client data under standard contractual clauses (SCCs) adopted by the European Commission. OpenAI and Microsoft have both published EU SCCs and UK IDTAs in their data-processing terms; Halstead & Rowe must verify that the correct instrument is in place for each data flow: UK-origin data uses the IDTA; EU-origin client data uses the EU SCCs. These are legally distinct instruments and cannot substitute for one another.

Regulatory notification and complaints handling differ procedurally. Under the DUAA (the duty to operate a complaints procedure, in force 19 June 2026), the firm must maintain a documented data-protection complaints procedure with defined response time limits and communicate it to data subjects. This obligation is UK-specific. Complaints from EU-resident clients who believe their data has been misused by AI tools are handled through the one-stop-shop mechanism under EU GDPR: the lead supervisory authority is determined by the firm's EU establishment position, addressed in Section 4 below. The firm must maintain separate escalation contacts for ICO complaints and for EU supervisory authority complaints.

The EU AI Act Article 50(2) obligation to apply machine-readable markings to AI-generated synthetic content does not come into force until 2 December 2026. No equivalent UK statutory obligation currently exists. When that provision commences, the firm will need a separate process for marking AI-generated documents intended for EU-resident clients. No equivalent action is required at this date for UK-only outputs.

The UK Equality Act 2010 imposes a duty, specific to the UK regime, to ensure that AI tools do not produce outputs that discriminate against protected-characteristic groups. There is no directly equivalent provision in the EU AI Act for the firm's current use cases (the Annex III high-risk categories that would engage the Act's non-discrimination obligations — such as AI in employment decisions — do not apply because the firm has confirmed it does not use AI for decisions about people). The Equality Act duty must nonetheless be addressed in the firm's AI use policy: fee earners must be instructed not to rely on AI outputs that make assumptions based on a client's age, disability, race, religion, sex, sexual orientation or other protected characteristic. This is a UK-specific action.

4. Points of Divergence — Stricter Obligation Applied

Where the two regimes diverge, this document identifies the stricter obligation and states that Halstead & Rowe must meet that stricter standard in all cases, because doing so will simultaneously satisfy the lesser requirement.

Automated decision-making. UK GDPR Article 22, as amended by the DUAA (in force 5 February 2026), widens the lawful bases on which solely automated decisions with legal or similarly significant effect may be made, and introduces new safeguards. EU GDPR Article 22 retains the original, narrower framework: solely automated decisions of this kind are prohibited unless one of three narrow gateways applies (necessity for contract; authorisation by law; explicit consent). The firm has confirmed it does not use AI for decisions about people, so Article 22 is not currently engaged in either regime. If this position changes, the EU GDPR standard — being stricter — must be met.

Transparency timing. EU AI Act Article 50 (in force 2 August 2026) requires disclosure at the point of interaction or at the time the AI-generated content is delivered. UK GDPR Articles 13 and 14 require disclosure at the point of data collection or within one month of indirect collection. The EU AI Act obligation is event-specific and real-time; it is stricter in that it cannot be deferred to a periodic privacy notice update. Halstead & Rowe must adopt the real-time disclosure standard for all client-facing AI outputs, which automatically satisfies the UK GDPR timing requirement.

Risk management documentation. The EU AI Act Article 9 requires deployers of AI systems to implement a risk-management system proportionate to the risks posed. The ICO AI Auditing Framework recommends but does not currently mandate a risk-management system for all AI deployers. The Article 9 obligation is therefore stricter. The firm must produce and maintain a documented AI risk register covering ChatGPT, Microsoft Copilot, and Lexis+ AI, their data inputs, and the controls in place. That document also satisfies the ICO's framework expectations.

Fines regime. The EU AI Act maximum fine for deployer violations (€15 million or 3%) exceeds the comparable ICO fine threshold for the firm's likely breach categories. The EU GDPR maximum (€20 million or 4%) is higher in euro terms than the UK GDPR equivalent (£17.5 million or 4%). The firm's compliance posture should be calibrated to the EU ceilings, which at current exchange rates exceed the UK ceilings in absolute terms.

