

Disclaimer. This is a template, not legal advice. It does not create a lawyer–client relationship. Before adopting it:

- adapt it to your jurisdiction(s), professional rules and client instructions;
- apply any court or regulator guidance that binds you;
- have it reviewed by qualified counsel.

Last reviewed: [date].

[FIRM / LEGAL DEPARTMENT NAME]: Policy on the Use of Artificial Intelligence

Version [x.x] · Approved by [body] on [date] · Owner: [AI Governance Lead] · Next review: [date]

1. Purpose and scope

1.1 This Policy sets the rules for using artificial intelligence (AI), including generative AI, in work done by or for [Firm/Department]. Its purpose is to:

- (a) protect client confidentiality and legal privilege;
- (b) keep our work accurate;
- (c) meet our duties to clients, courts and regulators.

1.2 It applies to [all partners, lawyers, trainees, paralegals, support staff, secondees, contractors and consultants] ("Users"), on any device, whenever they work on [Firm/Department] matters or handle [Firm/Department] or client information.

1.3 It covers all AI tools: tools licensed by us, AI features built into software we already use ([email, word processing, document management, e-discovery]), and publicly available tools.

1.4 This Policy adds to, and does not replace, our professional obligations. These include [the applicable code(s) of conduct, e.g. the Mandatory Code of Conduct for Legal Practitioners in the DIFC Courts; the applicable advocacy law and bar rules], data protection law, and the practice directions of the courts before which we appear. Where there is a conflict, the law, rule or court direction prevails.

2. Definitions

- **AI tool:** software that produces content, predictions, recommendations or decisions from inputs with a degree of autonomy. This includes chat assistants and tools for drafting, summarisation, translation, transcription, research and review.
- **Generative AI:** AI that generates new text, images, audio, video or code in response to a prompt.
- **Approved Tool:** an AI tool listed in Annex A after the review in Section 7.

- **Public Tool:** an AI tool used under consumer or standard online terms that [Firm/Department] has not contracted for and reviewed.
- **Input:** anything entered into or uploaded to an AI tool. **Output:** anything an AI tool produces.
- **Client Information:** all information relating to a client or matter, however obtained, including the fact that a matter exists.
- **Privileged Material:** material protected by legal professional privilege or professional secrecy under applicable law.
- **Personal Data:** as defined in the data protection law applicable to the processing.
- **Hallucination:** Output that appears plausible but is false, invented or unsupported, e.g. a non-existent case or statutory provision.

3. Approved and prohibited tools (acceptable use)

3.1 Users may use only Approved Tools for work, and only within the data classes allowed for each tool (Annex A and Section 4).

3.2 Prohibited without exception:

- (a) entering Client Information, Privileged Material or Personal Data into a Public Tool;
- (b) using AI to fabricate, alter or "enhance" evidence, or to draft a witness's evidence other than in the witness's own words;
- (c) presenting AI Output to a court, tribunal, regulator, client or counterparty without the human verification in Section 5;
- (d) using AI to make a final legal decision or give final advice without lawyer review;
- (e) running AI tools on work data through personal accounts or devices [unless approved under the BYOD policy];
- (f) circumventing tool settings fixed by [IT/Knowledge team], including re-enabling chat history or model training;
- (g) [using AI note-takers or recorders in client meetings or hearings without the consent of all participants].

3.3 **Permitted with an Approved Tool**, subject to Sections 4 and 5: [first drafts; document summaries; Arabic-English translation; clause extraction and comparison; legal research assistance; e-discovery and document review; proofreading; internal knowledge search].

3.4 Requests to approve a new tool go to [AI Governance Lead] using Annex B.

4. Confidentiality and client-data classification

4.1 Before using any AI tool, Users must classify the information they intend to input and follow this table:

Class	Examples	Public Tool	Approved general-purpose tool (enterprise terms, no training on our data)	Approved legal tool with [in-country hosting / approved region] and matter-level access controls
1. Public	Published laws and judgments, public news, our published articles	✓ Allowed	✓ Allowed	✓ Allowed
2. Internal	Firm know-how, templates with no client data, training material	✗ Not allowed	✓ Allowed	✓ Allowed
3. Client confidential	Client documents, correspondence, contracts, matter facts, client identity	✗ Not allowed	[✗ / ✓ only if anonymised under 4.3]	✓ Allowed [subject to client terms, 4.4]
4. Highly sensitive / privileged	Privileged advice, litigation strategy, sensitive personal data (health, criminal, children), government or [critical-infrastructure] client data	✗ Not allowed	✗ Not allowed	[✓ only with written client consent and [Partner/GC] approval / ✗ never]
5. Restricted by law or order	Data under a court confidentiality or sealing order; data a client contract says may not leave [country]; classified government data	✗ Not allowed	✗ Not allowed	✗ unless the order, contract or law expressly allows it

4.2 When in doubt, treat information as the higher class.

4.3 **Anonymisation:** removing names is not enough. Remove or replace every detail that could identify the client, the counterparty or the matter. Never use real client data to test or train tools or to build templates. Use fictional data.

