24 September 2025

David Connoley
Executive Director
Courts Administration Authority
GPO Box 1068
ADELAIDE SA 5000

The Law Society
OF SOUTH AUSTRALIA

By email: david.connoley@courts.sa.gov.au;
joshua.patterson@courts.sa.gov.au

Dear David

Harnessing AI Collective: Survey and interview results

2. On 30 May 2025, the Chief Justice launched a survey to the legal profession about the use of generative Artificial Intelligence (AI) in the South Australian courts. The survey was open for a period of three weeks. Written submissions were also invited. During June and July 2025, the CAA conducted a series of qualitative interviews to support the survey. We note that the CAA has completed the qualitative interview process, the results of which are contained in the report provided.

3. We understand that the Chief Justice has requested feedback from the Society on the report to inform the possible creation of a practice note or guidelines in relation to the use of AI within South Australian Courts.

5. The Society supports the CAA's broad and consultative approach to consideration of the use of generative AI within the Court and appreciates the opportunity to consider and comment on the preliminary results.

6. The Society observes the range of views summarised within the preliminary report on the survey results, which reflects an unsurprising diversity of experience, understanding and comfort existing within the legal profession.

7. Some members of the legal profession advise that they are using AI daily to assist in completing work tasks, but that generally AI is seen as a supplementary tool to assist rather than technology that can provide a definitive or correct answer. It is well known that as AI needs to output an answer, if it does not know the answer it will provide a "hallucinated" answer which may not be correct or may simply be made up. The use of AI needs to be verified using reliable sources.

8. The Society observes that tools which use generative AI technologies are being increasingly integrated into a broad range of applications used by the Courts, legal professionals, clients, litigants in person, and other participants in the justice system. The pace of change and innovation is extremely rapid. This carries both opportunities and risks for access to justice which warrant careful consideration. The Society considers that being overly prescriptive is unlikely to be helpful in such a rapidly evolving field.

9. The Society is supportive of the Court developing guidelines and resources in relation to the use of AI. The Society considers that in doing so, it should adopt a principles-based, rather than prescriptive, approach.

10. The Society considers that guidance to lawyers should specifically reference the existing professional and ethical obligations imposed upon them.

11. The Society's AI and Data Privacy Committee recommends consideration be given to providing guidance for non-lawyers (self-represented litigants) on the use of generative AI.

12. The Society notes that AI should not be equated merely with well-known and generic applications such as Chat GPT. While such applications are one factor to be considered, AI is also being utilised by well-known and reputable suppliers of extremely common IT tools including Microsoft, Adobe, Lexis Nexis and Thomson Reuters, all of which are in common use within the profession.

13. Some such tools are automatically integrated into existing products, while others require taking up new subscriptions. They facilitate tasks as broad-ranging as analysis of lengthy documents by preparing summaries, preparing suggested draft responses to emails, and facilitating legal research by collating and synthesising a selection of suggested resources. Anyone using Google is, to an extent, using AI due to the "AI Overview" response that is generated. The definition of what tools the policy or guideline would apply to will likely need to be defined.

14. There are also a raft of more bespoke tools in use, including proprietary software used to assist in large-scale discovery and document analysis processes (most commonly by large firms in large scale commercial litigation), and bespoke internal precedents systems reportedly being developed by some firms. Consultation with an extremely broad range of stakeholders – likely extending beyond the focus groups who have already participated – would be required to gather anything approximating a relatively comprehensive list of categories, and no list will ever be capable of being exhaustive and is likely to continually evolve.

15. The Society suggests that guidelines and resources around the use of such technologies ought to address broad issues of principle and ethics which arise in relation to the use of AI, and provide high-level guidance on the manner in which such principles apply to its use. The Society considers that this could include:

    15.1. Protection of confidentiality and privilege, and observance of *Harman* undertakings, in the use of AI technologies within legal contexts: there may be a need to ensure practitioners and litigants are reminded that the use of AI technologies offers no exemption or exception to such principles and professional obligations. Many such technologies (particularly those available freely online) harvest all information fed to them, such that their use in relation to client information or information obtained in the course of legal proceedings carries significant risks.

    15.2. Verifying output: The use of AI in drafting documents, submissions, etc., can be a useful starting point – but is a starting point only, and any information obtained from AI should always be confirmed as accurate by a solicitor. AI output should always be vetted (by a lawyer and not by another AI tool) and treated with caution.

    15.3. Personal responsibility for verifying work product: just as a practitioner or litigant who puts their name and signature to a document prepared by a junior employee or colleague is generally viewed to be taking responsibility for the content of that document, so too should a practitioner or litigant who relies on AI-based tools to prepare work which they submit to a Court. There are numerous existing examples within the forms prescribed by the Uniform Civil Rules in which certificates are required to be given by legal practitioners as to compliance with their obligations under those rules. It may be prudent to consider as part of guidelines around use of AI whether any updates are required in relation to current forms to expand that practice, or otherwise ensure that the person responsible for the preparation is

identified in all relevant cases, and to remind practitioners that use of AI offers no exemption or exception to ordinary principles regarding responsibility for the content of material filed with or put before the Court.