5. EU AI Act — Current Position for Halstead & Rowe

As of 8 August 2026, the following EU AI Act provisions are in force and apply to the firm as a deployer.

Article 50 transparency duties (in force 2 August 2026). The firm must ensure that any natural person — including EU-resident clients — who receives a document substantially generated by ChatGPT, Microsoft Copilot, or Lexis+ AI is informed of that fact. This applies to AI-drafted client correspondence and AI-generated case summaries shared with clients. The disclosure must be clear, timely, and in plain language. The engagement letter and covering correspondence must be updated immediately.

GPAI rules (in force 2 August 2025). ChatGPT and Microsoft Copilot are general-purpose AI models. The GPAI obligations under the EU AI Act apply to their providers (OpenAI and Microsoft), not directly to Halstead & Rowe as deployer. However, the firm should verify that its vendors have complied with GPAI transparency and safety obligations as part of due diligence on its data-processing agreements.

Article 5 prohibited practices. The prohibition on certain AI practices under Article 5 applies in full. None of the firm's declared uses — drafting correspondence, summarising documents, legal research — constitutes a prohibited practice. This assessment must be revisited if the firm's use cases change.

Annex III high-risk systems (compliance deadline 2 December 2027, per Digital Omnibus adopted 29 June 2026). The firm's current uses do not fall within the Annex III high-risk categories. The firm does not use AI for recruitment, credit scoring, access to essential services, or decisions about individuals. No high-risk obligations are triggered at this date. The firm must re-assess if it adopts AI tools for any purpose that could constitute case-outcome prediction or client-eligibility assessment.

Article 9 risk management. As a deployer, the firm must implement a risk-management system proportionate to its use cases. This means a documented AI risk register, reviewed at least annually, covering each tool's data inputs, the nature of outputs, client-confidentiality risks, and the controls applied.

6. Establishment and Representative Position

Halstead & Rowe Solicitors is established in the UK. It has no disclosed EU establishment (branch, subsidiary, or registered office in an EU Member State). For UK regulatory purposes, the ICO is the competent supervisory authority and the firm engages with it directly.

For EU GDPR purposes, because the firm has no EU establishment, there is no lead supervisory authority under the one-stop-shop mechanism. Any EU supervisory authority in the Member State of a data subject who makes a complaint may exercise jurisdiction. The firm should monitor which Member States its EU-resident clients are located in and be prepared to respond to supervisory authorities in those jurisdictions. If the firm's EU client base is concentrated in particular Member States, it should identify the relevant national data protection authority (for example, the CNIL in France, the BfDI in Germany, or the relevant authority in the client's home state).

For EU AI Act purposes, the firm as a deployer with no EU establishment is still subject to the Act by virtue of deploying AI systems whose outputs affect EU-resident persons (Article 2(1)(c)). The Act does not currently require a firm in this position to appoint an EU representative for deployer-only obligations, unlike the provider representative requirement. This position should be confirmed with specialist EU counsel if the firm's EU client volume increases materially.

For UK AI regulatory purposes, no AI-specific regulator currently exists. The ICO is the relevant authority for data-protection aspects of AI use. The SRA is the relevant authority for professional conduct aspects. The firm should maintain a single regulatory contact log identifying the ICO as its data-protection authority, the SRA as its conduct authority, and the relevant EU supervisory authorities for EU-client complaints.

7. Which Regulator Is Approached for What

The ICO is the firm's primary data-protection regulator for all UK GDPR and DUAA matters: data-subject access requests, complaints about UK-origin data processed by AI, breach notification (within 72 hours under UK GDPR Article 33), and engagement on the ICO AI Auditing Framework. The firm's designated data-protection contact must have direct access to ICO reporting channels.

The SRA is the regulator for professional conduct, client confidentiality, and legal privilege. Any AI-related conduct issue — including a fee earner relying on an unverified AI output in client advice or court submissions — must be assessed against SRA standards and reported where required. The Pinsent Masons case (May 2026) demonstrates that courts will impose reputational and costs consequences independently of regulatory action.

