LEGASTAT
Expert Litigation Support

GenAI. Disclosure. Privilege. Confidentiality.

Using AI in disclosure without compromising confidentiality and privilege



The Law Society recently published a practical note on Using artificial intelligence in legal practice. The guidance provides useful reminders and, more importantly, a framework for litigators considering how AI can safely be used in legal work.

The guidance does not prescribe a particular disclosure methodology, validation protocol or technology-assisted review workflow. Instead, its focus is firmly on professional responsibility and risk management.

For those involved in disclosure, we picked out four particularly important points.

Responsibility for the disclosure statement remains with the lawyer

There is currently no general requirement to tell the court simply because AI has been used to assist with research, drafting, review or document production. The lawyer whose name appears on the document remains responsible for its contents. That position may evolve.

The Civil Justice Council's 2026 consultation on AI and court documents considered whether different requirements may be appropriate for statements of case, advocacy documents, disclosure statements, witness statements and expert reports.

Among the approaches considered were specific declarations where AI materially affects the substance or presentation of evidence and, potentially, disclosure of prompts entered into AI systems.

For now, these remain proposals rather than a general obligation. However, they indicate the direction of travel: the more substantive the role played by AI, the greater the potential need for transparency around its use.

Breaching confidentiality and waiving privilege could be one click away

This is perhaps the most immediate concern for anyone considering AI-assisted disclosure. Disclosure datasets routinely contain confidential, personal, commercially sensitive and privileged information. Before that information is placed into an AI system, the legal team needs to understand where the data will be stored and processed, who can access it, whether information is retained and whether it could subsequently be used for monitoring, product improvement or model training.

The Law Society highlights *UK and R (on the application of Munir) v Secretary of State for the Home Department [2026] UKUT 81 (IAC).* The tribunal observed that uploading certain confidential information into a publicly available AI system could place that information into the public domain, potentially breaching confidentiality and waiving privilege.

This is where the environment in which AI operates becomes critical. There is a fundamental difference between putting disclosure material into a publicly available AI tool and using AI within a secure, closed eDiscovery environment designed to protect the underlying data.

But a system being described as closed or secure is not enough on its own. The contractual and technical safeguards still need to be understood. This is one of the areas where experienced eDiscovery providers have an increasingly important role to play: creating a controlled environment in which legal teams can take advantage of AI without exposing sensitive material.

Client transparency becomes more important as AI becomes more substantive

The guidance draws an important distinction between routine or administrative uses of AI and its use for substantive legal work. Specific disclosure or client consent may not be necessary for administrative applications, particularly where AI operates within secure organisational systems and client information is not being used to train the technology.

The position becomes more sensitive where AI is analysing disclosure material, processing identifiable client information, contributing to substantive legal work or potentially affecting evidence or court documents. This suggests a useful principle:

The greater the influence AI has on the substantive legal work, the more important transparency, governance and oversight become.

Law firms and their eDiscovery providers should therefore be able to explain what systems are being used, what they are being used for, whether client information enters those systems, how that information is protected and what human review sits behind the resulting work.

Human review remains essential

Secure technology addresses only one part of the risk. The other is over-reliance on the technology itself. The guidance specifically warns about automation bias, the tendency to accept an automated result even when it may be incorrect. AI outputs should instead be approached with appropriate professional scepticism, much as the work of a trainee or junior colleague would be reviewed.

For disclosure, that means AI should not operate as an autonomous decision-maker. Its role should sit within a controlled process combining secure technology, experienced eDiscovery project management, appropriate validation and legal oversight. The technology may assist with increasingly substantive work, but someone still needs to understand what it has done, what information it has considered, the limitations of the process and how its results have been checked.

What can you do to ensure privilege is protected?

As AI becomes integrated more deeply into disclosure, the eDiscovery providers are no longer simply supplying document hosting, processing capacity or review technology. They become part of the risk-management framework around the use of AI. In this context, it is important to understand:

- Where is the data hosted, including any backups or DR facilities?
- Are the GenAI systems using your data to train the algorithm?
- Is AI performing a substantive task in your disclosure?
- What quality checks are in place to validate the AI outputs?

The opportunity presented by AI in disclosure is significant. It can help legal teams analyse and navigate increasingly large volumes of information, but efficiency cannot come at the expense of confidentiality, privilege or professional responsibility.

If you are dealing with a complex or data-heavy matter and considering how AI could safely support the disclosure process, speak to Legastat about the technology, controls and workflows available.