GUIDANCE NOTE ON
THE USE OF LAWTECH IN LEGAL PRACTICE

A. PURPOSE

1. This Guidance Note[1] seeks to promote the responsible, secure, and ethical use of LawTech by legal professionals (for present purpose, including but not limited to their agents, members, or employees) in their professional practice. It provides some key principles and practical guidance to assist legal professionals to harness LawTech's benefits while safeguarding against the possible risks associated with the use of LawTech and upholding their fundamental professional duties.

2. This Guidance Note is intended for general reference. While it is not legally binding and is not intended to be exhaustive, it provides highly relevant reference material and practical support for legal professionals to draw upon when adopting LawTech in their practice. Legal professionals are strongly encouraged to follow this Guidance Note. However, following this Guidance Note does not relieve legal professionals of any professional, legal or regulatory obligations, nor does it absolve them of liability for any breach of those obligations.

3. Legal professionals must comply with the applicable codes and regulations of professional conduct, and remain solely responsible for conducting their own independent assessments, management of the usage of the LawTech tools and compliance checks in accordance with the needs of their specific practice.

---

[1] This Guidance Note has been formulated to incorporate comments and suggestions from the legal professional bodies, the Department of Justice's Consultation Group on LawTech Development, other experts and stakeholders.

B. LAWTECH

4. LawTech covers technologies powered by artificial intelligence ("**AI**"), generative AI or agentic AI, cloud technology and other technologies used in the context of legal practice. LawTech may assist, support, or automate legal or dispute resolution services and processes.

5. Use of LawTech may increase efficiency, quality and cost-effectiveness of the delivery of legal and dispute resolution services and hence access to justice. At the same time, LawTech also carries risks, including inaccurate, biased, or fabricated outputs, breaches of legal professional privilege and confidentiality, data leakage and diminished professional oversight, etc., if not selected, implemented or deployed properly.

C. OVERARCHING PRINCIPLE

6. LawTech does not exonerate the accountability of legal professionals who remain fully accountable for their professional work, and their duties to the court and to clients remain undiminished irrespective of whether LawTech is adopted. Reliance on LawTech, or any failure or error attributable to LawTech, does not relieve legal professionals of their duties, excuse any breach, or diminish any professional liability.

D. PRINCIPLES FOR USE OF LAWTECH

(1) Choose Suitable LawTech Tools

7. Choosing suitable LawTech tools is important because the needs and practice of different members of the legal sector differ. Optimising the deployment of LawTech requires a systematic approach

which begins with aligning specific needs (both technical and operational) with corresponding service provider(s).

8. Legal professionals should focus on their own specific needs. Adoption of a LawTech tool by their fellow professionals is not a guaranteed indicator of suitability. What works well for others may not fit one's own specific practice and work environment.

9. A practical and independent evaluation of a LawTech tool's capabilities, limitations and risks, and a thorough understanding of how the tool manages specific assignments, are important for users to ensure its suitability, review its output and assess its overall performance.

(2) Beware of Risks Associated with Shadow AI

10. Legal professionals should be alerted to the use of "shadow AI". It refers to the unauthorised use of AI/LawTech tools by members, agents or employees of a firm or an organisation for work purposes without the firm's or organisation's knowledge or approval. This may create unmanaged risks.

11. Legal professionals are recommended to conduct regular compliance audits of use of LawTech tools to identify unauthorised use and bring the same under their governance framework. Such oversight measures may include monitoring access to browser-based tools or periodic staff declarations.

12. Transparent guidelines and regular training on authorised implementation of AI or LawTech tools are conducive to mitigating such risks and fostering effective adoption and responsible use of LawTech.

(3) Understand Parameters and Risks of LawTech

13. LawTech, including AI, has limitations and may generate risks, such as inaccurate, outdated, misleading or biased outputs, fabricated

information resulting from hallucination and sycophantic outputs that favour user assumptions. Notwithstanding safeguards, for example, grounding, validation or retrieval-augmented generation, such risks cannot be completely eradicated. Legal professionals must be aware of these limitations and critically evaluate and verify the outputs generated.

14. LawTech involves the use of emerging and fast-evolving technology. It is vital for legal professionals to constantly undertake risk and impact assessments of the use of LawTech in professional practice and maintain a proportionate yet robust governance framework to mitigate risks arising from the use of LawTech.