The EU national supervisory authority in the relevant Member State handles complaints from EU-resident clients about EU GDPR violations. The firm must acknowledge and respond to such complaints and engage with the authority's process. No single lead authority exists given the absence of an EU establishment.

The EU AI Office (European Commission) oversees GPAI compliance and co-ordinates national enforcement of the EU AI Act. National market-surveillance authorities in each Member State handle deployer-level AI Act complaints. If a complaint is made about the firm's AI disclosures by an EU-resident client, the firm should expect the relevant national authority to investigate. The firm should respond promptly and transparently, referencing its documented compliance measures.

8. Consolidated Action List

The following actions are required for Halstead & Rowe Solicitors. Items are sequenced by urgency, with immediate items first. Each item identifies whether it satisfies one regime, both, or is specific to one.

ACTION 1 — IMMEDIATE (overdue): Draft and publish an internal AI Acceptable Use Policy. This policy must: list the approved tools (ChatGPT, Microsoft Copilot, Lexis+ AI) and prohibit all other AI tools without prior written approval from the firm's data-protection lead; prohibit submission of client names, matter references, or identifiable personal data to AI tools unless a lawful basis and a processor agreement are confirmed in writing; require every AI-generated output to be reviewed and verified by the responsible fee earner before use; and require declaration

of AI use in any court filing. Satisfies: UK GDPR Articles 5, 24, 25; EU GDPR Articles 5, 24, 25; EU AI Act Article 9; ICO AI Auditing Framework; SRA standards; UK Equality Act 2010 (must include a clause prohibiting reliance on AI outputs that reflect protected-characteristic bias).

ACTION 2 — IMMEDIATE (overdue): Update client-facing privacy notice and engagement letter to include (a) disclosure that AI tools may be used to assist with drafting correspondence and summarising documents; (b) identification of the tools by category; (c) confirmation that all AI outputs are reviewed by a qualified solicitor; and (d) the Article 50 EU AI Act disclosure in plain English for EU-resident clients. Satisfies: UK GDPR Articles 13–14; EU GDPR Articles 13–14; EU AI Act Article 50 (in force 2 August 2026).

ACTION 3 — IMMEDIATE (overdue): Execute or verify data-processing agreements with OpenAI (ChatGPT), Microsoft (Copilot), and LexisNexis (Lexis+ AI). Each agreement must include all Article 28 mandatory clauses. For EU-resident client data, verify that EU Standard Contractual Clauses are in place. For UK-origin data, verify that an International Data Transfer Agreement is in place. Satisfies: UK GDPR Article 28 (IDTA); EU GDPR Article 28 (SCCs).

ACTION 4 — WITHIN 30 DAYS: Produce a Legitimate Interests Assessment documenting the lawful basis for processing client personal data via AI tools. The assessment must identify the processing purpose, the necessity test, and the balancing test, having particular regard to the sensitivity of conveyancing, family and probate matter data and to legal professional privilege. Satisfies: UK GDPR Article 6(1)(f); EU GDPR Article 6(1)(f).

ACTION 5 — WITHIN 30 DAYS: Update the firm's Record of Processing Activities to include each AI-assisted activity (drafting correspondence, summarising documents, research and analysis), the tools used, the categories of data processed, the retention periods, and the third-country transfer safeguards. Satisfies: UK GDPR Article 30; EU GDPR Article 30.

ACTION 6 — WITHIN 30 DAYS: Produce a documented AI Risk Register covering ChatGPT, Microsoft Copilot, and Lexis+ AI. The register must identify: the data inputs used with each tool; the risk that client-confidential or privileged information is retained, used for model training, or disclosed to third parties; the controls applied (data minimisation, DPAs, oversight protocols); and residual risk ratings. The register must be reviewed annually and on any material change to the firm's AI use cases. Satisfies: EU AI Act Article 9; ICO AI Auditing Framework.

ACTION 7 — WITHIN 30 DAYS: Establish a documented DUAA-compliant data-protection complaints procedure, including defined response time limits, and communicate it to data subjects in the privacy notice. This is a UK-specific obligation (DUAA complaints duty, in force 19 June 2026). Satisfies: DUAA Part 5.