4.4 **Client instructions prevail.** Follow any engagement terms, outside-counsel guidelines or instructions that restrict AI use or data location. [Before inputting Class 3 or 4 information, we will obtain the client's informed consent [in the engagement letter / matter by matter].]

4.5 Do not disable security settings. Chat history and model training on our data must be off wherever the tool allows it.

5. Human verification of output and citations

5.1 The User who relies on an Output is responsible for it as if they had written it. AI is a tool and carries no responsibility.

5.2 Before any Output leaves [Firm/Department] or is relied on internally, a qualified lawyer must:

- (a) check **every** case, statute, regulation and quotation against a primary source or a recognised legal database. Confirm that it exists, says what is claimed, is current, and comes from the **correct jurisdiction** (e.g. DIFC common-law authority vs onshore civil-law provisions);
- (b) check facts against the matter file;
- (c) check Arabic–English renderings of legal terms against the authoritative-language text;
- (d) check for bias, omissions and over-confident conclusions.

5.3 Witness statements and affidavits must reflect the witness's own words and knowledge. AI may help only with format and language. The witness must confirm the content before signing any statement of truth.

5.4 Record the verification in the matter file [with the Annex C checklist / with the note "AI-assisted; verified by [initials] on [date]"].

5.5 Supervisors remain responsible for the AI-assisted work of the people they supervise.

6. Disclosure to clients and courts

6.1 **Clients.** [Our engagement terms tell clients that we may use Approved AI Tools and how we protect their information.] We follow any client instruction not to use AI. [We do not bill clients for time spent learning AI tools.]

6.2 **Courts and tribunals.** Follow each forum's rules:

(a) **DIFC Courts** (PGN 2/2023):

- declare the use, or intended use, of AI-generated content at the earliest opportunity;
- raise it with the other side and resolve any issues no later than the Case Management Conference;
- keep the client informed and obtain their consent to using generative AI material in submissions.

(b) **QFC Court and Regulatory Tribunal** (QICDRC PD 1/2026):

- no pre-emptive declaration is required unless the Court asks;
- be ready to identify AI-generated portions and explain how they were verified;
- always disclose AI-generated or AI-enhanced multimedia evidence.

(c) **Other courts, tribunals and arbitrations:** follow any applicable direction. Where there is none, [disclose material AI use where fairness requires it / refer to the supervising partner].

6.3 [Litigation Lead] keeps a forum register (Annex D) and updates it [quarterly].

7. Data residency and vendor due diligence

7.1 No AI tool may be approved until [AI Governance Lead], with [IT Security] and [DPO/Legal], has completed the Annex B questionnaire. It covers at least:

- (a) where Inputs, Outputs, logs and backups are stored and processed, and from which countries staff or sub-processors can **access** them;
- (b) whether Inputs or Outputs train or improve models, and whether that is contractually excluded;
- (c) the underlying model providers and sub-processors;
- (d) retention and deletion, including deletion when a matter closes;
- (e) encryption, access controls (SSO, matter-level permissions) and exportable audit logs;
- (f) the cross-border transfer mechanism relied on under each relevant law;
- (g) breach-notification timelines;
- (h) handling of government and law-enforcement requests;
- (i) independent security reports (ask for the reports themselves, not logos);
- (j) Arabic-language capability, if Arabic documents will be processed.

7.2 Tools that process Class 3 or 4 data must meet the data-location requirements of [the applicable data protection laws, client contracts and sector rules]. Record them in Annex A.

7.3 Re-review each approval [annually], and whenever the vendor changes its terms, models or sub-processors.

8. Intellectual property and ownership

8.1 Do not input third-party material in breach of licence terms (e.g. [subscription database content]), and do not ask a tool to reproduce protected works.

8.2 Before approval, confirm under the vendor's terms that [Firm/Department] [and the client] own or may freely use Outputs, and that the vendor gains no rights in Inputs.