(4) Uphold Professional Responsibilities

Professional judgment and accountability cannot be substituted

15. The fundamental principle is that professional obligations do not change whether legal professionals use LawTech. LawTech is an aid, not a substitute for professional judgment and accountability.

16. Legal professionals remain fully accountable for the professional work rendered to their clients and their duty to the court, regardless of whether LawTech is involved. Competence of legal professionals includes, in appropriate circumstances, considering whether LawTech tools should be used and if so, how and for what purpose, with a clear understanding of the capabilities, limitations and risks of the LawTech tools chosen.

Due assessment for each relevant task

17. When evaluating whether to use LawTech for a particular task, legal professionals may consider the following factors:

(a) The nature of the task (e.g. whether it is repetitive or high-volume);

(b) The level of risks associated (e.g. high-stakes tasks like court submissions would demand utmost caution, and the sensitivity of the information involved);

(c) The applicable regulatory framework (e.g. contractual or legal restrictions on the use of LawTech); and

(d) Whether the outputs by LawTech tools can be meaningfully and thoroughly reviewed and verified (e.g. the level of human oversight required).

Human oversight is of paramount importance

18. Legal professionals should ensure that outputs generated by LawTech tools as well as legal advice or work derived from any degree of reliance on such tools, are subject to reasonable and necessary human review to confirm that they are authentic, legally sound and contextually appropriate for the matters at hand. Such review should also involve reasonable steps to confirm the underlying source, reference or basis and that the outputs do not involve plagiarism or infringe any intellectual property or proprietary rights. For example, a legal professional should not cite any authority unless he/she has independently verified it against the primary sources.

19. Legal professionals should implement an appropriate system of proper oversight, reliable processes, risk assessments and effective safeguards to ensure commensurate management of risks, and that LawTech is used responsibly and ethically without undermining professional responsibilities.

(5) Comply with Legal and Regulatory Requirements

20. Legal professionals should ensure that all relevant laws, regulations, codes of conduct, practice directions, etc. are complied with when using LawTech. It is the legal professionals' duty to maintain a

clear and thorough understanding of the prevailing legal and regulatory framework in relation to the use of LawTech.

21. Different forums and jurisdictions may have different requirements. Legal professionals should check the specific practice directions or guidelines of the relevant court or tribunal as applicable.

(6) Uphold Confidentiality and Data Security

22. Prior to deployment, legal professionals should conduct commensurate risk assessments on LawTech tools, in particular AI agents, to evaluate their operating environment, access permissions and action boundaries, log maintenance and controls for human intervention. This ensures a reasonable level of data security, controllability and traceability while enabling human accountability.

23. Legal professionals should carefully consider the appropriate level of permissions and controls for access to LawTech tools and should constantly maintain oversight over them. Commensurate measures, including human oversight, contingency plans and mitigation measures, should be put in place to monitor data workflows, ensuring that unauthorised or unintended access is promptly revoked, breaches are contained and data is safeguarded.

24. Legal professionals must take all reasonable precautions to keep all client information confidential when using LawTech. As inputting sensitive or personally identifiable information into LawTech tools can result in data leakage or data being used for model training, legal professionals should give due regard to whether such input may compromise confidentiality requirements, undermine clients' right to legal professional privilege, or infringe upon personal data privacy.

25. Legal professionals should put in place, among others, the following to provide sufficient safeguards for confidentiality and detailed guidance for reporting misuse and mitigation measures:

(a) Security measures which satisfy prevailing standards on, for example, security operations, data encryption and data residency protocols;

(b) Guidelines for review of instructions to LawTech tools and cross-border transfer of data to ensure alignment with the prevailing personal data protection framework;

(c) Regular compliance audits of use of LawTech tools; and/or

(d) Internal governance and policies.

26. Where necessary, legal professionals may consult professionals with the requisite technical or cybersecurity expertise to review and maintain applicable security and data protection measures and policies.

27. By way of illustration, when adopting LawTech tools, legal professionals are recommended to:

(a) conduct a careful review of the terms of use and services, security specifications, in particular their privacy and data handling protocols, to ensure that they are consistent with the professional duties of the legal professionals, regardless of deployment tier or procurement model;

(b) identify how data is used, where data is stored, how it is processed and whether the LawTech tools are using users' data for model training, product improvement, secondary retention or sharing the data with third parties;

(c) assess the degree of safeguards to data security and confidentiality, and consider whether any data, document, or information that is privileged, confidential, or contains personal data, should be inputted into LawTech or AI

tools. Legal professionals should be cautious whether using publicly available, enterprise-tier or custom-built tools, as different environments may entail distinct risks;

(d) review privacy settings and consider opting out of model training as data may be retained or used for training by default; and request data deletion or refine data boundaries where appropriate or necessary; and

(e) verify that the LawTech tool and its deployment comply with the applicable data governance, privacy and cybersecurity standards.