ACTION 8 — WITHIN 60 DAYS: Deliver mandatory AI training to all fee earners and support staff. Training must cover: the approved tools and the prohibition on unapproved tools; the prohibition on entering client-identifiable data without a confirmed lawful basis; the requirement to verify all AI outputs; confidentiality and privilege risks; and the professional conduct consequences of unverified AI use (citing the Pinsent Masons case as a live example). Training completion must be recorded. Satisfies: UK GDPR Article 39 (if a DPO is appointed); EU GDPR Article 39; SRA obligations; EU AI Act Article 9 (human oversight).

ACTION 9 — BEFORE 2 DECEMBER 2026: Prepare for EU AI Act Article 50(2) machine-readable marking requirements for synthetic content. This obligation enters force on 2 December 2026. By that date, any AI-generated documents shared with EU-resident clients must carry machine-readable markings. No equivalent UK statutory obligation currently exists. The firm must review what its vendors (OpenAI, Microsoft, LexisNexis) will provide by way of automated marking and document the approach before the deadline.

ACTION 10 — ONGOING: Maintain a regulatory contact log identifying the ICO (data-protection complaints and breach reporting for UK-origin data), the SRA (professional conduct), and the relevant EU national supervisory authority for each EU-resident client's Member State. Review and update the log whenever the firm takes on EU-resident clients in a new Member State. Satisfies: UK GDPR Article 33; EU GDPR Article 33; EU AI Act deployer obligations.

ACTION 11 — ONGOING: Conduct an annual review of EU AI Act Annex III high-risk categories to confirm that the firm's AI use cases remain outside the high-risk classification. The Annex III compliance deadline is 2 December 2027. If any use case moves into a high-risk category before that date, preparatory work must begin immediately,

as the requirements (conformity assessment, technical documentation, human oversight systems) are substantial.

9. Obligations That Do Not Apply — Stated with Reasons

UK GDPR Article 22 and DUAA automated-decision-making safeguards. The firm has confirmed it does not use AI to make decisions about people. Article 22 is therefore not engaged at this date. If the firm adopts AI-assisted case-outcome prediction, client-risk scoring, or similar functions, this assessment must be revisited immediately.

EU AI Act Annex III high-risk obligations (compliance deadline 2 December 2027). The firm's declared uses — drafting correspondence, summarising documents, legal research — do not fall within the Annex III high-risk categories as they do not involve AI making or substantially influencing decisions about individuals in education, employment, essential services, law enforcement, migration, or administration of justice. These obligations do not currently apply. The position must be reviewed annually.

EU AI Act Annex I high-risk obligations (compliance deadline 2 August 2028). These apply to AI embedded in products covered by EU product-safety law. The firm's AI tools are software services, not safety-regulated products. These obligations do not apply.

GPAI provider obligations. ChatGPT, Copilot, and Lexis+ AI are provided by third parties. The GPAI obligations in the EU AI Act fall on providers (OpenAI, Microsoft, LexisNexis), not on deployers. Halstead & Rowe's obligation is limited to vendor due diligence confirming provider compliance, which is addressed in Action 3 above.

EU AI Act Article 5 prohibited practices. None of the firm's declared AI uses constitutes a prohibited practice (subliminal manipulation, exploitation of vulnerabilities, social scoring, real-time remote biometric identification, or prohibited emotion recognition). This assessment stands unless the firm's use cases change.

AI Supply Chain Risk Review

The risk that arrives through your vendors — including the vendors your vendors use.

Document Information

Document title: AI Supply Chain Risk Review. Prepared for: Halstead & Rowe Solicitors. Date: 08 August 2026. Prepared by: AI Compliance Consultancy. Classification: Confidential — Legal Privilege Claimed. This document forms part of the UK + EU Combined Compliance Framework for Halstead & Rowe Solicitors and should be retained on the firm's compliance file. It covers the three AI tools currently in use — ChatGPT (OpenAI), Microsoft Copilot, and Lexis+ AI — and the vendor supply chains behind them. It applies UK GDPR, the Data (Use and Access) Act 2025 (DUAA), the ICO AI Auditing Framework, EU GDPR, and the EU AI Act 2024/1689 in the versions current as at the document date.