8.3 Work product created with AI assistance belongs to [Firm/client] on the same terms as other work product under [the engagement terms / employment contracts].

8.4 Do not treat Output as original work for copyright purposes without legal review. [Label published AI-generated text or images as AI-generated.]

9. Training

9.1 No User may use an Approved Tool before completing [AI induction training]. It covers this Policy, data classification, verification, hallucination risk, forum disclosure rules and tool settings.

9.2 Refresher training happens **[annually]** and after any significant change to tools or rules. **[HR / L&D]** records completion.

9.3 **[Relevant training may count towards CPD where the regulator allows.]**

10. Incident reporting

10.1 Report to **[AI Governance Lead and DPO/IT Security]** **immediately**, and in any case within **[24 hours]**, if you become aware of:

- (a) Client Information, Privileged Material or Personal Data entered into a Public Tool, or into a tool not approved for that class;
- (b) Output with a hallucinated or wrong authority that has been sent outside the firm or filed;
- (c) tool behaviour suggesting a data leak, or a vendor security notice.

10.2 **[AI Governance Lead]** decides whether clients, courts, regulators or data protection authorities must be notified, and acts within the applicable deadlines.

10.3 A good-faith report does not by itself lead to discipline. Concealment does.

11. Governance roles

Role	Responsibility
[Managing Partner / General Counsel]	Approves the Policy; accepts residual risk
[AI Governance Lead]	Owens the Policy, Annex A (tools) and Annex D (forums); runs approvals and reviews
[IT / Information Security]	Technical review; configuration (training off, logging on); access control
[DPO / Privacy Counsel]	Data protection assessment; transfer mechanisms; breach notifications
[Risk & Compliance]	Monitoring, audits, incident log
[Practice-group leads / Supervising partners]	Enforce verification and supervision
All Users	Comply, complete training, report incidents

12. Monitoring and enforcement

12.1 **[Firm/Department]** may log and audit use of Approved Tools in line with applicable law and our **[IT/privacy notice]**.

12.2 A breach may lead to disciplinary action **[up to dismissal]** and, where required, a report to regulators.

13. Review cycle

13.1 Review this Policy every [6 / 12] months. Also review it when:

- (a) a court or regulator in a forum where we practise issues AI guidance;
- (b) a significant incident occurs;
- (c) we adopt a materially new tool.

13.2 Record the version history in Annex E.

14. Annexes

- **Annex A: Approved Tools register.** Columns: Tool | Vendor | Allowed data classes | Hosting region | Training off (Y/N) | Owner | Approved | Review date.
- **Annex B: New-tool request and due-diligence questionnaire.** Use the Section 7 list.
- **Annex C: Verification checklist.**
 - ☐ every authority checked against a primary source
 - ☐ jurisdiction correct
 - ☐ quotations exact
 - ☐ facts checked against the file
 - ☐ translation checked
 - ☐ forum disclosure rule applied
 - ☐ verification recorded
- **Annex D: Forum register.** Columns: Forum | Instrument | Disclosure rule | Last checked.
Pre-filled rows:
 - DIFC Courts | PGN 2/2023 | early disclosure
 - QICDRC | PD 1/2026 | on request
 - ADGM Courts | [check current position] |
 - Onshore courts | [check current position] |
- **Annex E: Version history.**

15. Acknowledgement form

I, [full name], [job title], confirm that I have read and understood the [Firm/Department] Policy on the Use of Artificial Intelligence (version [x.x]). I agree to comply with it, and I understand that a breach may lead to disciplinary action. I completed the required training on [date].

Signature: _____ Date: _____ Staff/ID number: _____

About this template

This is a template, not legal advice. It does not create a lawyer–client relationship. Court rules, regulator guidance and laws change; check the official sources linked and have the policy reviewed by qualified counsel in each relevant jurisdiction. Last reviewed: 16 October 2026.

The text of this page and the .docx downloads are licensed under [Creative Commons Attribution 4.0 International \(CC BY 4.0\)](https://creativecommons.org/licenses/by/4.0/). You may copy, adapt and share them, including commercially, if you give attribution and say whether you made changes. The Qanu name and logo are not covered by the licence.