(7) Adopt Transparency and Ethical Use

28. Legal professionals should use LawTech ethically in accordance with applicable professional conduct rules and standards.

29. Effective and transparent communication with clients regarding the use of LawTech can foster trust, clarify technical safeguards and parameters, and proactively manage client expectations. Legal professionals should duly consider whether to inform clients of the use of LawTech in delivering legal services, particularly where AI tools are used and such use is material to the legal work and carries billing or cost implications.

30. Similarly, where such tools are used to prepare submissions in respect of legal proceedings in court, legal professionals should duly consider whether to inform the relevant levels of court and other parties for transparency purpose. Legal professionals should consider the impact of the use of LawTech on their discharge of duty to the court.

E. CHECKLIST FOR USING LAWTECH IN LEGAL PRACTICE

31. To assist legal professionals in identifying the key considerations for adoption of LawTech, a template checklist is set out at the **Annex**.

F. DEVELOPMENT AND UPDATES

32. This Guidance Note may be updated from time to time to reflect technological development, emerging risks and legal market development.

33. Legal professionals should refer to and keep abreast of changes and updates in relevant laws, regulations and non-statutory guidance on the use of LawTech as promulgated by the relevant authorities and regulatory bodies from time to time.

Department of Justice
The Government of the Hong Kong Special Administrative Region
November 2026

Annex

CHECKLIST FOR USING LAWTECH IN LEGAL PRACTICE

A. Organisational Readiness	
☐	1. Have you implemented internal policies governing the approval, use, and monitoring of LawTech tools?
☐	2. Have you conducted a shadow AI audit to identify unauthorised AI use by members/agents/employees of your firm/organisation?
☐	3. Have you provided training to members/agents/employees of your firm/organisation or facilitated them to attend training on AI capabilities, limitations, risks, and ethical obligations?
☐	4. Have you established a record-keeping process sufficient to identify material AI use and the verification steps taken?
B. Selection and Procurement of LawTech Tools	
☐	5. Have you chosen a LawTech tool suited to your practice needs?
☐	6. Have you obtained sufficient information on the tool's data security and privacy protocols, including whether input data may be shared, stored, retained, or used for model training?
☐	7. Have you reviewed the product specifications and pricing to ensure they match your requirements and budget?
☐	8. Have you considered the need to run trial tests in a secure environment before expanding use to all members/agents/employees?
☐	9. If you are considering to adopt agentic AI, do you understand the scope and permissions of its autonomous action? Have you put in place mandatory human approval requirements at critical points?
C. Communication	
☐	10. Have clients imposed any restrictions or disclosure requirements regarding the use of LawTech, in particular AI tools?

☐	11. Have you given due consideration to the need to inform clients of your use of LawTech, including the extent of usage, billing or cost implications, etc.?
☐	12. In respect of legal proceedings, have you considered informing the court or tribunal and the other parties of the use of LawTech for transparency purpose?
D. Use of LawTech	
☐	13. Do you understand the current capabilities, limitations and risks of the LawTech tools you choose to use?
☐	14. Have clients given any instructions on whether to use LawTech tools and if so, how and to what extent? Are you complying with such instructions?
☐	15. Have you evaluated the risks of information input and assessed whether your intended input is not inconsistent with any requirements of confidentiality, legal professional privilege or data privacy?
☐	16. Have you conducted a comprehensive risk assessment for the relevant LawTech tool and established commensurate risk management measures, including mitigation protocols for data breaches, or operational failures?
☐	17. Have you put in place a mechanism to independently verify all LawTech-generated outputs, including citations, legal authorities, and factual assertions against the primary sources?
☐	18. Have you maintained a commensurate level of review across all LawTech-generated outputs, thereby mitigating the risks of automation bias or over-reliance?
☐	19. For agentic AI outputs, can you understand the reasoning process and trace action logs to explain how a result is reached?
☐	20. Are you using LawTech tools in any way that may result in non-compliance with the relevant laws, regulations, practice directions, and professional conduct rules, or AI governance and regulatory frameworks of a relevant jurisdiction?