1. Vendor Profiles — What Each Tool Is, Where It Sits, and What It Holds

ChatGPT is a large language model service provided by OpenAI, Inc., a Delaware-incorporated company. Halstead & Rowe fee earners are using it to draft client correspondence and summarise case documents. When a fee earner pastes text into a ChatGPT session, that text is transmitted to OpenAI's servers and processed there. Conveyancing, family, and probate files contain names, addresses, financial details, family circumstances, and other special-category or highly sensitive personal data. If any such content enters a ChatGPT prompt, OpenAI becomes a processor of personal data belonging to the firm's clients, including EU-resident clients. The firm does not currently have a data processing agreement (DPA) in place with OpenAI governing this processing, and fee earners are using consumer-grade ChatGPT accounts rather than the API or ChatGPT Enterprise, which carry different contractual and data-handling terms.

Microsoft Copilot is integrated into Microsoft 365 and provides AI-assisted drafting, summarisation, and research within Word, Outlook, Teams, and other applications. Microsoft Corporation is the provider; its European data-centre infrastructure means that, for business Microsoft 365 tenants, personal data is typically processed within the EEA or UK. However, this depends on the specific Microsoft 365 licence tier held by the firm. Copilot for Microsoft 365 (the commercial product) is governed by the Microsoft Products and Services Data Processing Agreement and the Microsoft EU Data Boundary commitments. The firm must confirm which Copilot product it holds and whether that DPA has been executed, because the consumer Copilot experience carries different terms. Any document the firm opens or drafts whilst Copilot is active may pass content to Microsoft's AI inference layer.

Lexis+ AI is the AI-enhanced research and drafting platform provided by LexisNexis, a division of RELX Group plc, incorporated in the UK. It is a purpose-built legal research tool and operates under LexisNexis's standard professional services terms and DPA. Because it is designed for law firms, it has explicit provisions on client confidentiality and does not use customer content to train its underlying models without consent. Lexis+ AI draws on LexisNexis's curated legal content. Personal data entered into research queries — for example, a client's name used as a search parameter — may nonetheless be processed on LexisNexis servers. The firm should confirm the current version of the DPA applicable to its subscription.

2. Sub-Processors — Disclosed Chains Behind Each Vendor

OpenAI publishes a sub-processor list for its API and Enterprise products, which includes cloud infrastructure providers (primarily Microsoft Azure) and specialist support vendors. However, the consumer ChatGPT product used by Halstead & Rowe fee earners without enterprise accounts does not carry the same contractual sub-processor disclosure obligations. This means the firm currently cannot confirm which sub-processors handle data entered into those sessions, cannot carry out the supply-chain due diligence required under UK GDPR Article 28 and EU GDPR Article 28, and cannot provide clients with accurate Records of Processing Activity (ROPA) entries. This is a material compliance gap. Switching to ChatGPT Enterprise or the OpenAI API with a signed DPA would bring sub-processor disclosure into scope.

Microsoft publishes a comprehensive sub-processor list for its online services at the Microsoft Trust Centre. For Microsoft 365 Copilot, sub-processors include Microsoft affiliates operating Azure, and a defined list of third-party support providers. Transfers outside the UK or EEA are covered by Microsoft's Standard Contractual Clauses (SCCs) and, for UK transfers, the International Data Transfer Agreement (IDTA). The firm should download and retain the version of this list current at the date of each annual DPA review, as it is subject to change with 30 days' notice under Microsoft's terms.

LexisNexis discloses sub-processors as part of its enterprise DPA. RELX Group operates data centres in the UK and EEA, and sub-processors are disclosed on request under the subscription agreement. The firm's account manager should be asked to provide the current list in writing so it can be appended to the firm's ROPA. LexisNexis has confirmed in its published documentation that it does not use customer content to train its AI models, but this representation should be captured contractually in the executed DPA.