Suggested attribution: Adapted from the AI use policy template for GCC law firms by Qanu (<https://www.qanu.ai/en/templates/ai-use-policy-law-firms>), licensed under CC BY 4.0 (<https://creativecommons.org/licenses/by/4.0/>). **[Describe your changes.]**

Sources cited in the drafting notes

- [1] DIFC Courts, Practical Guidance Note No. 2 of 2023: Guidelines on the use of large language models and generative AI in proceedings before the DIFC Courts <https://www.difccourts.ae/rules-decisions/practice-directions/practical-guidance-note-no-2-2023-guidelines-use-large-language-models-and-generative-ai-proceedings-difc-courts>
- [2] QICDRC, Practice Direction on the Use of Artificial Intelligence (No. 1 of 2026), 6 January 2026 (PDF) <https://www.qicdrc.gov.qa/sites/default/files/regulation-pdf/2026-01/Practice%20Direction%20on%20Artificial%20Intelligence.pdf>
- [3] QICDRC, Use of Artificial Intelligence <https://www.qicdrc.gov.qa/courts/court/use-artificial-intelligence>
- [4] QICDRC news release on Practice Direction No. 1 of 2026 and the accompanying Practice Guidance, 6 January 2026 <https://www.qicdrc.gov.qa/media-center/news/qicdrc-issues-practice-direction-no-1-2026-and-practice-guidance-use-artificial>
- [5] ADGM Courts, Practice Direction 2: Commercial and Civil Claims, re-issued 17 October 2025 (PDF) <https://assets.adgm.com/download/assets/Practice%2BDirection%2B2%2B-%2BCommercial%2Band%2BCivil%2BClaims%2B-%2B17102025.pdf/5c82008e45ca11efa420ae00860b11ec>
- [6] Government of Dubai Legal Affairs Department, CLPD course listing: “Ethics – An International Comparison on the use of AI in the Legal Sector” <https://training.legal.dubai.gov.ae/ethics-an-international-comparison-on-the-use-of-ai-in-the-legal-sector/?lang=en>
- [7] SDAIA, AI Ethics Principles (English edition, PDF) <https://sdaia.gov.sa/en/SDAIA/about/Documents/ai-principles.pdf>
- [8] SDAIA, مبادئ أخلاقيات الذكاء الاصطناعي (Arabic edition, PDF) <https://sdaia.gov.sa/ar/SDAIA/about/Documents/ai-principles.pdf>
- [9] SDAIA, About AI (Arabic page) <https://sdaia.gov.sa/ar/SDAIA/about/Pages/AboutAI.aspx>
- [10] SDAIA, Generative AI Guidelines for Public, 2025, v1 (PDF) <https://sdaia.gov.sa/en/SDAIA/about/Files/GenerativeAIPublicEN.pdf>
- [11] SDAIA, Generative AI Guidelines for Government (PDF) <https://sdaia.gov.sa/en/SDAIA/about/Files/GenAIGuidelinesForGovernmentENCompressed.pdf>
- [12] UAE Government portal, The UAE Charter for the Development and Use of Artificial Intelligence (July 2024) <https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/policies/Ai/The-UAE-Charter-for-the-Development-and-Use-of-Artificial-Intelligence>
- [13] Solicitors Regulation Authority (England and Wales), Misuse of AI warning notice, 17 August 2026 <https://www.sra.org.uk/solicitors/guidance/misuse-ai>

- [14] The Law Society (England and Wales), Generative AI – the essentials, updated 30 June 2026
<https://www.lawsociety.org.uk/topics/ai-and-lawtech/generative-ai-the-essentials>
- [15] American Bar Association, news release on Formal Opinion 512, 29 July 2024
<https://www.americanbar.org/news/abanews/aba-news-archives/2024/07/aba-issues-first-ethics-guidance-ai-tools>
- [16] American Bar Association, Formal Opinion 512 (PDF)
https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-opinion-512.pdf
- [17] CCBE, Guide on the use of generative AI by lawyers, 2 October 2025 (PDF)
https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Guides_recommendations/EN_ITL_20251002_CCBE-guide-on-the-use-of-the-use-of-generative-AI-for-lawyers.pdf
- [18] CCBE, Technical guide on the use of AI tools and models by lawyers, 27 March 2026 (PDF, not reviewed for this page) https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Guides_recommendations/EN_ITL_20260327_CCBE-technical-guide-on-the-use-of-AI-tools-and-models-by-lawyers.pdf
- [19] EU AI Act, Article 4: AI literacy (unofficial reader of Regulation (EU) 2024/1689)
<https://artificialintelligenceact.eu/article/4/>
- [20] EUR-Lex, OJ L 2026/1744 of 24 July 2026, amending Regulation (EU) 2024/1689 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202601744
- [21] EU AI Act, Annex III: high-risk AI systems (unofficial reader) <https://artificialintelligenceact.eu/annex/3/>