Law Society's Advisory on the Use of Publicly Available AI Tools

Dear Members,

The Law Society brings to the attention of members that the use of technology products or services that are not designed for business or enterprise use, in particular publicly available AI tools, including Generative AI tools, (referred to collectively as "**AI Tools**") may expose lawyers to breaches of the Legal Profession (Professional Conduct) Rules 2015 ("**PCR**"), in particular rule 6 on your duty to maintain client confidentiality.

The Law Society reminds members to be conscious of their various duties to clients, the courts, and fellow members. Publicly available AI Tools are usually intended for use by the general public and may not take into account the specific obligations and duties of lawyers.

Should members choose to use AI tools for legal work, the Law Society recommends that members use paid or enterprise versions of the AI Tools for their professional work after a review of their terms of use and have satisfied themselves that their use of such AI Tools will not lead to any breaches of the PCR.

Recommendations

The Law Society's Generative AI Committee is preparing more detailed guidance for members.

These non-exhaustive recommendations are being made in the meantime. When using publicly available AI Tools, members are reminded:

- To ensure that the terms of use are consistent with your professional duties, in particular your duty to maintain the confidentiality of any client information. Members are therefore advised to read and understand the tool's terms of use. Where the terms of use are in a foreign language, using an automated translation tool may not be sufficient. Members must understand the legal effect of the stated terms.

- If you wish to use such publicly available AI Tools, just like with any other tools available on the internet (i.e. LinkedIn, Twitter, Google searches etc), you must not upload or input (including in the text of a question/prompt) any data, document or information that: (i) is privileged, proprietary or confidential data; and/or (ii) contains personal data. Ensure that the client's confidentiality is maintained. Prompts and documents must be anonymised, and clients' confidential information removed (E.g., Company A / Contract B / Project C). Note that 'blackout tools' often only cover the information in black without removing the underlying text which can still be machine-read. Appropriate redaction software ought to be used by members to anonymise and/or redact documents.

- Where possible, users of both free and paid AI Tools should be aware that their input data may be retained or used for model training by default. Members should review the privacy settings of these tools and opt out if necessary to ensure that input data are not retained or used to train the provider's models.

- To check if the tools you are using have adequate cybersecurity safeguards. This means that the tools have to be compliant with relevant international data governance, privacy and cybersecurity standards.

References

Further information can be found at the resources below. Members are strongly encouraged to refer to them.

- The Law Society of Singapore's Guidance Note 3.4.1 on Cloud Competing
- The Law Society of Singapore's Cybersecurity Guide
- The Law Society of Singapore's Guide on the Adoption of LegalTech for Law Practices
- The Ministry of Law's Guide for Using Generative AI in the Legal Sector

Date: 2 April 2026