3. Contractual Position — DPA, Model-Training Terms, Liability Cap, Exit and Data Return

OpenAI (ChatGPT — consumer accounts): No DPA is in place. Consumer terms of service do not constitute a data processing agreement compliant with UK GDPR Article 28 or EU GDPR Article 28. OpenAI's consumer terms permit the use of inputs to improve its models unless the user opts out; this opt-out is not automatic and there is no evidence the firm has activated it. Liability under consumer terms is capped at amounts that are not calibrated to the value of a professional services relationship. There is no contractual right to data return or deletion on exit. This position is incompatible with the firm's obligations as a UK GDPR and EU GDPR controller. Action required: either migrate immediately to ChatGPT Enterprise with a signed DPA and model-training exclusion, or prohibit use of ChatGPT for any matter-related content until that migration is complete.

Microsoft Copilot: Microsoft's commercial DPA is comprehensive and GDPR-compliant for business customers. It excludes customer data from model training by default for Microsoft 365 Copilot. Liability caps apply per the Microsoft Customer Agreement or Enterprise Agreement; the firm should check whether those caps are proportionate to the value of the matters processed. On termination, Microsoft commits to deletion or return of customer data within 180 days, subject to the applicable service terms. The firm must confirm it holds a business or enterprise Microsoft 365 licence — not a personal or family licence — to ensure these terms apply.

Lexis+ AI (LexisNexis): A professional services DPA should be in place as part of the subscription agreement. LexisNexis states publicly that customer content is not used to train its models. Liability provisions in LexisNexis enterprise contracts are typically capped at 12 months' subscription fees; this should be reviewed in light of the potential value of matters affected by a data breach or AI error. On exit, the firm's data held on the LexisNexis platform — search history, saved research, uploaded documents — should be exportable and deletable. The firm should confirm the data return mechanism in writing before the next renewal.

Regulatory note: Under UK GDPR Article 28(3) and EU GDPR Article 28(3), a controller must only use processors that provide sufficient guarantees and must have a written contract specifying the subject matter, duration, nature and purpose of the processing, and the obligations and rights of the controller. The absence of any such agreement with OpenAI for consumer ChatGPT use is a direct breach of both regimes today.

4. Concentration Risk — Multiple Tools Resolving to One Provider

A concentration risk exists where two or more of the firm's AI tools share the same underlying infrastructure provider, meaning that a failure, regulatory action, or contractual change affecting that provider would disable several workflows simultaneously. In Halstead & Rowe's supply chain, both ChatGPT (OpenAI) and Microsoft Copilot share a significant dependency on Microsoft Azure. OpenAI's infrastructure is substantially hosted on Azure under its long-standing partnership with Microsoft. Microsoft Copilot itself runs on Azure. This means the firm's AI drafting and summarisation capability — which spans all three practice areas of conveyancing, family, and probate — is effectively dependent on the continued availability and compliance of a single cloud infrastructure provider.

If Azure suffered a major outage, if Microsoft amended its terms in a way incompatible with the firm's legal obligations, or if an ICO or EU AI Office enforcement action required the firm to suspend processing on Azure, the firm could lose access to two of its three AI tools simultaneously. LexisNexis also uses cloud infrastructure but its architecture is separate from Azure's dominance in this chain, providing some diversification.

The firm should document this dependency in its risk register and ensure that its business continuity plan (addressed separately in the Incident Response document) includes a manual fallback for AI-assisted drafting and research that does not assume any single cloud provider is available.

5. Vendor Failure or Withdrawal — Continuity Position

OpenAI is a privately held company subject to significant investor and regulatory pressure. It has faced regulatory action in multiple EU member states, including the Italian Garante's earlier investigation into ChatGPT (the resulting fine was subsequently annulled by a Rome court in March 2026 on procedural grounds, but the regulatory scrutiny has not abated). A regulator in any EU member state could suspend access to ChatGPT within that jurisdiction with relatively short notice. Given that Halstead & Rowe acts for EU-resident clients and processes their data through these tools, such a suspension would have direct operational consequences. The firm should not treat ChatGPT as a permanent fixture and should maintain the capability to operate without it.