15.4. Attribution and acknowledgement: legal practitioners and Courts are familiar with the need to provide references to authorities and evidence upon which they rely. The Court may wish to consider whether it thinks it appropriate that such principles be extended to require declaration or disclosure in relation to any material which has been prepared with the assistance of AI-based tools, both in the interests of transparency and accountability, and to facilitate more rigorous interrogation of whether other principles are being followed. Conversely, there may be complexities associated with such a requirement, arising from the very broad range of available tools, and the vastly differing level of input and impact their use may have into a finished product produced to the Court. It may be that subject to appropriately addressing the issue of personal responsibility for work product, it is preferable not to impose prescriptive rules of this nature.

15.5. Giving statements: it appears from some of the submissions and discussions in the report that the preparation of written forms of witness evidence such as affidavits, statements and expert reports is a particular topic which gives rise to strong and sometimes differing views – both in respect of the use of AI and existing practices. This is likely to be a particular area that warrants specific guidance.

16. The Society's AI and Data Privacy Committee suggests consideration of a 'traffic light' approach to guide users, such as:

- Red: No entry of client confidential, legally privileged, or sensitive personal information. This may need to be well defined.

- Yellow: Use with caution for semi-sensitive data and internal drafting, perhaps only with enterprise-grade AI solutions under contract (noting that this has some unknown risks).

- Green: Low-risk uses such as administrative support, summarising public material, formatting, brainstorming. Further examples may help to guide this interpretation.

Issues of data security

17. Extreme care should be taken in considering what types of information are appropriate to enter into AI systems and stronger safeguards or prohibitions should be considered for highly sensitive or privileged material.

18. While many generative AI providers state that users can opt out of having their data used to train models, there is currently no effective way to independently verify or enforce this. This presents a significant risk, particularly when sensitive or legally privileged information is involved.

19. Compounding this issue is the fact that the pool of freely available human-generated data scraped from the internet is diminishing. Some providers have already turned to using AI-generated content to train their models, but this approach has proven inadequate with reports indicating that such data often leads to unusable or degraded output data. As a result, providers may be driven to seek more creative, or even desperate ways to obtain authentic human-generated data (such as the user submitted data which was not supposed to be obtained). This raises concern that information entered into these systems could become a highly attractive target for future model training, regardless of current assurances that human-submitted data will not be used to train these systems.

20. Further, although existing guidance across the internet often recommends deidentifying data before inputting it into such systems, there is insufficient evidence that this is a reliable safeguard. Due to the way large language models operate, it may be trivial for the system to link separate fragments of information and effectively reidentify supposedly deidentified data.

21. As these models continue to advance, with computing power and capabilities increasing exponentially every few months, the risks compound. Data that may appear secure or anonymous now could, in future, be reidentified with relative ease as models become more powerful.

22. A useful comparison can be drawn to legal practice management systems. These are often offered 'on the cloud', often held overseas and under the control of a software vendor, or alternatively, on an 'on-premises' server where the firm retains effective control over both hardware and software. Highly sensitive data should only be used on a closed server environment where an organisation has effective and total control of the hardware. This is different from using, for example, a business ChatGPT or Copilot Business account which may state that all data is retained within the boundaries of the organisation's dataset, but in practice the infrastructure remains under the vendor's control and potentially open to exploitation and use by third parties.

23. In addition, much of this infrastructure is hosted in overseas jurisdictions where local laws may compel access to data for various reasons. It is timely to consider this, particularly as geopolitical and political tensions continue to increase.

24. The pace of AI technology and the need for commercial companies to be seen to be on the cutting edge of technology, may lead these providers to forego checks and balances in terms of data security to quickly create a competitive product they can roll out. Poor data handling and/or misusing data to improve their products may well be seen as an acceptable cost to these companies. The Society doubts whether accepting the word of commercial vendors is a reasonable discharge of a firm's obligations, if it is later shown that client data has left the server or been misused to train AI models.

Transcription services

25. The Society also considered the issue of automated transcription services which are increasingly used to audio/video record meetings with clients and generate transcriptions. These might be inbuilt into products such as Microsoft Teams or might be other standalone products. The Society observes the importance of obtaining consent to recording, especially where meetings include personal or other identifying information.

26. Practitioners also need to be mindful of their obligations under the Privacy Act 1988 (if applicable to their organisation) including in respect of use and disclosure and review their privacy and data collection policies where personal information is being input into AI tools. This is particularly so in circumstance where information is held by the vendor and AI tools may 'learn' from information, which may not be consented to by clients.

The Society thanks you for the opportunity to review the report and provide initial comments.

Should you have any queries, please do not hesitate to contact me.

Marissa Mackie
President