Microsoft is a large listed company and Copilot is integrated into its core enterprise product suite. The risk of abrupt withdrawal is lower than for OpenAI, but Microsoft has in the past altered Copilot features and pricing with moderate notice periods. Changes to Microsoft's EU Data Boundary commitments or UK data transfer arrangements following any future shifts in the adequacy landscape could also require the firm to reassess use. The firm's dependency on Microsoft for email, document management, and now AI means that any significant Microsoft contractual change has a disproportionate impact.

LexisNexis is the most stable vendor in this chain; RELX Group is a major listed company with deep roots in the legal market, and Lexis+ AI is a core product line. The risk of abrupt withdrawal is low. However, the firm should ensure its subscription agreement includes provisions on data return if it changes provider, and should not store irreplaceable research outputs solely within the Lexis+ AI environment.

Continuity action: The firm must be able to draft correspondence, summarise documents, and conduct legal research using only human resources and traditional databases at short notice. Fee earners should not become operationally dependent on AI tools to the point where their removal would cause service failure or client harm.

6. Regulatory Obligations Triggered by the Supply Chain

UK position: Under UK GDPR Article 28, every processor used by the firm must be subject to a written contract. Under the DUAA (most Part 5 provisions in force from 5 February 2026), the firm must maintain an updated ROPA reflecting all processors and sub-processors. The ICO AI Auditing Framework requires the firm to be able to demonstrate visibility of its AI supply chain, including the data flows into and out of each tool. The ICO's fine ceiling is £17,500,000 or 4% of global annual turnover, whichever is higher; the turnover-based limb cannot be computed without the firm's figures.

EU position: EU GDPR Article 28 imposes the same processor contract requirement for personal data of EU-resident clients. The EU AI Act 2024/1689 Article 13 (transparency) and Article 50 (transparency duties, now in force as of 2 August 2026) require that the firm, as a deployer, ensures clients are informed when AI systems are used in ways that affect them. Article 9 risk management obligations apply to higher-risk use cases. General-purpose AI model (GPAI) rules under the Act have applied since 2 August 2025, meaning OpenAI and Microsoft as providers of GPAI-based tools have obligations that the firm should verify have been met before deploying those tools on EU-resident client matters. High-risk Annex III obligations do not yet apply (deadline deferred to 2 December 2027 following the Digital Omnibus adopted on 29 June 2026), but the firm should monitor this, as AI used in legal proceedings could attract that classification in future. The EU AI Act fine ceiling is €35,000,000 or 7% of global annual turnover.

Article 5 prohibited practices: The firm does not use AI for social scoring, real-time biometric surveillance, subliminal manipulation, or any other prohibited practice listed in Article 5. Article 5 is therefore not directly engaged by the declared use cases, and prohibition compliance is not a current gap. However, the firm should note that new prohibitions come into force on 2 December 2026 and should review its use cases against those additions before that date.

Cross-jurisdiction divergence on processor contracts: The substantive requirements of UK GDPR Article 28 and EU GDPR Article 28 are materially identical. One compliant DPA with appropriate addenda covering both UK and EU processing satisfies both regimes. Where they diverge, the transfer mechanism differs: international transfers from EU-based processing require EU SCCs; transfers from UK-based processing require IDTAs or equivalent. Both must be in place where data moves across both jurisdictions, as it does when EU-resident client data is processed by OpenAI or Microsoft infrastructure.

7. Supplier Due-Diligence Questionnaire

The following questionnaire must be completed by any new AI tool vendor before the firm enters into a subscription or licence, and must be re-sent to existing vendors at each annual review. Responses must be obtained in writing and retained on the compliance file.

Section A — Corporate and Regulatory Standing. (1) Provide the full legal name, jurisdiction of incorporation, and registered address of the contracting entity. (2) Identify all group companies or affiliates that will process personal data under this contract. (3) Are you currently subject to any regulatory investigation, enforcement action, or court order in any jurisdiction relating to data protection or AI? If yes, provide details. (4) Have you received any fine or sanction from a data protection authority or AI regulator in the past three years? If yes, provide details including the outcome and remediation taken.

Section B — Data Processing and Sub-Processors. (5) Provide a current, complete list of all sub-processors that will process personal data supplied by Halstead & Rowe, including their name, location, and function. (6) What notice period do you give before adding or replacing a sub-processor, and what is the mechanism for objection? (7) Where are personal data stored and processed — specify all countries and data-centre locations. (8) What international transfer mechanisms are in place for transfers outside the UK and EEA (specify IDTA, SCCs, or adequacy reliance as applicable)?

Section C — Model Training and Data Use. (9) Does your system use customer inputs, prompts, or uploaded documents to train, fine-tune, or improve your AI models? If yes, describe the scope and the opt-out mechanism. (10) Is the opt-out from model training the default position for business customers, or must it be actively selected? (11) What retention period applies to customer inputs after a session ends, and when are they deleted from inference logs and training pipelines?

Section D — Contractual Protections. (12) Do you offer a data processing agreement compliant with UK GDPR Article 28 and EU GDPR Article 28? Provide the current version. (13) What is the liability cap under your standard terms, and does it apply to data breaches caused by your sub-processors? (14) On termination of the contract, what data return and deletion process applies, and within what timeframe? (15) What audit rights does the firm have under your DPA, and do you accept third-party audit reports in lieu of direct audit?

Section E — AI Act Compliance. (16) How do you classify your system under the EU AI Act 2024/1689 — is it a general-purpose AI model, a high-risk system, or neither? Provide your written classification rationale. (17) Have you complied with the GPAI obligations in force since 2 August 2025, including transparency and copyright compliance documentation? (18) Do you comply with Article 50 transparency duties (in force 2 August 2026) by disclosing to users when they are interacting with an AI system? (19) What technical and organisational measures do you apply to support human oversight of AI outputs, consistent with Article 9 risk management principles?

Section F — Security and Incident Response. (20) Provide your current ISO 27001 or equivalent certification, or describe your information security framework. (21) What is your contractual notification period following a personal data breach that affects Halstead & Rowe client data, and does it comply with the 72-hour notification window under UK GDPR Article 33 and EU GDPR Article 33? (22) Describe your business continuity and disaster recovery arrangements for the service, including target recovery time and recovery point objectives.

8. Immediate Actions Required

The following actions are required now, in priority order, based on the risks identified in this review.

First, prohibit fee earners from entering any client-specific personal data — including names, addresses, matter references, or case details — into consumer-grade ChatGPT accounts with immediate effect. This prohibition must be communicated in writing to all fee earners and support staff, and must be recorded in the firm's breach-prevention log. This is necessary to stop an ongoing breach of UK GDPR Article 28 and EU GDPR Article 28.

Second, either procure ChatGPT Enterprise with a signed DPA and model-training exclusion, or remove ChatGPT from the approved tool list entirely. The decision must be made and implemented within 30 days. If ChatGPT Enterprise is procured, obtain the sub-processor list and execute the DPA before any client data is processed.

Third, confirm the Microsoft 365 licence tier held by the firm and obtain the current version of the Microsoft Products and Services DPA. Confirm that Copilot for Microsoft 365 (commercial) is the product in use, not the consumer Copilot experience, and that the EU Data Boundary commitment applies to the firm's tenant.

Fourth, contact the LexisNexis account manager and request the current DPA and sub-processor list in writing. Confirm contractually that customer content is excluded from model training and document that confirmation on file.

Fifth, send the supplier due-diligence questionnaire in Section 7 of this document to OpenAI (if retaining ChatGPT Enterprise), Microsoft, and LexisNexis within 60 days, and record responses on the compliance file.

Sixth, update the firm's ROPA to reflect all three AI tools, their sub-processors, and the international transfer mechanisms relied upon, consistent with DUAA Part 5 obligations in force from 5 February 2026 and EU GDPR Article 30.

Seventh, review all three vendor contracts annually, re-issue the due-diligence questionnaire, and re-download current sub-processor lists. Mark the next review date in the firm's compliance calendar as August 2027.